House of Commons
House of Lords

Joint Committee on Human Rights

Human Rights and the Government's Response to Covid-19: Digital Contact Tracing

Third Report of Session 2019–21

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 6 May 2020

HC 343
HL Paper 59
Published on 7 May 2020
by authority of the House of Commons
and House of Lords

Joint Committee on Human Rights

The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders.

The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

Current membership

House of Commons

Ms Harriet Harman QC MP (*Labour, Camberwell and Peckham*) (Chair)

Fiona Bruce MP (*Conservative, Congleton*)

Ms Karen Buck MP (*Labour, Westminster North*)

Joanna Cherry QC MP (*Scottish National Party, Edinburgh South West*)

Mrs Pauline Latham MP (*Conservative, Mid Derbyshire*)

Dean Russell MP (*Conservative, Watford*)

House of Lords

Lord Brabazon of Tara (*Conservative*)

Lord Dubs (*Labour*)

Baroness Ludford (*Liberal Democrat*)

Baroness Massey of Darwen (*Labour*)

Lord Singh of Wimbledon (*Crossbench*)

Lord Trimble (*Conservative*)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publication

Committee reports are published on the Committee's website at www.committees.parliament.uk/committee/93/human-rights-joint-committee by Order of the two Houses.

Committee staff

The current staff of the Committee are Miguel Boo Fraga (Senior Committee Assistant), Samantha Granger (Deputy Counsel), Shabana Gulma (Specialist Assistant), Zoe Grunewald (Media Officer), Katherine Hill (Committee Specialist), Eleanor Hourigan (Counsel), Lucinda Maer (Commons Clerk), and George Webber (Lords Clerk).

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on Human Rights, Committee Office, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 2467; the Committee's email address is jchr@parliament.uk

You can follow the Committee on Twitter using @HumanRightsCtte

Contents

Summary

The Covid-19 pandemic presents significant challenges for governments across the world. In addressing the virus, the Government is required to protect the right to life, guaranteed by Article 2 of the European Convention on Human Rights (EHCR). The UK, like many countries, has sought to protect the right to life by enforcing "lockdowns" which have placed severe restrictions on individuals' movements, with significant and wide-ranging implications for human rights.

The UK Government now has plans to release a contact tracing app as part of its strategy to "test, track and trace to minimise the spread of Covid-19 and move towards safely reducing lockdown measures."[1] The app would notify individuals who may have been exposed to the virus to take the appropriate action such as to self-isolate or to get tested. If effective, a contact tracing app could pave the way out of current lockdown restrictions, enabling individuals to move around more freely whilst helping to prevent the spread of the virus.

However, any such app will have an impact on the right to private and family life, protected under Article 8 of the ECHR. If a contact tracing app enables people to move around freely and safely, and is accompanied with the sufficient protections, then the risk to privacy could be a more proportionate interference with individuals' human rights than current restrictions imposed by the lockdown. However, there are significant concerns about a tracking app being rolled out at speed with the potential longer-term effects on personal freedoms and concerns around surveillance encroaching on people's everyday lives. Such an app must not be rolled out nationally unless strong safeguards and protections are in place.

It is not clear that the current legal and regulatory arrangements provide satisfactory, indeed the necessary, legal oversight required. State-controlled apps that enable the mass surveillance of personal data, and that could then enable the (proportionate or otherwise) violation of fundamental rights are novel. The introduction of such an app is an innovative apparatus of state interaction with its citizens. The implications of such an app are so widespread, significant, and, as yet, subject to limited public examination, that they should be subject to the in-depth scrutiny of Parliament at the earliest opportunity. The Committee is concerned that this has not happened to date.

Previous extensions of state powers of surveillance and data collection for the purposes of terrorism prevention have been legitimised by legislation scrutinised by Parliament; and so, it should be for public health purposes.

Having a carefully considered legislative basis for this app would better engender public trust and participation.

Legislation would require a formal human rights assessment to take place. This degree of formal rights balancing is lacking at present, being left to the NHSX team and its advisory bodies. In particular, Parliamentary scrutiny would allow for consideration as to whether the use of a centralised system, as opposed to a decentralised system, is

1 *"Coronavirus test, track and trace plan launched on Isle of Wight"*, Department of Health and Social Care press release, 4 May 2020

reasonable and proportionate. The implementation and oversight of this app must, in our view, be urgently placed on a legislative footing; if rolled out without being governed by a clear legislative framework it risks not complying with the provisions of the ECHR.

In our view, a contact tracing app must not be rolled out nationally unless there are guarantees with respect to:

- Efficacy and proportionality: Unless the efficacy and benefits of the app are clear, the level of data being collected will be not be justifiable and it will therefore fall foul of data protection law and human rights protections. The Science and Technology Committee has been focussing on this and our Committee will focus on the necessary privacy protections. However, the app will not be as effective if uptake is low and uptake is likely to be lower without user confidence in privacy protections—so we consider that the privacy protections are themselves key to the effectiveness of the app.

- Primary legislation: The Government's assurances about intended privacy protections do not carry any weight unless the Government is prepared to enshrine these protections in law. Any data gathering by the app must be accompanied with the appropriate guaranteed protections for personal data to ensure the impact on privacy is minimised as far as possible. Privacy protections applicable to the contact tracing app must be placed on a legislative footing. This would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app; increase uptake; and therefore improve the efficacy.

- Oversight: There should be an independent body to oversee the use, effectiveness and privacy protections of the app and any data associated with this contact tracing. The independent monitoring body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how the app is working. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions.

- Child safeguarding: In all aspects of usage of the app, children under 18 must be given protection and support as expressed in the UN Convention on the Rights of the Child (UNCRC), the ECHR and in domestic legislation.[2] Children and parents should be given information and training in the use of the app and reassurances about safety.

- Efficacy review: The Health Secretary must undertake a review every 21 days of the app's efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data. The Health Secretary must report to Parliament on the conclusions of each review.

- Transparency: The Government and health authorities must at all times be transparent about how the app, and data collected through it, is being used, including publishing ethics reviews and sufficient technical specification information relating to the app and to data security.

2 See in particular, UNCRC, Article 3, and the Children Act 2004, Section 11

1 Introduction

What is contact tracing?

1. Covid-19 emerged in late 2019 in the city of Wuhan in Hubei province, China. Its origins are yet to be confirmed. It spread quickly through the population in Wuhan and to slow transmission the Chinese Government implemented a strict "lockdown" of the city and later the province. As the virus spread internationally, other countries introduced their own lockdowns, although the restrictiveness of the measures varied and few matched the intensity of the Chinese approach.

2. South Korea avoided imposing a blanket lockdown through a mass testing regime and tracing the contacts of those who had been infected so they could self-isolate and break the chain of transmission. This included the use of a contact tracing app but was combined with extensive manual contact tracing. With just 255 deaths as of 5 May 2020, and daily life largely proceeding as normal, it is widely recognised that much can be learnt from South Korea's response.

3. The Government announced on 5 May 2020 that the UK had passed 29,000 confirmed deaths from Covid-19, a similar amount to Italy and second only behind the United States in terms of the total death toll. The privacy concerns about the contact tracing app are certainly pertinent to human rights, especially Article 8, which protects the right to private and family life. However, Governments also have a responsibility to protect Article 2 ECHR, the right to life. If the app demonstrably protects lives and can help to ease the constraints of a lockdown, then this is a very relevant factor in assessing the proportionality of any interference with the right to a private life under article 8 ECHR. However, any contact tracing must only interfere with the right to privacy to the strict extent necessary to achieve its objectives of combatting the disease, so robust privacy protections will be important and where exactly the line is drawn is a matter of debate.

4. Contact tracing is one way of trying to control and track the spread of the virus. It involves notifying individuals when they have come into contact with others who may have been exposed to the Covid-19 virus and giving them appropriate advice, for example to get tested and or to self-isolate, in order to minimise the further spread of the virus. Several countries are using smartphones to speed up the process of contact tracing.

5. Digital contact tracing generally works by an app on a user's smartphone registering and storing details of another smartphone when it is within a defined distance for a certain period of time and if a user tests positive for (or is suspected of having) the virus, the app notifies these contacts that they may themselves be affected. There are a number of different approaches to digital contact tracing which have been discussed at length by academics in recent weeks. Some of the key differences, which have implications for privacy, are discussed briefly below.

Different models/approaches which exist

A centralised or decentralised approach?

6. A major area of discussion around the development of the app has been whether the NHSX should adopt a "centralised" or "decentralised" approach to data storing and sharing. The two models are explained briefly below:

- Decentralised models: most data is stored locally on an individual's phone and as little data as possible is shared with the NHS.
- Centralised models: data is shared with a central server managed by the authority which carries out data processing and/or storage.[3]

The Information Commissioner's Office, privacy experts and organisations, as well as the European Parliament and the European Data Protection Board (EDPB) have indicated a preference for a decentralised approach.[4] It is considered that this would provide greater protection against the abuse of people's data than apps which pull data into centralised pots and have a higher risk of security breaches as well as being much more invasive into the private lives of individuals. There are heightened risks with centralised models with their "potential to de-anonymise data and develop profiles of individuals' social interactions."[5] However, it is asserted that a centralised approach has "public health advantages," in that, it allows health authorities to analyse how the virus is spreading. In turn that allows them to help prevent the spread of the virus (and therefore deaths caused by it), to allow hospitals in virus hotspots to prepare for a surge in cases, and to lessen the invasive nature of the lockdown provisions to the extent possible. It also allows them to improve the efficacy of the app in future versions.[6]

7. The developers of the NHS tracking app have stated that the purpose for choosing a centralised database model over the more data-secure and private de-centralised model is that it allows for greater data analysis. It is not clear that the additional functionality of a centralised data system outweighs the risks inherent in such a model. Such risks may include:

- Less secure data storage (privacy) due to a centralised server.
- Greater incentives to hack centralised databases.
- Identifier numbers are permanent records of one individual, unlike in most de-centralised systems.
- The functionality of a centralised model, if preferred for the benefit of increased analysis, could encourage more data being requested from users in the future, 'mission creep'.

3 UK Parliament POST, Contact tracing apps for Covid-19, 1 May 2020

4 European Parliament, Joint Motion for a Resolution, 15 April 2020; European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak, Adopted 21 April; Written evidence from Professor Lorna McGregor et al (COV0090)

5 Written evidence from Professor Lorna McGregor et al (COV0090)

6 Oral evidence taken on 4 May, HC (2019–21) 265, Q19 [Matthew Gould]

- Issues with compatibility with de-centralised systems (notably the Republic of Ireland) used in the majority of other countries, as recognised by NHSX.

8. It has been noted that the UK is an outlier. While giving evidence to the Committee, Matthew Gould and Dr Michael Veale, lecturer in Digital Rights and Regulation, University College London, both accepted that the technical difficulties of switching the current model to a de-centralised system were manageable.[7] The NHS tracking app asks for post code area information. In some parts of England there are less than 10,000 people in a post code area. Three or four 'bits' of information can be can enough to identify individuals. If NHSX were to add location data to the current model, could easy and consistent individual identification become possible, especially with a centralised data system? The Committee expresses concern that the centralised model is being proposed without there having been the opportunity for Parliamentary debate and consideration of the alternative.

Self-reporting or diagnoses and testing?

9. Another difference between approaches is how to notify the app of an infection. This could be done via self-reporting into the app; by uploading confirmation of an approved test; or health authorities themselves uploading results onto the app server. Relying upon self-reporting alone may carry the risk of false alerts, thereby impacting on other people's rights if they have to isolate unnecessarily.

Voluntary or mandatory

10. Another area of discussion has been around whether a contact tracing app should be voluntary or mandatory to use. The Information Commissioner, the European Data Protection Board (EDPB) and other privacy experts have indicated that the use of contact tracing applications should be voluntary.[8] The EDPB have said that this would imply that "individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all."[9] Some academics in the UK have called for protection for groups who do not have access to smartphones to ensure that they are not penalised for not using the app.[10]

The UK's plan to release a contact tracing app

11. The UK Government is going ahead with its plans to release a contact tracing app. A Government press release dated 4th May 2020 contained details of the first phase of the Government's "test, tack and trace programme," which includes roll out of the NHS Covid-19 App in the Isle of Wight. The Government's intention is to use the app as a tool to "minimise the spread of Covid-19 and move towards safely reducing lockdown measures."[11]

7 Oral evidence taken on 4 May, HC (2019–21) 265

8 See, Information Commissioner's Office, Covid-19 Contact tracing: data protection expectations on app development, page 4, point 9, 4 May 2020.

9 European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak, Adopted 21 April.

10 Paper which includes a proposal for a draft bill by Professor Lilian Edwards and Co, see "The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates"

11 "Coronavirus test, track and trace plan launched on Isle of Wight", Department of Health and Social Care press release, 4 May 2020

12. We took evidence from Matthew Gould, CEO of the NHSX, the Information Commissioner, Dr Orla Lynskey and Dr Michael Veale and others on the UK's plan to release a contact tracing app.[12] We are grateful for their evidence. We were also assisted by a specialist advisor Adam Wagner with this inquiry.

NHSX's current approach to the app

13. The NHSX app will use the centralised model for data storage and sharing. It will work by logging the distance between an individual's phone and other phones nearby that also have the app installed using Bluetooth Low Energy. Unless a user becomes ill, this log will be stored on an individual's phone and the data deleted every 28 days. Matthew Gould, Chief Executive of NHSX, told us that users who become ill will then have the choice to upload the information from the app onto the central server. Users will also be able to give their anonymous contacts to the central database which will identify which contacts are at risk and notify them accordingly. It will also allow the NHS to use the anonymised data to understand how the virus is spreading.[13]

Concerns with the current approach

14. While a recent poll has shown that 65% of people in the UK are in favour of having an app to track the virus, a number of privacy concerns remain with the approach being adopted by the UK. The main concerns with the NHSX's current approach are outlined below:

- Efficacy and proportionality—there is a lack of evidence that a contact tracing app would be an effective tool in suppressing the virus.[14] Concerns have been expressed as to whether the contact tracing app will work on a technical level. Moreover there are significant concerns around interoperability with other countries systems, with particular concerns on the interoperability of systems on the island of Ireland. If it interferes with privacy rights but is too ineffective to fulfil its objective, then the interferences with the right to private life will not be proportionate.

- Mission creep—there are concerns that given NHSX's plans to upgrade the app in "future releases", there will be a risk of creating systems that can be changed incrementally, thus changing the privacy protections upon which the data was initially collected and shared. If that happens, vital privacy protections, and safeguards might be undermined. The capacity to include location data is a concern as it could reveal sensitive information, including relating to third parties.

- Purpose of data use and data retention—Matthew Gould has noted that the "data will only ever be used for NHS care, management, evaluation and research". There are concerns that this is a broad and unclear purpose and may extend

12 Oral evidence taken on 4 May, HC (2019–21) 265

13 National Cyber Security Centre, The security behind the NHS contact tracing app, 4 May 2020

14 The Ada Lovelace Institute's Rapid evidence review on the technical considerations and societal implications of using technology to transition from the Covid-19 crisis found that there is no public study into the effectiveness of digital contact tracing and its key finding was that there is "currently insufficient evidence to support the use of digital contact tracing as an effective technology to support the pandemic response," 20 April 2020.

beyond preventing the spread of Covid-19.[15] Matthew Gould in evidence said data shared with the NHS 'can be retained for research in the public interest or for use by the NHS for planning and delivering services', the latter potentially opening the way for sharing a) within government beyond the NHS and b) with private companies. Matthew Gould also said in evidence that data submitted to the NHS database will not be deleted and could be used in an anonymised form for research purposes. If data is held indefinitely even in an anonymised form, then this raises data protection concerns not least due to data reconstruction risks (i.e. that 'anonymised' data is used to identify individuals) and is likely to affect uptake of the app. The risk of data reconstruction may be enhanced by the fact that users of the app will be required to enter the first half of their postcode.[16]

- Need for legislation and oversight—Several academics and organisations have called for legislation to provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. There are also calls for proper oversight mechanisms to monitor efficacy, impact on privacy and other rights.[17]

Human rights framework

15. The overall Government response to Covid-19 raises core human rights considerations. In addressing the virus, the Government is required to protect the right to life, guaranteed by Article 2 of the European Convention on Human Rights (EHCR). In doing so, many countries, including the UK have placed severe restrictions on individuals' movements by enforcing "lockdowns", which themselves have wide ranging implications for human rights. The lockdown measures are a significant interference with the right to family and private life, (Article 8 of ECHR), the right to free movement (Article 12 International Covenant on Civil and Political Rights 1966), freedom of assembly and association (Article 11 ECHR), freedom of religion or belief (Article 9 ECHR), the peaceful enjoyment of possessions (Article 1 of Protocol 1 ECHR) and the right to education (Article 2 of Protocol 1 ECHR). One way of easing lockdown restrictions is to seek to contain the virus through a variety of other techniques including digital contact tracing, which itself will interfere with the right to private life (Article 8 ECHR) as well as requiring a very careful analysis of compatibility with data protection and privacy law.

16. In the UK privacy law is protected by Article 8 ECHR, the common law duty of confidence, the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (which has equivalent protections to the GDPR under the "UK GDPR" that will succeed the GDPR after Brexit transition).

17. The seven data protection principles under the GDPR[18] (and mirrored by the UK GDPR) provide a basis for considering the issues which need to be addressed before an app is released:

15 Written evidence from Professor Lorna McGregor et al (COV0090)
16 Oral evidence taken on 4 May, HC (2019–21) 265, Q15 [Matthew Gould]
17 Ada Lovelace Institute, Exit through the App Store? 20 April 2020
18 During the transitional period, until 31 December 2020, the GDPR (EU General Data Protection Regulation) applies to the UK. After this time, the same data protection principles will continue to apply, but flowing from the Data Protection Act 2018 and referred to as the "UK GDPR".

a) Data minimisation: The processing of personal data should be limited to what is necessary.

b) Purpose limitation: organisations need to be clear about the purposes for processing data from the start of data processing and collection. This must be specified in privacy information provided to individuals.

c) Storage limitation: Personal data must not be kept for longer than is necessary for the purposes for which the personal data is processed.

d) Integrity and confidentiality: Appropriate security measures must be in place to protect personal data e.g. from accidental breaches.

e) Lawfulness, fairness and transparency: Personal data must be processed in a transparent manner and data organisations must be clear about how they will use personal data.

f) Accountability and accuracy: Organisations must take responsibility for what they do with personal data and must take all reasonable steps to ensure that personal data held is not incorrect.[19]

19 For more information on these, see the Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), the Principles

2 Our proposals

Efficacy and proportionality

18. The lockdown itself constitutes an interference in the human rights of individuals and is currently justified by the need to protect human life. It is appropriate that the Government is exploring options to save lives and to ease the restrictions caused by lockdown. The app's contribution to reducing the severity of the lockdown and to helping to prevent the spread of Covid-19 must be demonstrated and improved at regular intervals for the collection of the data to be reasonable. This is the basis on which any discussion around the privacy concerns must proceed: if the digital contact tracing system does not work, or only has a minimal effect, the collection of huge amounts of data is indefensible.

19. **The amount of data the contact tracing app requires on the private and family lives of individuals is not justifiable if the app does not contribute meaningfully to the easing of lockdown restrictions and the combatting of Covid-19. Digital contact tracing will not be as effective if uptake is low. Uptake will be lower without user confidence in privacy protections—therefore robust privacy protections are themselves key to effectiveness of the app and the digital contact tracing system. Interoperability with other countries' systems will also be relevant to efficacy, not least to ensure that there is interoperability of systems in use on the island of Ireland. The Republic of Ireland has elected to use a decentralised app and if a centralised app is in use in Northern Ireland, there are risks that the two systems will not be interoperable which would be most unfortunate.**

Privacy and other Human Rights Protections

20. The Heath Secretary has informed us that he has appointed an independent Ethics Advisory Board.[20] That is welcome but insufficient. **There needs to be established by law and with sufficient powers a Digital Contact Tracing Human Rights Commissioner who would not only exercise oversight with the appropriate powers but also be able to deal with any complaints from the public and report to Parliament.**

21. ***The Government must not roll out the contact tracing app nationally unless the following protections are in place:***

a) ***Primary legislation: Government assurances about intended privacy protections for any data collected do not carry any weight unless the Government is prepared to enshrine these protections in legislation. A Bill would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app, increase uptake, and improve efficacy.***

b) ***Oversight: There should be an independent body, such as a Digital Contact Tracing Human Rights Commissioner, to oversee the use, effectiveness and privacy protections of the app and any data associated with digital contact tracing. The independent monitoring body should have, at a minimum,***

20 Response from Rt Hon Matt Hancock MP, Secretary of State for Health and Social Care, regarding the Government's plans to use digital technologies, dated 4 May 2020

similar enforcement powers to the Information Commissioner, to oversee how data collected is being used and protected. To guard against mission creep it cannot be left to the Information Commissioner's Office to be the only body with powers of oversight or sanction; such an Office is not designed to monitor the significant rights-based implications that app based surveillance raises and, in addition, the Information Commissioner has been involved in the development of the app. Matthew Gould in his evidence to the Committee stated "However, we do not yet know exactly how it will work; we do not know all the consequences. There will be unintended consequences and there will certainly be some things that we have to evolve." In light of this, the speed of piloting and intended roll out, it is imperative that an independent oversight body be established immediately. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions.

c) ***Child Safeguarding: Particular safeguards should be applied to children under 18. Children's use must be monitored in relation to data collection and use of data. Misuse must be identified and rectified promptly. Interviews with children and parents (where appropriate) must take place in order to support children and act on any concerns.***

d) ***Efficacy review: The Health Secretary must undertake a review every 21 days on the digital contact tracing system. Such reviews must cover efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data. The Health Secretary must report to Parliament every 21 days on the findings of such reviews.***

e) ***Transparency: The Government and health authorities must be transparent about how the app, and data collected through it, is being used. The Data Protection Impact Assessment must be made public and updated as digital contact tracing progresses.***

f) ***Time-limited: Any digital contact tracing (and data associated with it) must be permanently deleted when no longer required and in any event may not be kept beyond the duration of the public health emergency.***

Legislation

22. Once the app's utility is demonstrated, we recommend that the data and other human rights protections should be placed on a legislative footing. This would further improve efficacy by increasing uptake.

23. **The current data protection framework is contained in a number of different documents and it is nearly impossible for the public to understand what it means for their data which may be collected by the digital contact tracing system. Government's assurances around data protection and privacy standards will not carry any weight unless the Government is prepared to enshrine these assurances in legislation.** ***Such a Bill must include the following provisions and protections:***

a) ***Set out the clear and limited purposes of this app for data processing: Personal data may only be collected and processed for the purpose of preventing the spread of Covid-19. No personal data collected through the digital contact tracing app may be accessed for any other purpose. No personal data collected through the digital contact tracing app may be shared with third parties. There should be prohibition against data use for certain purposes such as legal proceedings, to support or deny benefits, data sharing with employers.***

b) ***Unless an individual has notified that they have Covid-19 (or have suspected Covid-19) and has chosen to upload their data, all personal data should only be held locally on the user's device and must be automatically deleted entirely from the app every 28 days.***

c) ***Any personal data held centrally (e.g. following a diagnosis of Covid-19 or suspected Covid-19) must be subject to the highest security protections and standards.***

d) ***Limit who has access to data and for what purpose: Data held centrally may not be accessed or processed without specific statutory authorisation, for the purpose of combatting Covid-19 and provided adequate security protections are in place for any systems on which this data may be processed.***

e) ***Data held centrally may not be used for data reconstruction (i.e. where different pieces of anonymised personal data are combined to reconstruct information about an individual through piecing together multiple data sets).***

f) ***Data held centrally must be deleted where a user so requests and may not be held for longer than is required and in any event for no longer than 2 years. All data collected must be deleted once the public health emergency is over.***

g) ***The Minister must undertake a review and report to Parliament on the efficacy and privacy protections relating to digital contact tracing every 21 days.***

h) ***Powers for a Digital Contact Tracing Human Rights Commissioner to ensure that authority has sufficient powers, staff and resources to oversee the roll-out of digital contact tracing, to look into individual complaints, to make binding recommendations on data protection, collection, storage, safety and use.***

24. Furthermore the introduction of this app raises issues that go beyond data protection and privacy. Other human rights which are protected under the Human Rights Act 1998 (HRA) and ECHR are engaged, for example, the right to non-discrimination in employment and immigration matters. The declaration of compatibility with the HRA which would be required to accompany legislation would put the framework for the app on a firmer rights-based footing and ensure protection of all the rights engaged..[21]

25. There might be concerns that legislating could entail delays which would be undesirable since a key objective is to safely ease the lockdown as soon as possible. But legislation enshrining assurances in law is perfectly viable in time for the national

21 Oral evidence taken on 4 May, HC (2019–21) 265, Q14, 4 May 2020. We also note that Australia has adopted legislation to address human rights concerns with their contact tracing app (The Guardian, Government releases draft legislation for Covidsafe tracing app to allay privacy concerns, 4 May 2020.) Dr Orla Lynskey evidence], and Q25 [Elizabeth Denham OBE]

roll out in the middle of this month. Parliament was able quickly to agree to give the Government sweeping new powers in the Coronavirus Act. If Parliament is able to swiftly enact legislation to confer powers it can do so to circumscribe them. The parties were able to agree that legislation and it should be possible to agree legislation to describe and circumscribe the contact tracing app expeditiously. The law could provide flexibility for any future changes which become necessary by enshrining the principles in primary legislation and the particulars in secondary legislation, which are easier to change but which still have the force of law.

Conclusions and recommendations

Efficacy and Proportionality

1. The amount of data the contact tracing app requires on the private and family lives of individuals is not justifiable if the app does not contribute meaningfully to the easing of lockdown restrictions and the combatting of Covid-19. Digital contact tracing will not be as effective if uptake is low. Uptake will be lower without user confidence in privacy protections—therefore robust privacy protections are themselves key to effectiveness of the app and the digital contact tracing system. Interoperability with other countries' systems will also be relevant to efficacy, not least to ensure that there is interoperability of systems in use on the island of Ireland. The Republic of Ireland has elected to use a decentralised app and if a centralised app is in use in Northern Ireland, there are risks that the two systems will not be interoperable which would be most unfortunate. (Paragraph 19)

Privacy and Other Human Rights Protections

2. There needs to be established by law and with sufficient powers a Digital Contact Tracing Human Rights Commissioner who would not only exercise oversight with the appropriate powers but also be able to deal with any complaints from the public and report to Parliament. (Paragraph 20)

3. *The Government must not roll out the contact tracing app nationally unless the following protections are in place*:

    a) *Primary legislation: Government assurances about intended privacy protections for any data collected do not carry any weight unless the Government is prepared to enshrine these protections in legislation. A Bill would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app, increase uptake, and improve efficacy.*

    b) *Oversight: There should be an independent body, such as a Digital Contact Tracing Human Rights Commissioner, to oversee the use, effectiveness and privacy protections of the app and any data associated with digital contact tracing. The independent monitoring body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how data collected is being used and protected. To guard against mission creep it cannot be left to the Information Commissioner's Office to be the only body with powers of oversight or sanction; such an Office is not designed to monitor the significant rights-based implications that app based surveillance raises and, in addition, the Information Commissioner has been involved in the development of the app. Matthew Gould in his evidence to the Committee stated "However, we do not yet know exactly how it will work; we do not know all the consequences. There will be unintended consequences and there will certainly be some things that we have to evolve." In light of this, the speed of piloting and intended roll out, it is imperative that*

an independent oversight body be established immediately. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions.

c) *Child Safeguarding: Particular safeguards should be applied to children under 18. Children's use must be monitored in relation to data collection and use of data. Misuse must be identified and rectified promptly. Interviews with children and parents (where appropriate) must take place in order to support children and act on any concerns.*

d) *Efficacy review: The Health Secretary must undertake a review every 21 days on the digital contact tracing system. Such reviews must cover efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data. The Health Secretary must report to Parliament every 21 days on the findings of such reviews.*

e) *Transparency: The Government and health authorities must be transparent about how the app, and data collected through it, is being used. The Data Protection Impact Assessment must be made public and updated as digital contact tracing progresses.*

f) *Time-limited: Any digital contact tracing (and data associated with it) must be permanently deleted when no longer required and in any event may not be kept beyond the duration of the public health emergency.* (Paragraph 21)

Legislation

4. The current data protection framework is contained in a number of different documents and it is nearly impossible for the public to understand what it means for their data which may be collected by the digital contact tracing system. Government's assurances around data protection and privacy standards will not carry any weight unless the Government is prepared to enshrine these assurances in legislation. *Such a Bill must include the following provisions and protections:*

a) *Set out the clear and limited purposes of this app for data processing: Personal data may only be collected and processed for the purpose of preventing the spread of Covid-19. No personal data collected through the digital contact tracing app may be accessed for any other purpose. No personal data collected through the digital contact tracing app may be shared with third parties. There should be prohibition against data use for certain purposes such as legal proceedings, to support or deny benefits, data sharing with employers.*

b) *Unless an individual has notified that they have Covid-19 (or have suspected Covid-19) and has chosen to upload their data, all personal data should only be held locally on the user's device and must be automatically deleted entirely from the app every 28 days.*

c) *Any personal data held centrally (e.g. following a diagnosis of Covid-19 or suspected Covid-19) must be subject to the highest security protections and standards.*

d) *Limit who has access to data and for what purpose: Data held centrally may not be accessed or processed without specific statutory authorisation, for the purpose of combatting Covid-19 and provided adequate security protections are in place for any systems on which this data may be processed.*

e) *Data held centrally may not be used for data reconstruction (i.e. where different pieces of anonymised personal data are combined to reconstruct information about an individual through piecing together multiple data sets).*

f) *Data held centrally must be deleted where a user so requests and may not be held for longer than is required and in any event for no longer than 2 years. All data collected must be deleted once the public health emergency is over.*

g) *The Minister must undertake a review and report to Parliament on the efficacy and privacy protections relating to digital contact tracing every 21 days.*

h) *Powers for a Digital Contact Tracing Human Rights Commissioner to ensure that authority has sufficient powers, staff and resources to oversee the roll-out of digital contact tracing, to look into individual complaints, to make binding recommendations on data protection, collection, storage, safety and use.* (Paragraph 23)

Declaration of interests[22]

Lord Brabazon of Tara

- No Interests declared

Lord Dubs

- No Interests declared

Baroness Ludford

- Vice Chair, JUSTICE

Baroness Massey of Darwen

- No relevant interests declared

Lord Singh of Wimbledon

- No Interests declared

Lord Trimble

- No relevant interests to declare

22 A full list of Members' interests can be found in the Register of Lords' Interests: http://www.parliament.uk/mpslords-and-offices/standards-and-interests/register-of-lords-interests/

Formal minutes

Wednesday 6 May 2020

Members present:

Ms Harriet Harman MP, in the Chair

Fiona Bruce MP	Lord Brabazon of Tara
Ms Karen Buck MP	Lord Dubs
Joanna Cherry MP	Baroness Ludford
Dean Russell MP	Baroness Massey of Darwen
	Lord Trimble

Draft Report (*Human Rights and the Government's Response to Covid-19: Digital Contact Tracing*), proposed by the Chair, brought up and read.

Ordered, That the Chair's draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 25 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Third Report of the Committee.

Ordered, That the Chair make the Report to the House of Commons and that the Report be made to the House of Lords.

[Adjourned till 18 May at 2.00pm.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 20 April 2020

Rt Hon Robert Buckland QC MP, Lord Chancellor and Secretary of State for Justice; **Andrew Waldren**, Deputy Director, Human Rights Team, Ministry of Justice	Q1–9

Monday 4 May 2020

Dr Orla Lynskey, Associated Professor of Law, London School of Economics; **Dr Michael Veale**, Lecturer in Digital Rights and Regulation, University College London	Q10–14
Matthew Gould, NHSX, Department of Health and Social Care; **Elizabeth Denham**, UK Information Commissioner, Information Commissioner's Office; **Simon McDougall**, Executive Director, Technology and Innovation, Information Commissioner's Office; **Dr Ian Levy**, Technical Director at National Cyber Security Centre	Q15–26

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

1 Professor Lorna McGregor; Professor Pete Fussey; Dr Daragh Murray; Dr Chris Fox; Dr Ayman Alhelbawy; Professor Klaus McDonald-Maier; Dr Ahmed Shaheed; Professor Geoff Gilbert (COV0090)

2 Supplementary evidence from Dr Orla Lynskey and Dr Michael Veale (COV0093)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2019–21

First Report	Draft Jobseekers (Back to Work Schemes) Act 2013 (Remedial) Order 2019: Second Report	HC 149 HL 37
Second Report	Draft Human Rights Act 1998 (Remedial) Order: Judicial Immunity: Second Report	HC 149 HL 41
First Special Report	The Right to Privacy (Article 8) and the Digital Revolution: Government Response to the Committee's Third Report of Session 2019	HC 313