

Written evidence from the Information Law and Policy Centre, Institute for Advanced Legal Studies, University of London (COV0098)

Submission Summary

The Information Law and Policy Centre (ILPC) is an academic research body within the Institute for Advanced Legal Studies, School of Advanced Study, University of London. The ILPC is focused on promoting, undertaking and facilitating cross-disciplinary scholarship and research in the broad area of information law and policy, both domestically and internationally.

This submission from the ILPC is in response to the recent call for evidence on ‘The Government’s response to COVID-19: human rights implications, from the Joint Committee on Human Rights. It addresses the following key issues and makes some recommendations for the consideration of the Committee:

1. Contact tracing and legally-binding safeguards
2. Data Protection Impact Assessment (DPIA) and Equality Impact Assessments

Author

Dr Nóra Ni Loideain, Director and Lecturer in Law, Information Law and Policy Centre, Institute of Advanced Legal Studies, University of London; Visiting Lecturer in Law, King’s College London; Senior Research Fellow, Faculty of Humanities, University of Johannesburg; Associate Fellow, Leverhulme Centre for the Future of Intelligence, University of Cambridge.

1. Contact tracing and legally-binding safeguards

- 1.1. The ILPC welcomed the opportunity to contribute to a draft bill on legislative safeguards, an initiative led by Professor Lilian Edwards (University of Newcastle): The Coronavirus (Safeguards) Bill 2020.¹ This policymaking initiative was cited by the Biometrics Commissioner in his recent ‘Statement on the use of symptom tracing applications’.²
- 1.2. The following section focuses on one specific legal requirement, namely that any large-scale collection and monitoring of the public’s data should be accompanied by explicit relevant safeguards which are legally binding.
- 1.3. The Rule of Law and the Principle of Legal Certainty – both of these principles require the adoption of any government emergency measure that has significant implications for human rights, as protected under the Human Rights Act 1998, to be accompanied by relevant safeguards that are ‘accessible’ and ‘foreseeable’ to the public within a binding framework.
- 1.4. Article 8 ECHR - protects the right to respect for private life and is clearly engaged by the use of the contacting-tracing app. This interference arises due to the collection and processing of location data and the collection of pseudonymised data (data that may be re-identified and is thus subject to the Data Protection Act 2018)³ and the fact that this data collection involves a vast amount of data obtained by the State from large number of members of the public.
- 1.5. Location data – NHSX has stated that the app will request that individuals provide the first part of their post code (eg ‘SW1’) which identifies a specific geographic area.⁴ In a centralised model, data collected from the monitoring of

¹ <https://osf.io/preprints/lawarxiv/yc6xu/>

² https://www.gov.uk/government/news/biometrics-commissioner-statement-on-the-use-of-symptom-tracking-applications?utm_source=3353e450-982f-403b-bec4-79edcc670835&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate

³ See Data Protection Act 2018 ICO guidance on pseudonymised data falling within the scope of personal data : <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>

⁴ Matthew Gould, Oral Evidence Session, Joint Committee of Human Rights, ‘The Government’s response to

various individual from these specific areas could easily be used to identify networks and clusters of communities and thereby track their movements and interactions with others. It is well established under EU and ECHR case law that the collection, retention, and access to such a significant quantity of data is highly sensitive and constitutes a serious interference with private life.⁵

1.6. Any measure that interferes with the right to private life, as protected under Article 8(1) ECHR, can only be justified if it meets the principles and safeguards required under the conditions of Article 8(2): the legality condition; pursues a legitimate aim; and the proportionality condition.

1.7. The legality condition of Article 8(2) of the ECHR provides that any contacting-tracing app that collects location data and personal data (pseudonymised data) at large scale must have a legal basis that meets the rule of law requirements of ‘accessibility’ and ‘foreseeability’.

1.8. Accessibility and Foreseeability: These tests mean that the legal framework must *explicitly* clarify that it permits the State to collect, retain, and use large amounts of location data and personal data for the legitimate purpose of ‘the protection of health’.

1.9. This means that the domestic law must be sufficiently accessible and clear to give the public an adequate indication to foresee the circumstances and the conditions in which public authorities are empowered to use the data collected from the contact-tracing app, for what specific purposes, and the safeguards that have been put in place.⁶

1.10. In line with the principle of the rule of law, it is essential that the relevant law is particularly precise with ‘clear and detailed rules’ if the technology involved is ‘continually becoming more sophisticated’.⁷ In practice, this means that the need for

COVID-19: human rights implications’, 4 May 2020: <https://www.parliamentlive.tv/Event/Index/6f0f52cf-9fda-4785-bf63-af156d18b6c7>

⁵ Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson*, judgment of 21 December 2016 (ECLI:EU:C:2016:970); *Big Brother Watch and Others v United Kingdom* (2018) ECHR 722.

⁶ *Big Brother Watch* (n 5) [306].

publishing any relevant safeguards in a binding legal framework increases given the increased risk of misuse and abuse that comes with novel and obscure monitoring powers.

1.11. This requirement is therefore particularly relevant to the contact-tracing app regime given its novel use of collecting location data and other personal data via voluntary uptake of a mobile phone app the State has developed using a centralised approach. This is a more privacy-invasive model of data processing that collects more personal data, as opposed to the less privacy-intrusive decentralised model that could be adopted which employs the key GDPR principle of ‘data minimisation’.

1.12. Data minimisation - complying with this principle means that ‘public health authorities and research institutions should process personal data only where adequate, relevant and limited to what is necessary, and should apply appropriate safeguards such as pseudonymisation, aggregation, encryption and *decentralization*.’⁸

1.13. It is well-established under the case law of the European Court of Human Rights that there is an increased need for these safeguards to be published in a legally binding document (ie, a statute, or legally binding code of practice) , where ‘the true breath’ of the authorities discretion to share and use the data is unclear from the relevant legislation.⁹ There is currently considerable ambiguity surrounding who may be permitted access to such data. To date, NHSX has stated that the data may currently be

accessed for those who fall within the very broad scope of ‘an appropriate public health reason’.¹⁰

⁷ *Zakharov v Russia* (2016) EHRR 63.

⁸ European Commission, ‘Commission Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis’ Brussels, 8 April 2020, 6: https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf (emphasis added).

⁹ *Big Brother Watch* (n 5) [315].

¹⁰ Matthew Gould (n 3).

- 1.14. The law should also be accompanied by an officially published document that is easily available and written in language understandable to the public. For instance, this could be a code of practice which should clearly explain how the proposed contact-tracing app will operate, a list of all competent authorities who may access the data.
- 1.15. The Code of Practice should also address and explain the lawfulness of the app, ie how it is complying with existing legal principles and safeguards, as required under the Data Protection Act 2018, the Equality Act 2010, Human Rights Act 1998, and other relevant legislation.
- 1.16. Preventing misuse and abuse - The publication of key legal safeguards for emergency data collection measures adopted by the State is essential in order to prevent the risk of any misuse or abuse of these powers by the State (or those acting on its behalf).
- 1.17. Otherwise, setting out these foreseeability safeguards solely in non-binding internal policies or public statements have been shown in the past to be ‘a recipe for confusion and the watering down of ... legislative standards’.¹¹

Recommendation: In line with well-established ECHR case law, the implementation of the contact-tracing app – given its large scale processing of location data and personal data - must be accompanied by clear and specific safeguards published in a legally binding document.

To not do so immediately calls into question the lawfulness of the data collection and its compatibility with Article 8 ECHR and the Human Rights Act 1998.

Recommendation: This law should also be accompanied by an officially published Code of Practice that is easily available and written in language understandable to the public.

The Code should clearly explain how the proposed contact-tracing app will operate, updated when necessary, and its lawfulness, ie how it meets the relevant principles and

¹¹ Tom Hickman, Joint Committee on the UK Draft Investigatory Powers Bill, Written Evidence (IPB0039)(2015) [34].

safeguards as required under the Data Protection Act 2018 and other relevant legislation.

2. Data Protection Impact Assessments and Equality Impact Assessments

2.1. While it is welcome that the NHSX has stated that a DPIA concerning the contact-tracing app will be made available to the public, there is considerable ambiguity surrounding what human rights impacts will be addressed by this DPIA.

2.2. It is very unclear from evidence presented to the Joint Committee on Human Rights if any consideration will be given in the DPIA to the impacts of the contact-tracing app for human rights other than privacy.

2.3. This raises serious concerns as the data collection and processing of personal data from the app definitely engages other rights, particularly given the monitoring of specific communities enabled by the collection of location data. For instance, it is without question that this processing engages the right to prohibition of discrimination (as protected under Article 14 ECHR) due to the risks of profiling posed by this data collection.

2.4. Given the high risks involved to other human rights, particularly the right to non-discrimination under Article 14 ECHR, it is submitted that an Equality Impact Assessment should also be undertaken and made available to the public.

2.5. Public trustworthiness – in order to make clear to the public that other human rights (in addition to privacy) have also been taken into account by the NHSX in the design

of this contact-tracing app, its legal framework and safeguards, a review of this Equality Impact Assessment should also be published by the Equality and Human Rights Commission.

2.6. As stated recently by David Isaac, Chair of the Equality and Human Rights Commission:

‘As difficult decisions are made we must not forget those people who will be more impacted by this crisis than others. Martin Luther King said: “The ultimate measure of a man is not where he stands in moments of comfort and convenience, but where he stands at times of challenge and controversy”. Britain is a world leader in human rights and now is the moment to demonstrate it.’¹²

Recommendation: The NHSX should make available to the public an Equality Impact Assessment on the impacts of contacting-tracing app for the right to non-discrimination, as protected under Article 14 ECHR, and the safeguards that have been adopted to mitigate these risks.

11/05/2020

¹² <https://www.equalityhumanrights.com/en/our-work/blogs/how-were-responding-coronavirus-pandemic> .