Written evidence from Open Rights Group, Article 19, Index on Censorship (COV117)

Dr. Niaz Chowdhury, Rachel Coldicutt, Ray Corrigan, Jon Crowcroft, Nicholas Gervassis, Wendy M. Grossman, Dr. Adam Harkens, Dr. Tristan Henderson, Arne Hintz, Dr. Julian Huppert, Dr. Argyro Karanasiou, Prof. Douwe Korff, Myles Jackman, Dr. Maureen O. Mapp, Victoria McEvedy, Andrew McStay, Andy Phippen, Prof. Blaine Price, Dr Felipe Romero-Moreno, Dr. Gilad L. Rosner, Javier Ruiz, Robin Callender Smith, Prof. Peter Sommer, Damian Tambini, Dr. Michael Veale

Drafted with the assistance of

Ravi Naik

22 May, 2020

Contents

0. Executive Summary

We welcome the JCHR aim of providing certainty and comprehensive protection for individuals' rights, in light of the upcoming deployment of the NHSX Contact Tracing system.

Clarifying the available safeguards would allow the public to better understand the functioning of the NHSX application, the consequences for their rights, and the remedies at their disposal. Further, as emergency situations may require rapid and bold responses, and protections of rights enshrined in law should be strengthened accordingly: in turn, public scrutiny and enforcement of rights would be enabled to keep pace with such rapid developments.

Likewise, we reject Matt Hancock's communication to the JCHR that a Bill is unnecessary as sufficient safeguards are present in Data Protection legislation and other general policy commitments[1] ; they are not. Data protection regulations leave a scope for differing protections and approaches, as they are not tailored to the situation at hand. On the other hand, public confidence would benefit greatly from a more specific approach which ensures particularly high protections.

Having said that, we are concerned about a number of issues raised in the current text of the draft Digital Contact Tracing (Data Protection) Bill.[2] We have divided those concerns into three groups:

- **Missed Opportunities:** we believe the Bill overlooks certain risks, whose potential for undermining public trust is significantly high;
- **Overlaps and Coordination with the GDPR:** we find that some provisions enshrined in this Bill are at risk of overlapping, conflicting or not properly coordinating with the current data protection regime;
- **Other Areas for Improvements:** finally, we cover certain aspects of the Bill which could be improved upon, in order to better attain the purposes of this Bill.

Each of these groups entails a number of issues, each (i) introducing the clause or clauses being discussed, (ii) briefly analysing the issues being raised, and (iii) recommending suitable changes to the Bill.

With this, we hope to contribute to ensuring that the Joint Committee on Human Rights Bill can really provide citizens with choice, control and confidence over the Government use of their personal data.

Please note that these concerns and considerations are not exhaustive. We would thus welcome the opportunity to discuss these concerns with the JCHR with a view to furthering and enhancing their work on technological responses to COVID-19.

1 Letter from Rt Hon Matt Hancock MP regarding legislation for contact tracing for Covid-19. Source: https://committees.parliament.uk/publications/1223/documents/10345/default/
2 Digital Contact Tracing (Data Protection) Bill. Source: https://committees.parliament.uk/publications/1026/documents/8461/default/

1. Missed Opportunities

1.1 Legislative protection against possible discrimination

It has been suggested that installation and use of the NHSX app is voluntary.[3] However, there are factors beyond the NHSX or public health policy reach where the voluntary nature of the app may be jeopardised. For instance, employers may force employees to use the app, or businesses could require it as a condition to access certain places or services (such as use of public services or transport).

Furthermore, without sufficient safeguarding, these incidents are likely to arise, be reported in the news and travel anecdotally. This would carry the potential of weakening public confidence: in turn, this would affect users' uptake of the NHSX app, undermining its effectiveness in countering the spreading of the virus.

Recommendations

- The use or installation of NHSX app should never be a basis to (i) enter or refuse to enter into an employment contract, (ii) for the employer to take any adverse action against an employee, and (iii) for a business or commercial activity to allow or restrict access to, or freedom of movement within, a given place;
- There are several model clauses that either have passed or have been proposed, which may constitute a valid reference with this regard:
    - ① Section 94H of the now-passed Australian "Privacy Amendment (Public Health Contact Information) Bill 2020"[4];
    - ① Section 3 of the proposed Coronavirus (Safeguards) Bill drafted for UK law.[5]

Proposed amendments

To move the following Clause —

"**No mandatory requirement to or sanction relating to installation or display of contact tracing applications**

(1) No person shall

(a) suffer, or be threatened with, criminal or civil sanctions or be subject to detention

(b) be denied, or be threatened with denial of, any public, contractual, employment or human rights, immigration status, benefits, immunities, opportunities, credits, or access to any place otherwise accessible to the public or to which they have a right to enter, or

(c) suffer discrimination under the Equality Act 2010

because they

(i) refuse or fail to install a contract tracing app on a personal device

(ii) refuse or fail to display to any person messages sent to, or statuses disclosed by, such an app or

(iii) disable, delete or remove an app installed on their phone

unless an exception is laid down in Regulations by the Secretary of State.

3 For instance, see BBC News. Source: https://www.bbc.com/news/technology-52532435

4 Privacy Amendment (Public Health Contact Information) Bill 2020, https://www.legislation.gov.au/Details/C2020A00044

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

(2) No person shall

(a) suffer, or be threatened with, criminal or civil sanctions or detention

(b) be denied, or be threatened with denial of, any public, contractual, employment or human rights, immigration status, benefits, immunities, opportunities, credits, or access to any place otherwise accessible to the public or to which they have a right to enter,

solely because they

(i) do not own a personal device compatible with a contact tracing app;

(ii) fail to ensure at any time that their personal device is on their person or in a vehicle in which they are travelling, turned on, is in working order, has signal, has any protocol, such as Bluetooth, enabled, or is fully or partially charged

(3) Negligently or innocently providing false or partial data to a symptom tracking or contact tracing app shall not constitute an offence under the Malicious Communications Act 1988 s 1(a)(iii).

(4) A parent or guardian shall be entitled to install a symptom tracking app or contact tracing app to the personal device of their child under 16, subject to paragraphs (5) and (6) below

(5) A child shall have the right to veto such a choice or delete the app, if they are of sufficient age and maturity to understand the consequences of these actions

(6) Maturity in paragraph (4) shall be rebuttably presumed at age 13.

(7) For the purposes of this section

A "contact tracing app" is a computer program which can be installed on a user's personal device, including computer code that is installed within the operating system of the personal device of the user, and which —

(a) determines by a procedure to be designated in regulations by the Secretary of State that a contact incident has occurred

(b) takes consequent steps, such as reporting this contact incident to a public health authority or other public authority, whether straightaway or when a certain number of contact incidents has accumulated, or providing guidance or instructions to the holder of the personal device or their household

A "contact incident" occurs where a potentially infected person has come within 2 metres for 15 minutes or more of another living person (the "contact"), or what other definition is laid down from time to time by the Secretary of State"

1.2 New transparency requirements

Public trust will in turn be crucial to the ultimate success of the app, as without sufficient uptake the utility is undermined. To this same end, we suggest increased transparency beyond the requirements of the DPA / GDPR.

Recommendations

The Bill should introduce requirements for NHSX to publish:

1. All Data Protection Impact Assessments, Equality Impact Assessments, and other human rights analysis;
2. All data sharing arrangements, whether with private companies or other public authorities;
3. Clarification of who the relevant data controllers are, and all joint controller agreements / agreements with data controllers and processors;
4. Clearly available terms of use, with comprehensible language and easy opt ins and outs for users;
5. The purposes of the application should be made clear and limited to the purposes that are necessary for the functioning of the application. Guidance should be provided to ensure that processing is limited to those purposes and in order to avoid "mission creep".

1.3 Enforcement

The Joint Human Rights Committee has previously noted how enforcement is key to ensuring protection for individuals' rights.[6] We therefore encourage (i) the Bill to extend mechanisms for enforcement and (ii) a reconsideration of the role of the proposed "Commissioner".

1.3.1 Review role of the Commissioner and oversight mechanisms

The Bill provides for

- the establishment of a new Commissioner, with equal "powers and proceedings"[7] of the ICO, and the power to review, inspect, and handle complaints in relation to, the Contact Tracing App (§5);
- periodic security assessments to be carried out by National Cyber Security Centre (§10);
- a review, to be conducted periodically by the Secretary of State (§13);
- the publication of the minutes of and reports of the Contact Tracing Ethics Advisory Board (§14[1]c).

Appointing a Commissioner with overlapping and potentially conflicting jurisdiction would be ripe to under-resourcing and regulatory arbitrage and confusion.

Further, the ICO is already equipped with the necessary personnel and expertise to audit data processing activities (both by government bodies and private entities), while a new Commissioner would have to build such capacity from scratch. On the other hand, we understand that the ICO has apparently stood down its audit work, and reduced its regulatory oversight efforts over the course of the pandemic.[8] This comes in conjunction with a general stay of proceedings before the Information

6 JCHR, Right to Privacy and the Digital Revolution, paragraph 101 p. 30-31

7 The Bill provides the "provisions of the Data Protection Act 2018 about the powers and proceedings of the Information Commissioner apply (with any necessary modifications) to the Commissioner."

Tribunal, the forum for data protection complaints[9] Thus, priority should be to compel existing oversight mechanisms to stand up to their role.

Finally, the scope of the other oversight mechanisms in the Bill could be further clarified. For instance, it is not right that NCSC should be the body reviewing the security of the system given that they designed it. Also, there is no obligation to follow the recommendations made in any review, nor for the recommendations to be made public once they are dealt with. Further, it is not clear how this assessment, as well as the Ethics and Advisory Board report, would interact with the review which is carried out by the Secretary of State.

Recommendations

- The Bill should not duplicate, remove or restrict ICO's supervisory role of data protection compliance in the field of contact tracing;
- Rather, the Bill could compel the ICO to review, approve and publicise DPIAs and other data-protection related-documents, as well as to release a Code of Practice under s.128 DPA 2018 for processing relating to the response to COVID-19, whether relating to contact tracing, health data sharing and beyond;
- There should be a reconsideration of the proposed Commissioner, including its procedures, and remit to ensure that it is fit for purpose and meets the aims of the Bill;
- Security reviews should be conducted by an independent body, whose role, along with that of the Ethics and Advisory Board should be clarified, in particular to ensure that their recommendations are made public, and that their consideration and follow up by the Secretary of State and NHSX app can be publicly scrutinised.

1.3.2 Collective redress

The Bill should provide for stronger enforcement mechanisms. In particular, the Bill should introduce "representative actions" under s189 DPA 2018 (Article 80.2 GDPR), and allow organisations to bring actions concerning potential breaches of the data protection regime without the need for an individual data subject. Such a mechanism would allow for close and continued scrutiny of the deployment of the application. .

In the absence of such collective redress systems, individuals may be prevented from seeking remedies or regulatory enforcement on their own, as:

- the complexity of the contact tracing system and its functioning, as well as of the different roles played by a number of private and public bodies make the factual situation complex;
- the nature of the contact tracing data (health data, intimate encounters), which could potentially expose private aspects of one's own life;
- the circumstance of certain individuals being part of a vulnerable group.

8 See The ICO's regulatory approach during the coronavirus public health emergency, point 4 p. 4. Source: https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf
Also, see Wired, *It looks like the UK's data regulator has given up, blaming coronavirus*. Source: https://www.wired.co.uk/article/ico-data-protection-coronavirus

9 The Information Tribunal is currently closed. See: https://www.judiciary.uk/wp-content/uploads/2020/04/01-Apr-20_SPT_GRCinfo-rights-Directions-for-a-General-Stay.pdf
And its extension: https://www.judiciary.uk/wp-content/uploads/2020/05/Stay-of-270420.pdf

Further, there may be gaps in regulatory oversight, and the ability of the numerous supervisory bodies being involved in contact tracing to effectively cooperate and coordinate their efforts is yet to be tested. Therefore, representative actions could act as a line of defence against regulatory breaches, and make sure that Supervisory Authorities do not overlook or fail to take action against infringements.

Finally, legal aid and cost capping orders should be extended to challenges to ensure legal actions are not curtailed due to resource restrictions.

Recommendations

- The Bill should provide for a representative action system, following the requirements of Article 80(2) GDPR;
- Such measures should be supported by the extension of the following regulations:
    - ① Schedule 1 of the Legal Aid and Sentencing of Offenders Act 2012 should be extended to ensure legal aid is available under the Bill.
    - ① Cost capping orders under the Criminal Justice and Courts Act 2015 should be extended to the Bill, to ensure extended coverage of such CCOs including representative actions against private actors.
- A committee of regulators that would allow for joint investigations between regulators in the model of the Regulatory Reform (Collaboration etc between Ombudsman) Order 2007. This committee should also act as a forum to encourage the sharing of best practice between regulators and support horizon scanning activity.

Proposed amendments

After section 7 (2) - insert

Section 7 (3)

In relation to the processing of personal data to which this Act applies a not-for-profit body, organisation or association organisation which meets the conditions set out below at (4) and (5), may, independently of a data subject's authorisation, exercise the rights of a data subject under the independent complaints system established by the Commissioner if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing.

(4) The first condition is that the body or organisation, by virtue of its constitution or an enactment -
    (a) is required (after payment of outgoings) to apply the whole of its income and any capital it expends for charitable or public purposes,
    (b) is prohibited from directly or indirectly distributing amongst its members any part of its assets (otherwise than for charitable or public purposes), and
    (c) has objectives which are in the public interest.

(5) The second condition is that the body or organisation is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data.

To move the following clause

Schedule 1 of the Legal Aid and Sentencing of Offenders Act 2012 is extended to cover the provisions of this Bill

2. Overlaps and Coordination with the GDPR

2.1 Consent

The Bill mandates users' consent in order to collect contact tracing data (§11), as well as to share them outside of the users' device (§12[5]b).

However, the NHSX Tracing App entails a number of processing activities beyond collection and sharing of data, such as recording proximity events, uploading data to the centralised database, and sharing anonymised data for research purposes.

Furthermore, the NHSX DPIA suggests that the lawful bases will be wider than consent including, for instance, processing on public health grounds.

The Bill introduces an unparticularised definition of consent for collection and sharing of data. This will in turn deprive individuals of the protection given by GDPR definition of consent (i.e. to be freely given, specific, informed, and the result of an unambiguous indication) and further conditions in Article 7 GDPR (e.g. to be able to withdraw consent as easily as it was given). These safeguarding conditions in Article 7 GDPR are designed to prevent common malpractices (e.g., forcing users into bundled consent, or spreading key information into different documents), which have been recognised as problematic by the JCHR.[10] We encourage the Bill to use the GDPR requirements of consent.

Recommendations

- The Bill should clearly state that "consent" operates pursuant to Article 4(11) and clarified by Article 7 of the GDPR;
- When asking for users' consent, the GDPR standards in Articles 4 and 7 GDPR should apply regardless of the legal basis upon which data is being processed;
- The Bill should ensure that individuals can withdraw consent and choose whether to allow the processing of their data for research purposes.

2.2 De-identified data

The Bill introduces an offence of "knowingly or recklessly to re-identify de-identified digital contact tracing data" in section 9(5). Such "de-identified" data is defined at section 9(6)a). Re-identification is defined as the act of taking "steps which result in the information no longer being de-identified" (section 9(6)(b)).

Section 171 DPA 2018 however already contains the following offence:

> *It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.*

The offence in the Bill therefore replicates the offence in §171 DPA 2018: we do not see the need for the repetition of the offence, particularly where it will lead to an overlap with the powers of the ICO.

10 JCHR, Right to Privacy and the Digital Revolution, paragraph 22 pp. 11-12

Further, the new offence in the Bill does not contain the safeguards within §171 DPA 2018 such as appropriate defences being made available.

In any event, there is a larger concern that NHSX may be overly relying on the data being anonymous when in fact it may be pseudonymous.[11] The Bill should address this concern.

Recommendations

- The offence should be removed;
- The Bill, whenever needed, should emphasise that contact tracing data will be pseudonymous, rather than anonymous, within the meaning of Article 4(5) of the GDPR;

Proposed amendments

Move that section 9(5) is removed.

Move that section 9(6)(a)-(b) is removed.

2.3 Processing of digital contact tracing data

The Bill provides at §9(1) for an offence "for a person who is not an authorised person to collect or process digital contact tracing data." Again, this is very similar to the offence in §170 DPA 2018. We do not see the need for the repetition of the offence, particularly where none of the safeguards in the DPA are provided.

Further, §9(3) provides for an offence that "authorised person may not collect or process digital contact tracing data other than for a permitted contact tracing purpose." It is not clear what a "permitted contact tracing purpose" is nor how that will be regulated. We suggest that the purpose limitation principle in Article 5(1)(b) GDPR already contains clear requirements on purpose limitation. Rather than enforce this through ill-defined offences, we suggest that regulatory action and capacity for civil society actions would act as a better deterrence.

Proposed amendments

Move that sections 9(1) - (3) are removed.

2.4 Data Subjects Rights

The Bill provides for specific arrangements for the deletion of contact tracing data, within the meaning of §12(1), so as to "ensure that digital contact tracing data is deleted where a data subject so requests (§12[5]e)".

Although the GDPR is already providing for this as well as other individual rights over one's own personal data right, the DPIA reveals the NHSX may avoid their application without a legitimate ground.

11 See Covid-19 & Tech responses: Legal opinion, paragraph 26 p. 12 . Source: https://www.awo.agency/covid-19-legal-opinion.pdf

Namely:

- The Contact Tracing App allows data to be uploaded and linked in the centralised database, but NHSX claims the need to assess the technical feasibility of establishing the same link when it comes to allow users access and deletion of their data in the central database.[12]
- Also, the DPIA claims that the processing of contact tracing data does not involve users' profiling, and is not at risk of significantly affecting individuals. However, it is the nature of contact tracing to profile and evaluate the level of risks resulting from our daily encounters, and the consequences of such evaluations may result in individuals' limitation of their freedoms either directly (e.g. as self-isolation or quarantine) or indirectly (e.g. lockdown due to public health response based on contact tracing data).

Therefore, there is a case to bolster users' exercise of rights to erasure, but also other data subjects rights, such as the right to access and to rectify personal data, the right to restriction of processing, the right to object, and the right not to be subject to a decision based solely on automated processing, including profiling.

Recommendations

- The Bill should bolster the rights of data subjects under Chapter III GDPR to ensure that users are on request able to access, rectify and delete the data associated with them and their device. We suggest that the Bill demand such erasure should be available on device;
- The Bill should clarify the circumstances users may ask for the restriction of processing, object to it, and how he or she would be allowed to contest a decision taken solely on the basis of contact tracing profiling;
- The Bill should bolster rights within the meaning of Articles 15 to 22 of the GDPR, such as by removing the need for "legal effects concerning him or her or similarly significantly affects him or her" in Article 22 GDPR, removing the qualifying criteria for the right to erasure in Article 17 GDPR, shortening the timeframe to respond to a SAR in Article 12(3) GDPR to 7 days etc.

12 "*The technical practicality of this needs to be assessed*". Source: DPIA NHS COVID-19 App PILOT LIVE RELEASE Isle of Wight, p.26

3. Other Areas for Improvement

3.1 Stricter purpose limitation

The Bill restricts the purposes for the processing of contact tracing data to "protecting the health of individuals who are or may become infected with Coronavirus"(§2a) and to "preventing or controlling the spread of Coronavirus" (§2b).

While we fully agree with the decision of enshrining the purposes of processing in law, we also believe that their wording could be improved, to reduce discretionary powers and cut off interpretative loopholes. To this end, the NHSX DPIA already identifies the purposes of the Contact Tracing App as: i) logging proximity encounters for COVID-19 self- diagnosis, (ii) to alert users who have come in contact with other users reporting symptoms, (iii) public health planning in the context of the COVID-19 public health emergency, and (iv) research (in the same context). It is surprising that the JCHR Bill has provided substantially wider purposes for NHSX than NHSX have themselves identified, which undermines the utility of such statutory purpose limitations.

The NHSX position could be a good starting point, as it would reassure the public against "mission creep", or an overly extended use of their data. However, enshrining these purposes into primary legislation would prevent NHSX from radically modifying these purposes over time, while leaving an acceptable degree of flexibility.

Stricter statutory purpose limitation would further act as a safety net against loose contractual arrangements or conflict of interpretation between the Government and its private partners, whose role in the development and operation of the system has been highlighted by the NHS.[13]

Recommendations

- The Bill should list more in details the admitted purposes of the processing, to avoid any public or private body to repurpose these data within the limits permitted by the GDPR;
- Such purposes could include contact tracing, users alerts, as well as public health planning and research in order to prevent or control the spread of Coronavirus.

3.2 Additional safeguards for the appointment of authorised persons

The Bill restricts the collection and processing of contact tracing data by authorised entities or personnel (§9[1]), whose appointment is made by the Secretary of State under regulations (§9[2]b).

The Bill should also state the criteria to be followed by the Secretary of State in appointing such entities or personnel. To this end, note that the Australian draft legislation expressly provides for collection and use of personal data to be permitted to persons which are either officers, employees, contractors or in service of a health authority involved in the processing of contact tracing data.

Recommendations

- The Bill should provide the criteria which a subject needs to meet in order to be authorised to the collection and use of contact tracing data;

13 See for instance UK Gov Healthtech Blog, Source: https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

- Section 94(2)D of the Australian "Privacy Amendment (Public Health Contact Information) Bill 2020" may constitute a valid reference with this regard;

3.3 Additional safeguards for data anonymisation

The Bill obliges the digital contract tracing system to comply with approved arrangements for the deletion of contact tracing data (§12[1]). These arrangements include "that any digital contact tracing data held by an authorised person is anonymised as soon as is practicable after it is obtained" (§12[5]c), and that it is "deleted or anonymised as soon as it is no longer required for a permitted contact tracing purpose" (§12[5]d).

The burden is the wrong way round in the Bill. Data should be provided in anonymous form unless necessary to be provided without anonymity.

Further, the current wording of this clause allows for data to be anonymised only after its purpose has been exhausted. In turn, commercial uses or other kinds of repurposing may occur. This is a real risk, as data de-anonymization and repurposing is the field of expertise of some of the companies which are going to handle contact tracing data (e.g. Palantir).[14]

Proposed amendments

To move the following clause

(1) Personal data collected by or processed must be deleted or anonymised as soon as the purpose of its processing is completed, or at latest after the end of the emergency period, by the data controller (s) or any other persons then processing it, whichever is sooner, or;
(2) at the latest at the end of 28 days [or what period recommend as strictly necessary by public health authorities];
(3) The Secretary of State shall indicate in a Code of Practice, after consultation with security and privacy experts, what steps, technical and organisational, must be taken to stringently anonymise personal data;
(4) The Commissioner shall have the right to review before publication, and require amendments to, the Code.

28/05/2020

14 "*Palantir is working to pull NHS data into one of its two data platforms, Gotham and Foundry. There it can be cleaned and merged with other datasets, enhancing the ability of NHS administrators and the government to run analyses quickly.*", The Economist. Source: https://www.economist.com/britain/2020/03/26/palantir-a-data-firm-loved-by-spooks-teams-up-with-britains-health-service
See also: https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information