COVID-19 and personal data: April briefing

Executive summary

The Government is running significant risks to trust and policy delivery by failing to communicate its approach to data and privacy. It has failed to explain a number of decisions, from the use of aggregated mobile data ***(3.2)*** to procuring services from Palantir, and failing to explain its coming approach to data hungry projects.

The use of personal data could be critical to lifting lockdown through 'contact tracing' and 'immunity passports' ***(1.1).*** These tasks can be done with privacy-friendly technologies, or invasive tools.

Privacy preserving technologies are more likely to succeed in maintaining the widest public trust and participation. 'Contact tracing' mobile apps will be challenging to deliver, requiring very high take-up and significant clinical effectiveness. Contact tracing apps will also need to work cross-border, allowing people from Ireland and Europe to travel to the UK and vice-versa, through use of the same technologies or using interoperable standards to allow data exchanges.

Immunity passports similarly could be delivered through invasive 'centralised databases', or through privacy-preserving technologies. ***(1.2)***

The government must provide clarity about its technology choices, collaboration with European projects and the Government's own needs for future contact tracing. It should ask what is intended relating to immunity passport technologies.

ICO Advice

The ICO needs to provide more specific advice on the use of (a) anonymous location data (b) identifiable location data. The ICO also needs to give general advice about how and when to collect health data by non-government actors. ***(2)***

The law

This document provides a general guide to the operation of data protection law. Protections in data protection law continue to exist even when consent is no longer required or emergency arrangements put in place. In particular: *lawfulness, fairness and transparency; purpose limitation; data minimisation; storage limitation; integrity and confidentiality* continue to be required. ***(3)***

1 Lifting the lockdown: contact tracing and immunity passports

1.1 Contact tracing

It is the general consensus that in lifting the lockdown, some form of technology for tracking the population is likely to be necessary. Many forms of technology have been proposed from geotracking wristbands in Hong Kong[1], to the assessment of effectiveness of home quarantine measures by tracking individuals through their phones, seen in Taiwan[2], to using state surveillance apparatus to track the population movements, as we see in Israel[3].

While the purpose of such initiatives are the same - slowing the spread of the virus - their methods will have drastically different impacts on fundamental rights, and the effectiveness in achieving the overall goal.

So far it is unclear what the UK Government's proposal will be. There have been unconfirmed rumours of a contact tracing application for smartphones[4] similar to that used in Singapore[5]. This system uses data from bluetooth, stored locally, to track the proximity between devices. When an individual tests positive for covid19, their local bluetooth data is uploaded and the other devices that have been in close proximity are informed. This was seen as a reason for the relatively low occurrences of the virus in Singapore[6], and contributed to the Government not instituting lockdown. Recently however, the Government have imposed a lockdown as necessary when individuals were coming down with the virus and the source could not be traced[7].

While the effectiveness is more disputed than previously, proximity tracing appears to be the strongest privacy-preserving model available. It is estimated that around 60% of the poulation need to use such an app for it to be effective. Around 80% of adults have a smartphone; so the vast majority of them will need to be persuaded to install it. This makes a privacy preserving approach very important, to gain the trust of people otherwise worried about using it.

Within this form of technology there are different set-ups that can protect or interfere with privacy. The Pan European Privacy Preserving Proximity Tracking Project[8] (PEPP-TP) is an example of a collaboration of various different institutions coming together to present a proximity tracking solution that retains privacy standards. However, within that group there are different theories available. For example, a centralised system that generates identifiers for individuals then used to construct contact graphs risks creating a system that could be easily repurposed (breaking the purpose limitation principle of data protection), whilst a decentralised model where more data is

---

[1]https://qz.com/1822215/hong-kong-uses-tracking-wristbands-for-coronavirus-quarantine/
[2]https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine/
[3]https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases
[4]https://news.sky.com/story/coronavirus-govt-set-to-release-contact-tracking-app-which-detects-nearby-virus-carriers-11966243
[5]https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether
[6]https://www.latimes.com/world-nation/story/2020-03-24/coronavirus-singapore-trace-together
[7]https://www.straitstimes.com/singapore/health/singapore-to-shut-workplaces-and-schools-to-curb-spike-in-virus-cases
[8]https://www.pepp-pt.org/

stored locally (on individual's devices) and not stored with a central entity ensures no sensitive data is transmitted.[9]

It is at this point unclear how the Government is working with PEPP-TP, although it seems very likely to need to ensure that UK contact tracing will work across borders.

PEPP-TP, and the decentralised protocol proposal point to areas we think the Committee should seek to explore, in particular the need for international cross-border collaboration while upholding strong standards of data privacy.

There are many roads for the UK Government to choose in lifting the lockdown and determining technology's role within that. A collaborative, privacy preserving model would be best for preserving the trust and confidence of the British public.

The Government should explain:

- What safeguards and scrutiny will be provided to safely allow for the "tracking" of individuals.
- What other data, combined with traffic or location data, may be necessary to effectively combat the spread of coronavirus.
- What conversations it has had with other governments on cross-border data initiatives to prevent the spread of coronavirus.
- How the Government are engaging with PEPP-TP.
- The Government's criteria for assessing the different technology approaches to contact tracing apps.
- If the Government is to adopt technology solutions for monitoring the spread of the virus after lifting the lock-down, and whether it will commit to the strongest strong privacy-preserving model to combat the spread of the virus.

1.2 Immunity Passports

Immunity passports have been mentioned as a possible technological means to help people can return to normal work. These could be produced in a privacy-friendly way, allowing just the attestation to be communicated. However, they could also be governed by a central database or register, much as the national ID card system was intended.

We do not know what the Government's thinking is at this stage, but swift procurement processes could easily result in the creation of an intrusive data system for no better reason than carelessness.

The Government should explain:

- What the procurement process and criteria are; whether companies and technologies have been identified, and what their approaches are.

---

[9] See the Decentralised Privacy-Preserving Proxmity Tracing: Simplified Overview, https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Simplified%20Three%20Page%20Brief.pdf

- What other forms of technology the Government are considering introducing as they prepare to lift the lockdown, and the legal and ethical implications of these.

2 The urgent need for guidance from the Information Commissioner's Office

So far the Information Commissioner's Office has provided a statement regarding the use of generalised location data trend analysis and its use in tackling the coronavirus crisis[10]. The statement correctly points out that providing this data is properly anonymised and aggregated data protection law does not apply.

However, it has so far failed to engage in the second basis for processing: consent from users and subscribers. It is important for the ICO to produce guidance on this for two reasons:

1. Anonymisation of location data is generally considered to be of great difficulty without severe degradation.
2. This traffic or location data may have to interact with other applications that are currently being developed, such as the reported UK Government contact tracking app[11], which may seek to take this data from anonymous to personal data.

These two factors should contribute to the ICO prioritising further guidance in this area.

Furthermore, there is a lack of guidance for companies, housing associations, landlords and others who may seek to use or collect health data during the crisis. Often they will have no need or power to do so, and should avoid doing so. The ICO should clarify who can legitimately ask for information, why and when; and who should not.

The Information Commissioner must provide clear advice on best practice for the use of the available legal bases for processing various types of data in the context of public health emergencies and identify whether there may be a need for further legislation in order to provide the safeguards required by GDPR.

The advice should include advice to affirm rights under Recital 54 of GDPR: processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

The ICO should state when it intends to provide advice to government and other parties about their use of data during this crisis.

3 The legal framework

3.1 UK DPA 2018

The UK DPA 2018 does not contain specific powers to deal with a public health emergency, for example waiving specific requirements, but contains general powers that should provide sufficient legality to the handling of data for public health purposes.

---

[10]https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/statement-in-response-to-the-use-of-mobile-phone-tracking-data-to-help-during-the-coronavirus-crisis/

[11]https://news.sky.com/story/coronavirus-govt-set-to-release-contact-tracking-app-which-detects-nearby-virus-carriers-11966243

The UK DPA 2018 compliments GDPR and provides some of the requirements for member state law to give a local setting and further detail to the powers found in GDPR.

Recital 54 of the GDPR sets out the scope of "public health":

> The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council.

It is important to note that the above only set the legal basis for the processing, but not all the details on how to do it. The above sections and schedules of the DPA 2018 do not set all the safeguards required in GDPR for the processing of data for maintaining public health. These safeguards are found elsewhere in health legislation and specific policies, but it is unclear whether these are detailed enough in relation to public health emergencies, particularly for innovative uses of big data and artificial intelligence or the use of data from internet companies or other third parties outside the health sector.

The processing of any data for a public health emergency may be lawful, but it has to comply with the general principles of data protection: fairness, accuracy, security, data minimisation, etc.

In order to preserve democratic values in this crisis the Government needs to maintain public trust and ensure the support of the population for the measures required. This means that the data protection principle of transparency is paramount.

The Government should

- Publish a detailed explanation of the uses of data under consideration to monitor the population or effect behavioural change.

3.2 E-Privacy: use of traffic and location data

When it comes to the use of traffic data held by telecommunication firms the E-Privacy Directive provides guidance.

The privacy and confidentiality of electronic communications are regulated through specific legislation that complements the General Data Protection Regulation: the E-Privacy Directive from 2002. This EU law is implemented in the UK under the Privacy of Electronic Communications Regulations (PECR). Mobile data including location is protected by these laws. Governments cannot access location data without specific legal instruments.

E-Privacy is stricter than GDPR on what companies can do with traffic data – including mobile phone and web usage – and location data. The general principle in the E-Privacy Directive is confidentiality of communications, where data required for providing a communications service should not be used freely. This data can provide intimate details about the user's life, as it will "contain information on the private life of natural persons and concern the right to respect for their correspondence".[12]

[12] para 26, E-Privacy Directive, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058.

Traffic data is the by-product of providing a communications service, including data that can tell who communicates with whom, for how long and when. The law is clear that without consent traffic data should be deleted or anonymised after a communication has taken place except to provide billing.

Location data gives information about the geographical position and time, including direction of travel, where a user or the equipment may be. All mobile phones generate location data when they connect to phone masts in order to work. Location data is more heavily regulated than traffic data because it can reveal a lot about an individual's habits. There is more risk of identifying someone, particularly when combined with any other information. Location data can only be processed either with consent for value-added services, or when anonymised.

Sometimes traffic data may also be location data. For example, phone mast data, also known as cell tower ID, could be traffic data when the mast is used for a call or text, as it is required for the delivery of the communications service. But phones are constantly communicating with masts when in stand-by. In this case, it is more likely that the dataset that registers which phone masts a mobile has been linked to at different times of the day would not be considered traffic data but location data.

In principle, if telecoms want to share location data with governments to help fight the epidemic, they should anonymise it or get consent from their users. Anonymisation of location data is very hard, and some would argue impossible without severe degradation.[13]

Article 15 of the E-Privacy Directive contains provisions for governments to legislate to create restrictions on the above framework for reasons of public security. These powers were used to create indiscriminate data retention laws, although many of these have been found disproportionate and unlawful.

Mobile companies cannot share location data without a legal basis. This point has been made clearly by the European Data Protection Board:[14]

> "When it is not possible to only process anonymous (location) data, the ePrivacy 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."
>
> "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)."

---

[13] https://www.nature.com/articles/srep01376?

[14] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf