Written evidence from Open Rights Group, Big Brother Watch, Privacy International, Deighton Pierce Glyn (COV0221)

Our organisations each work on surveillance and privacy issues. Open Rights Group, Privacy International and Big Brother Watch worked together on the Don't Spy on Us campaign, which looked in detail at the powers now embedded in the Investigatory Powers Act. Deighton Pierce Glynn have acted as our solicitors in key cases about surveillance law at different points including at the CJEU and ECHR.

During the COVID-19 pandemic, we have been concerned about the potential use and abuse of these powers, which are wide ranging and secretive. Near the start of the crisis, we wrote to the Secretaries of State for the Home Department, Foreign & Commonwealth Affairs and Health for clarification of how these powers may be used, copying in the Investigatory Powers Commissioners Office. However, the Government Legal Department declined to say anything substantial and the Investigatory Powers Commissioner's Office is not obliged to make any particular statement about how powers may be used. Through the period it has of course been concerning that Parliamentary oversight has been absent, due to the lack of a working Intelligence and Security Committee.

In this note, our concerns focus on the potential for the sweeping powers Government has obtained to be abused. Because of the lack of any public statement, we are necessarily speculating about how capabilities may be used, rather than stating that they are being used in such a way. Our first concern therefore is for Parliament to ensure that the Government declare how or whether powers are being used.

This crisis shows the potential for these sweeping powers and capabilities to be misappropriated. Privacy International has documented the use of such powers internationally, in many cases deeply inappropriately.[i] It begs the question whether bulk powers in particular are appropriate: the ability for these to be redeployed has the potential to erode trust between citizen and state, once it is understood how much information the state can easily acquire about in order to define how it treats a citizen.

Joint Biosecurity Centre

The approach employed by the Joint Biosecurity Centre claims to be very similar to a counter terrorism model.[ii] It is headed by Tom Hurd, who comes from a security background.[iii] This raises the obvious question as to whether use of national security powers or capabilities are used, including at the very broad level of analysing trends in the spread of infection, sentiments, population movements or quarantine arrangements. It would be very helpful for Government to rule out the use of surveillance powers regarding the Joint Biosecurity Centre.

GCHQ

The COVID pandemic is a national emergency. GCHQ and its internal UK equivalents have enormous capabilities to capture and analyse data as a result.

Potential uses of their capabilities could include:

Contact tracing: some other countries, such as Israel, did indeed deploy surveillance capabilities for contact tracing. The acquisition of bulk communications data done by GCHQ would provide a route for contact tracing to be conducted. It would be useful for the Government to rule out the use of mass surveillance capabilities to be used in this way.

Population location data: Similarly, bulk data could be used to monitor population movements, similar to the data provided by mobile telcos to government. It could even be used to verify the accuracy of results provided this way.

There have been multiple media reports of government discussions with telecommunications companies regarding the use of mobile phone data to monitor the public's compliance with lockdown restrictions, including reports of Downing Street and Cabinet Office meetings with BT and EE in March.[iv]

Some companies have provided limited information about talks through public statements. A spokesman for BT said the company was in talks with the government to "assist with the national public health effort", including "actively exploring possibilities" in relation to the use of mobile data. BT owns EE, which is one of the largest UK mobile operators.

An O2 spokesperson said the company was "fully engaged in helping in the fight against Covid-19" and that it has "the potential to build models that help to predict broadly how the virus might move" without identifying individuals.[v] The ICO was reported to have approved the notion of nationwide mobile phone monitoring.[vi] However, no surveillance measures have been expressly avowed by the government and no further details have been provided by it, nor the ICO, the Investigatory Powers Commissioner's Office (IPCO) or the Intelligence & Security Committee (which had not been constituted).

One of our concerns is that the draconian Investigatory Powers Act 2016 could be used in the pandemic context. It is possible that sweeping powers could be used to collect and analyse bulk datasets under Part 7 powers, or potentially even to access and track identifiable location data of individuals in the UK with the virus or subject to isolation restrictions under Part 3, s.60A(7). However, on our analysis the use of secret surveillance powers to track individuals in this context could never be necessary or proportionate. This would be inappropriate and a further shift from any sense that data is used in a limited and targeted way for the detection of crime, so should be ruled out.

Population sentiment: It is known that it is possible to monitor communications traffic to spot 'sentiment', by GCHQ as well, and hostile actors have been known to intervene to shape opinion, much in the way that hostile actors are believed to do. In some scenarios, if public opinion was shifting in a way that was dangerous for the Government's handling of the pandemic, use of these capabilities might be considered. Such tools, especially when based on mass interception of data, are well beyond what ought to be considered appropriate in a democratic society, so should be ruled out.

Enforcing quarantines: The bulk data collected by security agencies could be deployed to understand whether quarantines, including by individuals or in local lockdowns, are being observed. This would be entirely inappropriate and should be ruled out.

Unanswered questions

In our letter to the government, we made the case that much greater transparency around the use of surveillance powers is possible in the context of a public health emergency than when tackling serious crime and terrorism. The nature of the threat, and the need for large scale public policy measures to combat it are widely acknowledged. The efficacy of the use of surveillance powers is not undermined by public transparency in this context. There is no 'tipping-off' risk. However, the government still declines to comment[vii]. Some of the questions we believe should be answered are as follows:

1. Whether any Surveillance Measures include the processing of communications data of the public in general or large sections thereof (whether anonymised or not). If so, whether such data is anonymised. If limited to sections of the public, what these are or what thematic basis is relied upon to identify them.

2. Whether any Surveillance Measures include the use of location data relating to the use of personal electronic devices by the public in general or large sections of the public, and whether that location data is at the level of phone mast location data or GPS coordinates.

3. Whether any Surveillance Measures include the processing of real-time or near contemporaneous (i.e. within the last 24 hours) communications data.

4. What safeguards will ensure the security of any data processed pursuant to any Surveillance Measures.
5. What limitations are applied to the people and government bodies and departments having access to data processed pursuant to any Surveillance Measures and any onward use or sharing of the data either within the United Kingdom, to external contractors or to other States.

6. What limitations have been placed on the length of time which any data relating to any Surveillance Measures may be retained.

7. What statutory powers have been used to obtain data; whether new warrants have been necessary, or the government has been able to rely on existing warrants.

8. Whether the government's work in relation to the pandemic is a specified Operational Purpose for the purpose of bulk warrants (as defined in s142 IPA).

22/07/2020

---

[i]https://privacyinternational.org/examples/tracking-global-response-covid-19

[ii] https://www.instituteforgovernment.org.uk/explainers/joint-biosecurity-centre

[iii]https://www.theguardian.com/world/2020/may/12/former-counter-terror-official-tom-hurd-put-in-charge-new-uk-biosecurity-centre-coronavirus

[iv]Phone location data could be used to help UK coronavirus effort – Mark Sweney and Alex Hern, the Guardian, 19th March 2020: https://www.theguardian.com/world/2020/mar/19/plan-phone-location-data-assist-uk-coronavirus-effort

[v]Ibid.

[vi]Watchdog approves use of UK phone data to help fight coronavirus – Mark Sweney, the Guardian, 27th March 2020: https://www.theguardian.com/world/2020/mar/27/watchdog-approves-use-uk-phone-data-if-helps-fight-coronavirus

[vii]https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2020-06-16/HL5807/