EXTRACTION OF INFORMATION FROM ELECTRONIC DEVICES: DRAFT CODE OF PRACTICE

CONSULTATION RESPONSE

July 2022

Open Rights Group is a digital rights campaigning organisation fighting to protect digital rights, including robust data protection. We have over 20,000 engaged supporters across the United Kingdom and engage with groups across civil society including those advocating for migrants rights, to combat violence against women and girls and against the over-policing of communities among other missions. We advocate evidence-based policy, guided by respect for fundamental human rights.

We welcome the opportunity to respond to a draft code of practice for the extraction of information from electronic devices under the Policing, Crime and Sentencing Act 2022, open for responses until 19 July 2022, found online here.

Our response

Part 1 - Introduction

Q1 (a) To what extent do you agree or disagree with the guidance the code of practice provides on the circumstances in which the powers can be used and the requirements that must be met for section 37?

- Disagree

Section 37 states that an authorised person can extract information from an electronic device to investigate a crime etc, if the device has been voluntarily provided and if the user has agreed for the extraction to take place. The section also details that it must be in pursuit of a crime and where there is a reasonable belief that the information on the device is relevant to a reasonable line of inquiry. And that the power to be exercised is relevant and proportionate.

The code states that "there is no barrier to a suspect or person of interest handing over their device and agreeing to the extraction of information from it." This statement is factually wrong and fails to take into account the interaction between the PCSC and the right to silence, or the right against self-incrimination. The code of practice should

consider the specific circumstances that arise from using these powers afforded by Section 37 against suspects, or in the event where volunteering one's device for extraction would be at risk of self-incrimination.

For instance, we'd like to draw attention to the problems around voluntary provision and agreement, in particular, and in relation to instances of "stop and search."

Research has shown that in the past, stop and search was conducted under spurious grounds and those being subjected to the powers are sometimes asked to hand over their mobile phone although it is not clear which powers allows for this to take place.

It therefore raises the concern that s.37 powers could be invoked in instances of stop and search and that problems around "voluntary" and "agreed" provision of devices for the extraction of their data will emerge. Informed consent to device extraction is contentious as those being asked to supply their devices should be aware of their rights and the implications, which is not always the case. There is a power imbalance play between a police official and a member of the public, heightened when that person could be considered "suspect." This is of increasing importance as we note that stop and search could expand due to provisions under the new bill as a result of Serious Violence Reduction Orders.

Informed consent also becomes of relevance due to the introduction of immigration officers as authorised persons receiving extraction powers. We note a track record by the Home Office for seizing and extracting data from mobile phones considered unlawful and think the code should address language barriers and forms of duress; one way would be to ensure an interpreter is present.

Part 2 of the code provides an overview of how the new powers interact with the data protection regimes of the Data Protection Act and the UK General Data Protection Regulation (UK GDPR), and human rights legislation.

Q2. (a) To what extent do you agree or disagree with the guidance that the code of practice provides on the exercise of the powers in accordance with data protection and human rights legislation for section 37?

- Strongly disagree

The bill and code come at a time when the government has announced a raft of legislative changes, including to the Human Rights Act and the Data Protection Act 2018, which are cited as key safeguards and considerations of the PSCS bill and the

Code of Practice for extraction powers. Therefore, these safeguards do not exist in their current form, taking into account the new Data Reform Bill and Bill of Rights.

We note that data reforms will empower police officials by liberalising the invocation of the public interest argument when handling personal data and conducting their balancing act of right to privacy with right to fair trial.

The code also makes no mention of how and when a data protection impact assessment (DPIA) or Equality Impact Assessment (EIA) will be made.

Article 35(1) of the DPA 2018 states a DPIA must be conducted where a type of processing is likely to result in a high risk to the rights and freedoms of individuals:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

An EIA should also be carried out when the need for a new policy or practice is identified, or when an existing one is reviewed. This should be internal not just high-level.

The code should iterate the necessity for each force to carry out a DPIA and EIA in relation to extraction powers.

Evidence shows that technology can replicate existing discrimination and there is currently a disproportionate number of searches of Black people in England and Wales, which a police watchdog found to be unfair and discriminatory.

That discrimination has also been found to exist when immigration officers make stops.

There are also risks in processing people's data after extraction and in the past police forces have failed to encrypt people's data after extraction and there has also been loss of people's sensitive files.

Finally, s.54 of the Code of Practice state that, in order to minimise the risk of obtaining other information, the person conducting the extraction "should include use of appropriate technologies to support selective extraction and use of targeted key words, date ranges or other specifics to identify necessary information." While we do agree in principle with these guidelines, we ought to emphasise their lack of detail and

vagueness: in particular, this section should develop in detail technical and procedural safeguards with the aim of defining, before the extraction takes place:

- What information will we searched for;
- What criteria will be adopted to refine this search (such as with the use of targeted key words, date ranges or other specifics) in relation to each specific piece of information that the extraction is meant to provide;
- What criteria will be used to define if the information being collected is relevant, and what procedure will be in place to delete the information that does not meet this threshold;
- How the extraction will be conducted in practice, whether the proposed procedure is compatible with the aims being pursued and whether its adherence to these aims have been reviewed by a Data Protection Officer.

Part 3 of the code provides information on when and for what purposes the section 37 and 41 powers can be used, and guidance on reasonable belief, necessity, and proportionality requirements.

Q3. (a) To what extent do you agree or disagree with the guidance offered in the code on assessing necessity, proportionality, relevance to reasonable line of enquiry or reasonable belief when determining when the powers in sections 37 and 41 should be used for section 37?

The current guidance is too broad to ensure a considered assessment of necessity, proportionality and relevance to a reasonable line of enquiry or reasonable belief when determining when s.37 extraction powers can be used.

There should be time limits on examination, retention and deletion of data and provision for its secure storage while needed.

Part 4 of the code provides guidance on the criteria that must be met for a person to be treated as having voluntarily provided a device and agreed to the extraction of information from it.

Q4. To what extent do you agree or disagree with the guidance the code of practice provides on how authorities meet the requirements stated in section 37(1) in the Act, to ensure a person has voluntarily provided their device and agreed to the extraction of

information from it?

The code notes that there is a power imbalance, particularly, in relation to victims of sexual abuse and domestic violence but it does not acknowledge other forms of power relations, that can be palpable under stop and search, at the border or when individuals are undergoing an asylum claim.

Mere acknowledgment and agreement cannot be consent. Informed consent must involve full communication of the process. It must also be clear what happens to data collected and whether it will be shared with any other bodies, either directly or via inclusion on official systems and databases. For instance, §63 includes a list of information that should be provided to the individual agreeing to the phone extraction, but omits to consider how individuals should be informed of whether they are being required to hand over their phone as witnesses or suspects, and how their right of silence or right against self-incrimination may be affected by their decision.

Language barriers must be addressed including by provision of an interpreter.

Asylum claimants in particular may experience duress and feel they have no choice but to hand over their devices. It should also be noted that parting with their devices has a psychological impact including being unable to contact family or friends and can contribute to the traumatising effect of fleeing difficult circumstances. Therefore, clear time limits on voluntary seizures should be communicated.

Part 5 of the code provides guidance on what authorised persons should consider when using the section 37 power with persons who may be vulnerable due to the trauma they have experienced, and who may need more support to make an informed decision as to whether they volunteer their device and agree to the data extraction from it.

Q5. To what extent do you agree or disagree with the guidance that the code of practice provides on how to recognise when a person is vulnerable?

- Agree

There is a broad approach to identifying someone who is vulnerable, which is good as many factors may contribute to their vulnerability and while we appreciate an exhaustive list may not be possible, there are some common examples missing from the list, which could be a quick aid for officers. For example, the list would benefit from including migrants, refugees, asylum seekers and undocumented persons. While it is acknowledged that difficulty communicating may contribute to someone's

vulnerability, including language barriers, this may not be the case for the above mentioned group, yet they are inherently vulnerable due to their precarious circumstances and unfamiliarity with their rights or legal environment, for example.

In the case of undocumented migrants, it is important to note that undocumented migrant women experience an inherent vulnerability. As noted in a super-complaint launched by Liberty and the Southall Black Sisters, victims of crime with insecure immigration status are afraid to file reports due to data sharing arrangements with immigration enforcement. The complaint was rejected and a temporary pause of sharing conceded but this does not go far enough in erasing vulnerability.

The guidance notes children are vulnerable but it should also note that minors stopped and searched by the police are vulnerable and anyone under 10 in possession of illegal items should be considered a victim of exploitation as well and thus vulnerable.

Q10. To what extent do you agree or disagree that with the approach the code of practice provides on how to assess and manage the risk of obtaining confidential material, and how to proceed when it is unintentionally obtained?

As technology capabilities vary between forces, much of which is “off-the-shelf,” the code could note protocols around tech procurement, making it necessary for privacy protection to be built in and prevent excessive capabilities that can handle irrelevant data from the offset. As many police forces have access to technology that provide them with the capability for further analysis of personal data outside of purpose it is collected for and there must be adequate provision to prevent this analysis.

Further, procedural safeguards should not only assess the relevance of the information being sought before extraction takes place, but include an ex-post assessment of the information that has been extracted and whether this is actually relevant. This should be an ongoing assessment for as long as the information is retained, and should be subject to review by a DPO.

The code should note how consent be recorded and under which form, including the clear lawful basis for extracting the information and the level of search to be conducted on the phone. For example, will the search involve specific images and texts or will it be a forensic search of the hardware; in addition, what data is being searched i.e. only texts, images, GPS location or app data as well.

Thinking now about the overall approach to the exercise of the powers that is recommended in the code.

Q12. Are there any gaps in the guidance that should be addressed?

- Yes

Training and lesson learning

Previous concerns have emerged over the lack of awareness within forces over powers and relevant justifications, therefore, the code should mandate extraction powers should only be exercised after they have received training. Training should be uniform and rolled out consistently else there is a risk different forces will implement different standards.

Police forces have in the past come under scrutiny due to their cavalier attitudes toward data extraction; it is important for forces to have taken stock of inappropriate handling of data and abuse of powers through in-force training.

Also there are serious concerns around immigration officers having powers due to their track record of irresponsible data collection at the border and in facilities, the scant knowledge and training immigration officers ecieive and the power imbalances between immigration officials and those they surveil. Robust training, awareness and safeguards are needed and this is missing in the code.

Disciplinary process

The code notes that a report to the Information Commissioner will be made and disciplinary procedures instigated for non compliance with the code. However, consequences for data breaches and the misuse of powers should be clearer and the escalation stages involved.