Extraction of information from electronic devices: code of practice CONSULTATION RESPONSE

19 July 2022

About StopWatch

StopWatch is a coalition of legal experts, academics, citizens and civil liberties campaigners. We aim to address excess and disproportionate stop and search, promote best practice and ensure fair, effective policing for all.

Our response

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?

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- **Strongly disagree**

Please explain the reason for your answer

We are concerned that section 37 guidance fails to address the 'voluntary' nature of police/civilian interactions surrounding data extraction. We have anecdotal stop and search evidence of police officers attempting to obtain mobile electronic devices and extract data from them by stating to the person being searched that it is a legal requirement for them to hand over the device. This is what we understand to be 'undue pressure', as described in paragraph 86 of the document.

The claim is made in order to persuade an individual to voluntarily hand over a device where an officer might otherwise use force to obtain it. In these circumstances, the behaviour of the officer fails to meet the requirements of section 37, and so the individual searched is not protected by section 37.

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 agree
- Agree
- Neither agree nor disagree

- Disagree
- **Strongly disagree**

Please explain the reason for your answer

This code of practice on the extraction of information from electronic devices comes at a time when the government has also proposed changes to data protection (*Data Reform Bill*) and human rights legislation (*Bill of Rights*). If legal protections from those areas are weakened, then so are the safeguards against abuses of police power concerning the extraction of information from electronic devices.

We fear data reforms will empower law enforcement authorities by liberalising the invocation of the public interest argument in their favour over the handling of 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 *Data Protection Act* (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. Therefore, the code should iterate the necessity for each force to carry out a DPIA and EIA in relation to extraction powers. We believe this may be necessary in the case of the new Serious Violence Reduction Orders passed under the *Police, Crime, Sentencing and Courts Act* 2021 legislation, as the Home Office has already acknowledged that 'there may be a disproportionate impact of the orders on the black adult population'.

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?

- Strongly agree
- Agree
- Neither agree nor disagree
- **Disagree**
- Strongly disagree

Please explain the reason for your answer

While the use of the section 37 power requires a device user, or their representative (in the case of child or adult without capacity), to agree to information extraction **in writing**, it is too risky to ensure an oral agreement as a second option during a stop and search if the person has an impairment of any sort. The person is demonstrably too vulnerable to agree to anything, therefore the only course of agreement ought to be via their representative in writing.

Q11. In your view is the suggested approach to use of the powers detailed in the code one that can be implemented operationally?

- Yes
- **No**

Please explain the reason for your answer

In the case of stop and search, the individual searched is a person of interest to officers, but the hostile nature of many stops suggests that any approach to exercising powers under section 37 of the code of practice concerning the extraction of information from an electronic device will not work. There are also reports of a backlog of more than 20,000 mobile devices waiting for examination across all UK police forces, which represents a potential data processing blockage so vast that it renders the well-meaning intentions of this code completely redundant.

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

- **Yes**
- No

Please explain the reason for your answer

From the perspective of stop and search regulation, we believe there are gaps in the guidance that can only be addressed elsewhere, namely in the PACE code of practice. This is because the proposed code of practice builds on an assumption that there is a sufficiently clear legal basis for the police obtaining devices during stops, either voluntarily or through seizure. In fact, as our 2019 report on police seizure of mobile phones states, there appear to be only 2 justifications for obtaining devices during stops. The first is clear cut, the second is not:

1. Part I section 1 of the *Police and Criminal Evidence Act (PACE)* 1984 gives what may be '*the only clear-cut legal basis*' for seizing such a device – that it would be considered on reasonable grounds to be stolen – and so electronic devices '*found suspected to be stolen would need to be searched to confirm this.*

2. *PACE* part II section 19 states that during a search, a constable may seize anything on the premises or may require any information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible, if he has reasonable grounds for believing: a) it is evidence in relation to an offence which he is investigating or any

> other offence; or b) it has been obtained in consequence of the commission of an offence. This decision relies on the judgment of the constable, whose 'reasonable belief' is unlikely to be called into question, yet confers upon them extraordinary powers to breach an individual's right to privacy. There are no safeguards to prevent such an abuse of power.

By extension, the second point lends itself to other vaguely worded legislation such as section 43 of the *Terrorism Act* 2000, under which police are permitted to search those they suspect of terrorist activity and seize anything they feel is evidence of this. Some have suggested this would extend to searches of phones, but this is not explicit. The *Misuse of Drugs Act* 1971 contains a similar uncertainty in its wording: 'to seize and detain, for the purposes of proceedings under this *Act*, anything found in the course of the search which appears to the constable to be evidence of an offence under this *Act*'. Again, while some could suggest this may include a phone, without guidance on this, it remains ambiguous.

And the police are known to take advantage of this: our report found a forum discussion on *UK Police Online* (2011) in which members claimed that they were 'always told that if you are conducting a stop search in the street under s23 for example, you can have a look through the mobile phone' and that 'if someone has enough drugs to (or has drugs in a way that would) implicate dealing then as a matter of course surely everyone seizes any mobile phones as evidence'.

With attitudes like this, failing to provide clarity on *PACE* guidance runs the risk of making a regularly coercive police behaviour appear consensual. There is a power dynamic at play between a police official and a member of the public, heightened when that person is considered 'suspect', and informed consent to device extraction is contentious as those being asked to supply their devices are not always made aware of their rights.

On 2019 report on mobile phones made the following recommendations:

- Police searches of mobile phones and the data contained within them should be halted until their legality can be clarified and until appropriate data protection guarantees are in place;
- The government should review the legality of the searches for and of mobile phones under the acts covered by the *PACE* code of practice A;
- The government should issue guidance on mobile phone searches for police and public;
- The government should revisit the legality of search powers regarding phones under the *Terrorism Act* 2000. Up to date guidance should be produced for police and public on the powers under this *Act* regarding public photography;
- The government should commission research on the police and public experiences of, and attitudes towards, mobile phone searches.

We believe that these points should be addressed before further codes of practice are ratified in legislation.

References

GOV.UK (2022). Home Office measures in the Police, Crime, Sentencing and Courts Bill: Equalities Impact Assessment
https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-equality-statements/home-office-measures-in-the-police-crime-sentencing-and-courts-bill-equalities-impact-assessment

legislation.gov.uk (2021). Police and Criminal Evidence Act 1984
https://www.legislation.gov.uk/ukpga/1984/60/contents

Channel 4 News (2022). Police backlog of over 20,000 digital devices awaiting examination
https://www.channel4.com/news/police-backlog-of-over-20000-digital-devices-awaiting-examination

StopWatch (2019). Call it off: Are police searching mobile phones illegally?
https://www.stop-watch.org/what-we-do/research/mobilephone-report-call-it-off/