9 NGOs' Response to the Consultation on The Extraction of Information from Electronic Devices Code of Practice [The Police, Crime, Sentencing and Courts Act 2022]

By:

Big Brother Watch

Centre for Women's Justice

End Violence Against Women

Rape Crisis England & Wales

Refuge

Liberty

Privacy International

Fair Trials

Defend Digital Me

July 2022

Introduction:

We welcome the opportunity to respond to this consultation on The Extraction of Information from Electronic Devices Code of Practice, which contains guidance about the exercise of powers in sections 37(1) and 41(1) of The Police, Crime, Sentencing and Courts Act 2022 ("the Act" hereafter).

The 9 NGOs who are signatories to this consultation response span expertise on human rights, privacy, and women's and victims' rights. We welcome improvements to the digital extraction system, but are concerned that the draft Code of Practice is insufficient to protect vital data, privacy and equality rights that are critical in the context of digital extractions, particularly as they relate to complainants of rape, domestic abuse and sexual offences.

Set against the backdrop of the Government's intended repeal of the Human Rights Act 1998 and 'reform' of the Data Protection Act 2018/UK GDPR, and heightened attention during the Conservative leadership contest on the possibility of withdrawal from the European Convention on Human Rights, we are concerned that new digital extraction practices risk lacking elemental protections that are vital to protect victims' and witnesses' (and suspects') rights. The draft Code of Practice ('the draft Code' hereafter), which refers frequently to the Human Rights Act and Data Protection Act/UK GDPR as the foundational framework with which digital extraction must comply, must be read with this alarming and highly uncertain context in mind.

We have outlined the key issues that require rectification below.

1) **The draft Code of Practice insufficiently describes what defines an agreement and how to record it**

2) **The draft Code of Practice contains inadequate safeguards to prevent excessive digital extractions**

3) **The draft Code of Practice fails to allow complainants or witnesses to obtain a review of a request for digital extraction**

4) **The draft Code of Practice fails to limit police possession of a device**

5) **The draft Code offers insufficient protections for individuals met with digital extraction requests by immigration officers**

1) The draft Code of Practice insufficiently describes what defines an agreement and how to record it

The written agreement

The draft Code of Practice states that where the use of the section 37 power requires a device user, or their representative (in the case of child or adult without capacity), to volunteer the device and agree to the information extraction, this agreement must first be provided in writing. This appears to merely restate the requirement of s.37 of the Act. The Code of Practice offers no guidance as to what the written agreement should actually include.

The draft Code does state that the authorised person must provide the person with a written notice specifying certain aspects of the digital extraction request, but the requirement for a written notice is treated separately to the requirement of a written agreement - there is no guidance as to what shape the latter should take.

This is a grave oversight. These documents are complicated and it should be crystal clear to the individual what exactly they are agreeing to. As is stands, the written agreement could be a one line email.

RECOMMENDATION: The Code must outline the required format of the written agreement document which, in particular, must include at least the information contained in the written notice.

The written notice

The draft Code states that the current Data Processing Notice produced by the NPCC in September 2021 is approved for use by police forces in England and Wales to be used as the written notice. Whilst we welcomed the revised Data Processing Notice in September 2021, it has not been properly implemented and the measures in the Act and draft Code are inadequate to ensure proper implementation. Furthermore, under the new digital extraction process under the Act, we are of the view that the Notice requires additional safeguards as set out in this response.

Therefore, and without the draft Code containing additional notable safeguards regarding the written notice and agreement, this means the draft Code merely entrenches the status quo that the Act claimed to tackle. The fact that the status quo complies with the draft Code is a reflection of the fact that the draft Code is inadequate.

The draft Code states that the written notice, which provides the device owner with details about the nature of the extraction request, should have certain features – which closely mirror the features set out in the Act. The draft Code states that the written notice must specify (we have put requirements that are in the draft Code but not in the Act in bold):

- the information that is sought
- the reason why the information is sought (**and, where relevant, how it supports a reasonable line of enquiry**)

- how the information will be dealt with once it has been extracted (**including who will see it**)

- that the person may refuse to provide the device or agree to the extraction of information from it

- that the investigation or enquiry for the purposes of which the information is sought will not be brought to an end merely because of a refusal to provide the device or agree to the extraction of information.

Where digital extraction is sought for a purpose under s.37(2)(a) of the Act, that is "preventing, detecting, investigating or prosecuting crime", the reason why the information is sought can only be adequately explained by its relation to a specified line of enquiry. Indeed, s.37(5)(a) is clear that an authorised person may only extract informed for this purpose if they "reasonably believe that information stored on the electronic device is relevant to a reasonable line of enquiry". Therefore, in RASSO and domestic abuse investigations where s.37(2)(a) extractions apply, how the information sought supports a reasonable line of enquiry will always be relevant and this should be made an explicit requirement of a written notice.

RECOMMENDATION: The Code should require that a written notice includes why the information subject to digital extraction is sought *and* how it supports a reasonable line of enquiry if the extraction is sought for a purpose under s.37(2)(a).

The draft Code further states that the device user should be "informed" of the following:

- of how any collateral information obtained will be managed

- of when the device is likely to be returned

- that they can make a complaint to the controller if they feel the request for information is excessive, or that they have been coerced into providing the device and giving agreement

However, this information is not required to be included on the written notice and as such, could be given verbally.

The current Data Processing Notice in use in England and Wales (DPNa) does contain a box titled 'Collateral intrusion' which invites the authorised person to explain 'To what extent is there a risk of collateral intrusion and what steps, if any, have been taken or can be taken to mitigate this'.

However, the current notice does not contain information about when the device is likely to be returned, or about how an individual can make a complaint to the controller.

Information about the length of time for which the device may be out of the user's possession is critically important to enable an informed agreement, and to address a common obstruction to rape investigations. Further, information about the ability to make a complaint about the request is a critically important safeguard on the written notice, and must be stated clearly to ensure that individuals are aware of their options when reviewing a request and deciding whether to agree to it.

RECOMMENDATION: The Code should require that all of the above three points are features of the written notice, rather than simply matters that an individual should be informed of by any means.

Further, the draft Code should require that the written notice includes an explanation of what less intrusive methods to obtain the information were considered before the request for extraction was made and why no less intrusive means are possible.

The current NPCC Data Processing Notice already contains a similar box, titled 'Detail what alternatives to extraction have been considered and rejected'. This should be a requirement of a written notice. Information about the less intrusive methods that may or may not be available, and an explanation of why that is so, is vital for an informed, genuine agreement to be made. This information is central to the necessity and proportionality of the request.

Indeed, the draft Code states that the authorised person "should record their rationale as to why the information extraction is necessary and proportionate in the circumstances" (paragraph 48) but neither states where this should be recorded, nor that this should be shared with the individual affected in the written notice in order for them to make an informed decision. Likewise, paragraph 79 of the draft code states:

"Authorised persons should record in writing their rationale for their decisions to use these powers, to include the points noted above – the relevant information sought, why the use of these powers is necessary and proportionate, what alternative options for obtaining the information have been considered and, if any were identified, why it was not reasonably practicable to use them."

However, the draft Code neither states where this should be recorded, nor that this should be shared with the individual affected in the written notice in order for them to make an informed decision.

RECOMMENDATION: The Code should require that a written notice includes an explanation of what less intrusive methods to obtain the information were considered before the request for extraction was made and why no less intrusive means are possible.

RECOMMENDATION: The Code should require that a written notice includes a record of the authorised person's rationale as to why the information extraction is deemed necessary and proportionate in the circumstances.

2) The draft Code of Practice contains inadequate safeguards to prevent excessive digital extractions

Under the Act, an authorised person may only extract digital information for the prevention, detection, investigation or prosecution of crime (s.37(2)(a)) if the person "reasonably believes that information stored on the electronic device is relevant to a reasonable line of enquiry" (s.37(5)(a)) and if they are "satisfied" that it is "necessary and proportionate" to achieve that purpose (s.37(5)(c)). If there is a risk of obtaining information other than that which is necessary to achieve the purpose, a proportionality test is set out, creating a threshold that there are no other means of obtaining the information sought which avoid that risk, or that there are such means but it is not "reasonably practicable" to use them.

This could mean that the entire contents of a person's phone could be downloaded if, for example, the police force does not have software capable of specifying and limiting the data extraction, although it may exist (i.e. if it is not reasonably practicable to use more proportionate means). This risks a continuation of the types of practices and justifications around digital strip searches that campaigners have fought to end, and that have been found to be unlawful. The draft Code offers no mitigation of this serious risk, only further confusion.

Paragraph 48 of the draft Code correctly states:

"In order for the exercise of [the extraction] power to be necessary and proportionate, the authorised person will have to be satisfied that the information sought is required to achieve the relevant purpose (e.g. preventing crime) and that the purpose **cannot be achieved by less intrusive means**" (our emphasis).

The draft Code also states that, where there is the risk of extracting excess information:

- other methods, including examining the suspect's phone or taking screen shots, should be considered (paras. 49-50)
- this may include the use of appropriate technologies to support selective extraction (para. 53)

- it may also include the use of targeted key words, date ranges or other specifics to identify necessary information (para. 53)

- delay alone is not sufficient justification not to pursue an alternative method unless there is an immediate risk of harm (para. 51)

- extracting information from a victim/witness' device should be the last resort (para. 51)

- authorised persons should be aware of, and keep up to date with, technology options available in their organisations and ensure they use the most selective tool (para. 53).

The draft Code rightly states in paragraph 48 that the proportionality test requires that the purpose "cannot" be achieved by less intrusive means – not that it "is not reasonably practicable" to achieve the purpose by less intrusive means.

However, paragraph 48 also later states:

"The authorised person should consider the value of the information extracted for the relevant purpose and **where possible ensure that the amount of information extracted is minimised.**" (our emphases)

It is a legal requirement under the Data Protection Act 2018/UK GDPR that the information extracted is minimised. This should be made much clearer in the Code.

Further, paragraph 49 states that if there is a risk of obtaining excess information the authorised person "must be satisfied that there are no other means of obtaining the information that avoid that risk, or if there are such means, it is **not reasonably practicable** to use them." (our emphasis)

The draft Code states that "reasonably practicable" is an "objective" test, but gives a circular definition of the test: "The authorised person must assess whether it would be reasonably practicable to use other means in the circumstances." This is unacceptably vague and leaves intrusive methods prone to inappropriate use.

On our analysis, this is highly likely to be incompatible with the right to privacy protected by Article 8 of the European Convention on Human Rights or with the Data Protection Act 2018. We are not aware of any legal basis for allowing processing to take place, even though a less intrusive alternative is available, because it is judged not to be 'reasonably practicable'. Practicability is not and has never been an appropriate test on which to balance individuals' privacy rights. If less intrusive means are available to obtain data, they should be adopted to meet the requirement that processing is strictly necessary and proportionate, protecting privacy rights and also ensuring access to justice.

The use of less proportionate means was explored at length in the *Bater-James & Anor v. R* judgment, and nowhere in this judgment was 'practicability' set out as a legitimate reason for excessive privacy intrusion. If less intrusive means of obtaining data are available, they must be used, or the extraction is unlikely to meet the test of strict necessity and proportionality.

RECOMMENDATION: The Code must make clear that the least intrusive means of obtaining necessary data must be used in order for the extraction to meet the necessity and proportionality test.

RECOMMENDATION: The Code should require that relevant organisations procure technology options that offer the most selective tools to conduct digital extractions.

3) The draft Code of Practice fails to allow complainants or witnesses to obtain a review of a request for digital extraction.

As discussed, the draft Code states that the device user should be "informed" that they can make a complaint to the data controller if they feel that the request for information is excessive, or that they have been coerced into providing the device and giving agreement. This information is not required to be included on the written notice and could be given verbally. Further, paragraph 193 of the draft Code states that the authorised person is likely to be the 'controller'. This means that the individual will be complaining to the same authorised person who has made the extraction request to them.

Whilst a complaint mechanism is important, and should be stated expressly on the written notice, it is no replacement for a right to an independent review of a request.

We believe a review mechanism is an important process to ensure that the requesting individual has correctly analysed the complex factors of strict necessity and proportionality, accounting for multiple factors such as less intrusive methods, technical capabilities and the user's legal rights. A process by which complainants can request a review of personal data requests is being trialled by Thames Valley Police in conjunction with the Ministry of Justice. This was an action that emerged from the Government's end-to-end rape review, published in June 2021. We welcome this pilot and believe it is vital that a right to a review is maintained in the Code of Practice.

At present, if an individual is met with an unreasonable or excessive request for digital information they can only comply or refuse, and in choosing either option may make a complaint, but they cannot simply request a review. Our organisations are aware that, despite the renewed Digital Processing Notices as of September 2021, which according to this draft Code of Practice will be maintained, excessive requests for personal information are still routinely made, particularly to RASSO complainants. Faced with such a choice, some complainants decide to withdraw from the process altogether. A review mechanism is a simple and vital safeguard that will both help culture change in police forces and act as a safety net for investigations where complainants are met with unnecessary or disproportionate requests, thereby improving access to justice.

RECOMMENDATION: The Code of Practice should set out a mechanism by which an individual may obtain a review of the strict necessity and proportionality of a proposed agreement referred to in section 37(1).

RECOMMENDED PARAGRAPH:

(X) A user may obtain a review of the strict necessity and proportionality of a proposed agreement referred to in section 37(1). A review of a proposed agreement referred to in section 37(1) must be conducted by a Detective Chief Inspector or individual of more senior rank listed in Schedule 3 of the Act who is independent of the investigation (the 'Reviewer') and a decision returned in writing to the user and authorised person within 5 working days. In conducting a review of a proposed agreement, the Reviewer must consider the views of:

(a) the user, which may include representatives appointed by the user,

(b) the authorised person, and

(c) the Crown Prosecution Service.

In conducting a review of a proposed agreement, the Reviewer must take account of guidance provided by:

(a) the Information Commissioner's Office and

(b) the Commissioner for Victims and Witnesses.

4) The draft Code of Practice fails to limit police possession of a device

As discussed above, the draft Code states that the device user should be "informed" of when their device is likely to be returned to them. However, this information is not required to be included on the written notice or agreement. The current written notice (DPNa), which the draft Code states is acceptable as the written notice under the Act, does not contain information about when the device will be or is likely to be returned. Only in the accompanying generic notice, the FAQ (DPNb), is there a statement that:

"We will keep your device for the minimum amount of time necessary. The length of time will be determined by a number of factors and the officer to whom you give your device will give you an indication of how long this will be."

This has proven to be an entirely insufficient safeguard against lengthy possession periods, and in our experience is an insufficient mechanism to give complainants and witnesses accurate information about how long their device will be held or confidence in the process. In entrenching this practice, the draft Code is structured to fail.

It has been common for police digital extractions to result in lengthy delays to investigations, and for complainants to be left without their phones for months and even years. In recognition of the harm this can inflict on victims and the obstruction of justice, the Government's end-to-end rape review committed to ensuring "no victim will be left without a phone for more than 24 hours, in any circumstances, and our priority is that victims have their own phones returned within this period" and that this goal would be met by the end of this Parliament. Not only did the Act fail to deal with this issue, but the draft Code has also failed to deal with this serious, recurring issue.

A Freedom of Information investigation by Big Brother Watch in 2019 found that average wait times for devices to be examined varied across forces from 3 weeks to 5 months. However, our groups are also aware of cases where a phone has been retained for over 2 years, as in some cases devices may be retained until the end of criminal proceedings or when the case is closed.

This lengthy retention of devices can take away a lifeline from vulnerable people, particularly RASSO or domestic abuse complainants, who may be in a state or trauma and are likely to be in particular need of social support. It particularly disadvantages individuals who cannot afford to replace the device and as such would be unable to easily communicate, socialise or even work without an electronic device such as a phone or laptop. It also disadvantages victims of crime who are reporting an offence without the knowledge of their friends or family as it may be difficult to explain why they no longer have a device such as a phone. As such, the risk of losing possession of a device for a prolonged period of time prevents many individuals from pursuing their complaint or even reporting an offence in the first place.

The digital extraction technology available today, including mobile extraction kiosks which are now commonly possessed by police forces, mean that these delays and lengthy retention of devices are not strictly necessary and therefore cannot be justified. It is possible for specified data to be extracted rapidly and we believe that it is paramount that police forces are given the right funding and training to make this capability possible nationwide. The draft Code places no responsibility on forces to acquire such technology.

RECOMMENDATION: The draft Code should require that the written notice contains information about how long the device will be in police possession, and this should ordinarily be no longer than 24 hours but in any case, no longer than 30 working days. If the agreed time frame elapses without extraction taking place, a new agreement should be sought.

Further, to give individuals reassurance and foster trust, they should be given the option of being present during the digital extraction in the same way that an individual reporting a home invasion or burglary would be present during a search of their home.

It is important to remember that complainants and witnesses agreeing to a digital extraction are assisting police with an investigation of a crime – they are not suspects, and should not be treated as such.

RECOMMENDATION: The draft Code should state that the user may choose to be in the presence of the authorised person during the extraction unless either the user or the authorised person deems it impracticable or inappropriate, in which case an explanation must be set out in writing in the written notice and agreement.

5) The draft Code offers insufficient protections for individuals met with digital extraction requests by immigration officers

On our analysis, it was inappropriate to include immigration officers as "authorised persons" to conduct digital extractions in Schedule 3 of the Act, particularly in light of reports of frequent mass digital downloads in relation to asylum seekers.

The draft Code explains that vulnerable people may need more support to decide whether to provide their device for extraction (para. 106), and that vulnerable people may include "someone who has been the victim of people trafficking", "someone who fears repercussions from working with an authorised person to further an investigation", "someone who is suffering fear or distress", and someone with "language barriers", among other examples (para. 114). Some or all of these features are likely to be common in immigration cases, particularly cases where immigration officers are seeking to conduct a digital extraction. Therefore, the draft Code should require that all individuals subject to a request for a digital extraction by an immigration officer are treated as vulnerable individuals.

RECOMMENDATION: The Code should require that all individuals subject to a digital extraction request by immigration officers are treated as vulnerable people.

Paragraph 125 states: "If language is an additional barrier to understanding what is being asked of the individual, an interpreter should be made available."

The Code must make clear that if language is a barrier, an interpreter **must** be made available. Otherwise, the individual cannot be deemed to be making an agreement and the data processing cannot be considered lawful in accordance with the provisions of the Act. Police possession of a device without the full understanding and informed agreement of the device user is more akin to a seizure and requires different powers.

RECOMMENDATION: The Code must be clear that if language is a barrier to an individual understanding any aspect of the digital extraction request, an interpreter must be made available.