Victims' Commissioner briefing on the data extraction power clauses in Part 2 Chapter 3 of The Police, Crime, Sentencing and Courts Bill

Background on the impact of digital disclosure on victims

In recent years, the issue of digital disclosure, particularly in rape cases, has rightly been given a great deal of attention and scrutiny. There can be no question that 'on the ground' it has become practically routine for rape complainants to be asked to hand over digital devices and for most, or all, of the material held therein to be trawled. Through my recent survey of rape complainants and through my network of stakeholders, I hear that the CPS will frequently seek this level of material and a complainant's refusal to submit will result in the case not proceeding to charge.[1] This is highly troubling for victims, has a chilling effect on their confidence in reporting crimes, and may impact victim attrition.

Analysis conducted by my office of a Rape Crisis administrative dataset showed that one in five victims withdrew complaints, at least in part, due to disclosure and privacy concerns. [2] Victims in 21% of complaints had concerns about digital downloads and disclosing GP, hospital, school, employment records, and a combination of negative press coverage.

Home Office data also shows an increase in withdrawal of rape complaints pre-charge, from 20% in 2014/15 to 42% in year to September 2020.[3]

I echo the concerns of many senior police chiefs that there has been a fall in public and victim confidence in the police, in particular in relation to rape cases. The issue of digital data extraction plays a big role in this.

The Northumbria sexual violence complainant's advocacy scheme pilot (SVCAS) engaged local solicitors to provide legal advice and support to rape complainants in Northumbria primarily related to complainants' Article 8 rights to privacy.[4] The pilot demonstrated what is happening in practice, at least in that region. About 50% of requests were not strictly necessary and proportionate. These were challenged by the advocates through the scheme.

Some police officers who participated in the scheme expressed concern about this culture:

> *"I could talk all day about third-party material, and it is the real bone of contention. It's one of the things that has given me sleepless nights over the years, you know. It has… And I had a rape team investigator say to me on one occasion, or a former rape team investigator, say to me, 'I had to like leave the rape team because of what I was being asked to do, in relation to victims, I couldn't do it'. And I think, you know, that, for me just spoke volumes. And lots of*

[1] *Rape survivors and the criminal justice system*, Victims' Commissioner, Oct 2020: https://victimscommissioner.org.uk/published-reviews/rape-survivors-and-the-criminal-justice-system/

[2] https://victimscommissioner.org.uk/news/the-reasons-why-victims-of-rape-and-sexual-violence-withdraw-from-the-criminal-process-without-seeking-justice/

[3] https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-year-to-september-2020-data-tables

[4] *Final Report: Evaluation of the Sexual Violence Complainants' Advocate Scheme*, Dec 2020, Olivia Smith & Ellen Daly: https://needisclear.files.wordpress.com/2020/11/svca-evaluation-final-report-1.pdf

people were expressing their concerns, including me, but when that officer said that to me, I kind of thought, d'you know what, there's something sadly wrong here." (Police Manager 1)

"…The CPS routinely ask us to obtain peoples 3rd party, medical, counselling and phone records regardless of whether a legitimate line of enquiry exists or not. Further to that they insist that we check the voluminous data in its entirety. This is usually PRE-CHARGE." (Police Officer Case 27, Case Files, emphasis in original)"

As well as impacting victim attrition, we also know that it is a factor in decision making about whether to even report in the first place.

My survey of rape complainants showed that, for some, scrutiny of their personal lives including their digital lives was a consideration in their decision not to report. [5]

And for those who did report, the experience was felt to be invasive and traumatic with many feeling the process was not adequately explained.

"Just 33% agreed that the police clearly explained why any request to access mobile phone and other personal data were necessary, and 22% that they explained how they would ensure that data would only be accessed if relevant and necessary. Requests for these data were often considered invasive and intrusive, and survivors had serious concerns about this."[6]

In fact, many respondents felt they had no choice but to hand over devices for scrutiny, which raises issues of what *voluntary* means in the context of a police power and arguably confirms the need for safeguards in legislation.

"Many survivors said that they wanted to help with the investigation and achieve a positive outcome. Some did not believe that they could refuse such requests, that they did not have anything to hide, or thought the requests were simply part of normal investigation procedures. However, most survivors had concerns around the disclosure of personal data and access to records."[7]

A 2020 report by the Information Commissioner (ICO) on data extraction from mobile phones outlined that the way in which police were operating did not comply in a number of respects with data protection legislation and argued that the gateway of 'consent' which police had been reliant on was not open to them for a number of reasons.[8] They could rely on 'strict necessity' for law enforcement purposes but that comes with a number of prior conditions which must also be met. The report additionally outlined concerns about the realities of such downloads impacting on others' right to privacy, such as family and friends whose sensitive data may also be contained on a complainant's mobile but from whom consent is never sought.

[5] Ibid. 1
[6] Ibid. 1
[7] Ibid. 1
[8] Mobile phone data extraction by police forces in England and Wales Investigation report, June 2020: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

Whilst a great deal of work has been done at a policy level to address some of these issues. None of the work to date has sought to alter police powers to obtain and scrutinise a digital device.

What led up to these proposed new powers?

The police quite separately sought a power in legislation which addresses a very specific circumstance whereby a member of the public might offer a phone to an officer stating there is relevant evidence on there, please examine it. The clauses in Part 2, Chapter 3 of The Police, Crime, Sentencing and Courts Bill[9] were originally designed to allow police to take a phone in these circumstances, addressing fears that should they currently accept a device this way, they would not be compliant with the framework in the Investigatory Powers Act 2016 (IPA)[10]*

I was consulted about the clauses whilst in draft form and raised some concerns that the power, whilst intended to address the above circumstance would also have implications for victims of crime, particularly victims of rape.

With agreement from the National Police Chiefs Council and the Information Commissioner's Office I suggested some amendments to the clauses (Appendix A) but in the end, the Government chose not to incorporate most of them. The power in the bill is wide ranging and I fear it effectively provides a legal basis for current practice, with the safeguards for victims of crime relegated to guidance.

Existing case law legislation and guidance makes clear that agreement for digital extraction can only be sought if the officer believes relevant material can be extracted from a phone; for criminal investigations this means relevant to a reasonable line of enquiry.[11] In Bater-James, judges were clear that this means no speculative searches, there must be specificity based in a reasonable line of enquiry.[12] Further, such information may only be extracted in so far as it is strictly necessary and proportionate for the investigation, the officer must also be satisfied that there are no other less intrusive means of pursuing the line of enquiry available to him/her.

It is also vital that whilst from a data protection legislation perspective the police can rely on strict necessity for law enforcement, victims are agreeing to the download, which means that they fully understand what is being sought and that agreement is freely given.

[9] https://publications.parliament.uk/pa/bills/cbill/58-01/0268/200268.pdf

[10] https://www.legislation.gov.uk/ukpga/2016/25/contents * unless they also comply with the requirements of the Regulation of investigatory Powers Act 2013 and secure a directed surveillance authority or 2-way consent

[11] Bater-James & Mohammed v R [2020] EWCA Crim 790, The data Protection Act 2018, The Attorney General's Guidelines on Disclosure, Criminal Procedure and Investigations Act 1996

[12] Ibid.

What are the clauses in the Bill?

I have highlighted some of our concerns with the drafts in text boxes alongside the clauses with further discussion below.

36

(1) An authorised person may extract information stored on an electronic device from that device if—

(a) a user of the device has voluntarily provided the device to an authorised person, and
(b) that user has **agreed to the extraction of information** from the device by an authorised person.

Agreement is not defined in the legislation, nor is there any requirement for police to be specific about what information is being

(2) The power in subsection (1) may be exercised only for the purposes of—

(a) **preventing, detecting, investigating or prosecuting crime,**
(b) helping to locate a missing person, or
(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

For section 2 (a) 'preventing, detecting, investigating or prosecuting crime' this means information must be relevant to a reasonable line of enquiry.

(5) An authorised person may exercise the power in subsection (1) only if—

(a) the authorised person **reasonably believes** that information stored on the electronic device is relevant to a purpose within subsection (2) for which the authorised person may exercise the power, and
(b) the authorised person is satisfied that exercise of the power is **necessary and proportionate** to achieve that purpose.

Reasonable belief in relevance is not the same as it forming a reasonable line of enquiry.

The test in law is strict necessity.

(6) Subsection (7) applies if the authorised person thinks that, in exercising the power, there is a risk of obtaining information other than—

(a) information necessary for a purpose within subsection (2) for which the authorised person may exercise the power, or
(b) information necessary for a purpose within subsection (2) of section 4 (investigations of death) for which the authorised person may exercise the power in subsection (1) of that section.

(7) The authorised person must, to be satisfied that the exercise of the power in subsection (1) is proportionate, be satisfied that—

(a) there are no other means of obtaining the information sought by the authorised person which avoid that risk, or
(b) there are such other means, but it is not **reasonably practicable** to use them.

The use of the phrase reasonably practicable is a problem both because it is incompatible with data protection legislation and because we are concerned that this gives police a means of easily dismissing other options.

(8) An authorised person must have regard to the **code of practice** for the time being in force under section 5 in exercising, or deciding whether to exercise, the power in subsection (1).

The code of practice whilst welcome, is without teeth, as the legislation specifically limits liability for breach and in any event the code is secondary to the legislation.

(9) This section does not affect any power relating to the extraction or production of information, or any power to seize any item or obtain any information, conferred by an enactment or rule of law.

What are the problems with these clauses?

1. **There is no definition of 'agreement' in the legislation**.

   I assume 'agreement' takes its normal meaning, but in practice I am aware that all too often 'consent/agreement' is being sought by police from complainants of sexual violence in circumstances where they are either not fully informed or are being coerced.

   I accept that it is a requirement of the legislation that the Secretary of State produce a Code of Practice, which I have been advised may cover agreement and other areas of concern. It is a fact that the legislation takes primacy over anything else and further the legislation as drafted precludes an 'authorised person' from being prosecuted or sued if they fail to adhere to the Code of Practice.

   I therefore think an important safeguard against abuse of this power would be to define agreement in the legislation. At the very least to make clear that agreement means informed and freely given.

   Additionally, linked to agreement is the need for the police (and others) to be specific about what data it is they are seeking, it is only by being specific that the data owner can give informed agreement to extraction.

2. **Reasonable line of enquiry**

   The legislation nods to this by use of the word 'relevant' but for the purposes of investigating and prosecuting crime, material sought from a suspect or complainant will only be relevant in as much as it is part of a reasonable line of enquiry. It is imperative that this is clearly defined in the legislation. Without a clear definition, the 'legal' hoop for police is merely *reasonable belief* in relevance. This risks further embedding a culture of wholesale downloads and intrusion into privacy. As outlined above, this increases the likelihood of victims losing trust in criminal justice agencies and risks increasing attrition rates.

   I further recommend that guidance mandates that the decision-making process of the authorised person in identifying a reasonable line of enquiry is recorded so that is can be scrutinised at a later date.

3. **Strict Necessity**

   I earlier advised that the test for authorised persons in using the power should be that the authorised person is satisfied that exercise of the power is strictly necessary and proportionate to achieve that purpose. This is because statute[13] and case law[14] insist on strict necessity as the only appropriate test in circumstances where sensitive data will be processed, that is for example health data, sexuality data etc. and/ or that

[13] Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[14] Bank Mellat v Her Majesty's Treasury (No 2): https://www.bailii.org/uk/cases/UKSC/2013/39.html

information about others. A complainant's phone will nearly always contain such information and so will automatically require sensitive processing. Additionally, as detailed elsewhere other options for obtaining the material should be considered first. The Government have in their clauses removed 'strictly' from the test, this creates a far lower threshold than the one which the Data Protection Act intended for processing of this type of material and means that victims' Article 8 ECHR rights are less protected.

4. Reasonably practicable

The term 'strictly necessary for the law enforcement purpose' under the Data Protection Act places a high threshold for processing based on this condition. Controllers (authorised persons or police here) need to demonstrate that they have considered other, less privacy-intrusive means and have found that they do not meet the objective of the processing. The test is not: having considered alternative means it is not practical to get the information via those means which is what the clauses effectively mandate. The risk for rape victims in this scenario is that both culturally and due to operational constraints the most practical, or easiest, path to obtaining the information sought will nearly always be the victim's phone. This insertion by government means, again, that normal practice is being bolstered by this legislative power with limited safeguards for victims.

5. Other issues

There are other issues with the legislation as drafted.

I am hugely concerned that the authorised person has no obligation to obtain views of children[15] and those without capacity[16] when seeking to obtain information from their phones. Whilst I accept that these groups cannot give agreement, I do feel an important safeguard of their human rights would be to include at least a duty to explore their views, as both groups may have very valid reasons why they may not wish their phones to be scrutinised. As it stands there is no obligation on either the police or the person giving agreement in their stead to ensure their views are considered.

Whilst I welcome a code of practice attached to this legislation, I have no idea what it may contain as this is not mandated in the legislation. Further there is no duty on the secretary of state to consult victims' representatives or champions in the process of creating it. As outlined above, it is also not a suitable alternative to protections for victims' being contained in the actual legislation.

Whilst not referenced in the legislation, much has been made of the digital processing notices (DPN's) or consent forms provided by police to complainants'[17] and whilst it is

[15] The Police, Crime, Sentencing and Courts Bill 37(1) onwards.
[16] The Police, Crime, Sentencing and Courts Bill 37(6) onwards.
[17] The NPCC are now working on a permanent version as the current DPN is temporary and does not address the concerns in the ICO report in any event.

important that those forms conform with the law, they provide no protection either. Firstly, they are of even less legal relevance than a Code. Secondly their status is merely as an available document. Neither the College of Policing nor NPCC has any power to compel their use in forces whose practices are dictated by their Chief Constables. Experience shows that many forces do not use any national form of DPN but use their own.

How do our proposed clauses (in full at Annex A) differ from the Government's clauses?

Government Clauses	**Scenario and commentary**	**Our clauses**	**Scenario and commentary**
(1) An authorised person may extract information stored on an electronic device from that device if— *(a) a user of the device has voluntarily provided the device to an authorised person, and* *(b) that user has agreed to the extraction of information from the device by an authorised person.*	As neither voluntarily or agreed are defined in the legislation, they will be taken to hold their normal meaning. This is problematic because it does not preclude forced or coerced agreement.	(1) Subject to Conditions A to D below, insofar as applicable, an authorised person may extract information stored on an electronic device from that device if— *(a) a user of the device has voluntarily provided the device to an authorised person, and* *(b) that user has agreed to the extraction of specified information from the device by an authorised person.*	We have aligned our clauses to the iterative process which has been outlined through case law and statute. We have also clearly defined agreement (see below) so that forced or coerced agreement is ruled out under the legislation. We also included the need for police to be specific about what it is they are seeking, so that the device user knows what it is they are agreeing to.
(2) The power in subsection (1) may be exercised only for the purposes of— *(a) preventing, detecting, investigating or prosecuting crime,* *(b) helping to locate a missing person, or* *(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.*		*2) Condition A for the exercise of the power in subsection (1) is that it may be exercised only for the purposes of—* *(a) preventing, detecting, investigating or prosecuting an offence,* *(b) helping to locate a missing person, or* *(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.*	Our clauses and the government clauses align here, the difference being that we have made this one of a number of conditions (see below) which must be fulfilled in order for the authorised person to use the power.
(5) An authorised person may exercise the power in subsection (1) only if—	The Government have used reasonable belief in relevant information but have failed to define that relevant for	*(4) Condition B for the exercise of the power in subsection (1) is that the power may only be exercised if—*	Although we have used reasonable belief here too, this is defined in sub-section 5 below as only

(a) the authorised person reasonably believes that information stored on the electronic device is relevant to a purpose within subsection (2) for which the authorised person may exercise the power, and *(b) the authorised person is satisfied that exercise of the power is necessary and proportionate to achieve that purpose.*	a purpose outlined in subsection 2(a) must mean relevant to a reasonable line of enquiry	*(a) the authorised person reasonably believes that information stored on the electronic device is relevant to a purpose within subsection (2) for which the authorised person may exercise the power, and* *(b) the authorised person is satisfied that exercise of the power is strictly necessary and proportionate to achieve that purpose.*	relevant for a purpose outlined in subsection 2(a) if it is relevant to a reasonable line of enquiry
		(5) For the purposes of subsection (4)(a), information is relevant for the purposes within subsection (2)(a) in circumstances where the information is relevant to a reasonable line of enquiry.	As stated above the Government does not define the need for there to be a reasonable line of enquiry in the legislation.
(6) Subsection (7) applies if the authorised person thinks that, in exercising the power, there is a risk of obtaining information other than— *(a) information necessary for a purpose within subsection (2) for which the authorised person may exercise the power, or* *(b) information necessary for a purpose within subsection (2) of section 4 (investigations of death) for which the authorised person may exercise the power in subsection (1) of that section.* *(7) The authorised person must, to be satisfied that the exercise of the power in subsection (1) is proportionate, be satisfied that—*	This is a complicated section and is designed to cover a scenario where an unrelated third party's information such as texts they have sent may be obtained as well as the information sought. Under the Data Protection Act (DPA) 2018 the test of strictly necessary for law enforcement, the authorised person in this case the police must show they have considered less privacy-intrusive means and have found that they do not meet the objective of the processing. Here the Government have effectively provided police with an excuse not to	*(6) Condition C as set out in subsection (7) applies if the authorised person thinks that, in exercising the power, there is a risk of obtaining information other than information necessary for a purpose within subsection (2) for which the authorised person may exercise the power.* *(7) Condition C is that the authorised person must, to be satisfied that the exercise of the power in the circumstances set out in subsection (6) is strictly necessary and proportionate, be satisfied that there are no other less intrusive means available of obtaining the information sought by the authorised person which avoid that risk*	Our clauses here mirror the strictly necessary for law enforcement provisions in the DPA 2018.

(a) there are no other means of obtaining the information sought by the authorised person which avoid that risk, or (b) there are such other means, but it is not reasonably practicable to use them.	meaningfully consider an alternative means of obtaining the information sought by adding that where such means are identified they do not have to use them if it is not reasonably practicable. This means that intrusion of the victim's article 8 rights and third parties whose private information may also be contained on their device will always just be the collateral damage as police will opt for scrutiny of their phone in the majority of cases, deeming alternatives as not reasonably practicable.		
(8) An authorised person must have regard to the code of practice for the time being in force under section 5 in exercising, or deciding whether to exercise, the power in subsection (1).		*(8) Condition D is that an authorised person must have regard to the code of practice for the time being in force under section {data1c} in accordance with section {data1d} below.*	Although both we and the Government have included the need to have regard to the code of practice, we say that in the case of the Government's clauses this code alone is not adequate for safeguarding victim's rights.
(10) In this Chapter— "adult" means a person aged 16 or over; "authorised person" has the meaning given by subsection (1) of section 7 (subject to subsections (2) and (3) of that section); "child" means a person aged under 16; "electronic device" means any device on which information is capable of being stored electronically and includes any component of such a device; "enactment" includes—	The Government has failed to define agreement, leaving it with its' normal meaning which is open to abuse of power.	*(10) In this section and sections {data1a} to {data2}—* *"adult" means a person aged 16 or over; "authorised person" means a person specified in subsection (1) of section {data2} (subject to subsection (2) of that section); "child" means a person aged under 16; ""agreement" means that the user has confirmed explicitly and unambiguously in writing that they agree to (i) provide their device; and (ii) the extraction of specified data from that device. Such an explicit written confirmation*	We have extensively defined agreement.

(a) an enactment contained in subordinate legislation within the meaning of the Interpretation Act 1978, (b) an enactment contained in, or in an instrument made under, an Act of the Scottish Parliament, (c) an enactment contained in, or in an instrument made under, an Act or Measure of Senedd Cymru, and (d) an enactment contained in, or in an instrument made under, Northern Ireland legislation; *"information" includes moving or still images and sounds;* *"user", in relation to an electronic device, means a person who ordinarily uses the device.*		*can only constitute agreement for these purposes if, in accordance with the Code of Practice issued pursuant to [relevant clause], the user:* *(i) has been provided with appropriate information and guidance about why the extraction is considered strictly necessary (including, where relevant, the identification of the reasonable line of enquiring relied upon);* *(ii) has been provided with appropriate information as to: (i) how the data will or will not be used in accordance with the authorized person(s) legal obligations; (ii) any potential consequences arising from their decision;* *(iii) has confirmed their agreement in the absence of any inappropriate pressure or coercion.* *"electronic device" means any device on which information is capable of being stored electronically and includes any component of such a device;* *"enactment" includes— (a) an Act of the Scottish Parliament, (b) an Act or Measure of Senedd Cymru, and (c) Northern Ireland legislation;* *"information" includes moving or still images and sounds;* *"offence" means an offence under the law of any part of the United Kingdom;* *"user", in relation to an electronic device, means a person who ordinarily uses the device.*	

In summary, the clauses as drafted provide the police with a wide ranging and unfettered power to obtain and scrutinise victim' phones, with virtually no safeguards for the victim in legislation. Some protections are said to be intended to be put in a code of practice, but one which police are free to ignore.

I fear that this legislation as drafted will provide the police (and Crown Prosecution Service via the police) with a legal basis to carry on as they have been. I think it can and should be challenged as incompatible with human rights legislation.

I should also make the point that the police accept my proposed amendments to the clauses are appropriate to their purpose and give a better balance for victim protection.

Appendix A – Proposed Amended Clauses

PROPOSED AMENDED CLAUSES

1 Extraction of information from electronic devices [data1]

(1) Subject to Conditions A to D below, insofar as applicable, an authorised person may extract information stored on an electronic device from that device if—

(a) a user of the device has voluntarily provided the device to an authorised person, and

(b) that user has agreed to the extraction of specified information from the device by an authorised person.

[Notes:
It is important that it is immediately obvious to the reader that the power may only be used if the conditions below are set out. In accordance with the Court of Appeal's judgment in *R v CB* [2020] EWCA Crim 790; [2020] 2 Cr. App. R. 20, alternatives to extraction should be considered before a request is made to, for example, a sexual violence victim. The clauses below have been amended to emphasis that there are a number of conditions upon the exercise of this power.

We have offered a definition of agreement that, in our view, will ensure that in the exercise of this power, the authorised person is also acting in accordance with their obligations under s.35 DPA 2018. We also note the comments of Fulford LJ in this regard in paragraphs 90-93.

Finally, the individual providing agreement must know what information is to be taken – and the power should only be exercisable in respect of the information so specified. It should not be used as a blanket power to take 'information' from a phone.]

(2) Condition A for the exercise of the power in subsection (1) is that it may be exercised only for the purposes of—

(a) preventing, detecting, investigating or prosecuting an offence,

(b) helping to locate a missing person, or

(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

(3) For the purposes of subsection (2) an adult is an at-risk adult if the authorised person reasonably believes that the adult—

(a) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(b) is unable to protect themselves against the neglect or harm or the risk of it.

(4) Condition B for the exercise of the power in subsection (1) is that the power may only be exercised if—

(a) the authorised person reasonably believes that information stored on the electronic device is relevant to a purpose within subsection (2) for which the authorised person may exercise the power, and

(b) the authorised person is satisfied that exercise of the power is strictly necessary and proportionate to achieve that purpose.

[Notes: The requirement should be that the exercise of the power is strictly necessary. There are a range of alternatives to the extraction of material from a device, which should be considered first. The Supreme Court in *Elgizouli v SSHD* [2020] UKSC 10, and the Court of Appeal in *Johnson v Secretary of State for the Home Department* [2020] EWCA Civ 1032,

confirmed that in this type of context necessity means strict necessity. Moreover, by its very nature, extraction in a criminal context is likely to involve in most instances the processing of special category data, to which primary legislation makes clear the strict necessity test applies.]

(5) For the purposes of subsection (4)(a), information is relevant for the purposes within subsection (2)(a) in circumstances where the information is relevant to a reasonable line of enquiry.

[NB: It should be clear that the test discussed in R v CB applies: see paragraphs 68-78].

(6) Condition C as set out in subsection (7) applies if the authorised person thinks that, in exercising the power, there is a risk of obtaining information other than information necessary for a purpose within subsection (2) for which the authorised person may exercise the power.

(7) Condition C is that the authorised person must, to be satisfied that the exercise of the power in the circumstances set out in subsection (6) is strictly necessary and proportionate, be satisfied that there are no other less intrusive means available of obtaining the information sought by the authorised person which avoid that risk.

[We do not agree that the proposed alternative limb is compatible with: (a) Article 8 ECHR and (b) the Data Protection Act 2018. If less intrusive means are available to obtaining a data extraction, they should be adopted in order to meet, in particular, the requirement that processing is strictly necessary and proportionate. 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'.
The test of proportionality under the ECHR was set out at paragraph 74 of *Bank Mellat* [2013] UKSC 39.

The available alternatives which apply to the consideration whether any extraction is proportionate are set out, for e.g. in the Criminal Court of appeal's judgment in case *R v CB*, at paragraphs 79-89 of Fulford LJ's judgment. The incremental nature of the correct approach is also emphasised.]

(8) Condition D is that an authorised person must have regard to the code of practice for the time being in force under section {data1c} in accordance with section {data1d} below.

(9) This section does not affect any power relating to the extraction or production of information, or any power to seize any item or obtain any information, conferred by or under an enactment.

(10) In this section and sections {data1a} to {data2}—

"adult" means a person aged 16 or over; "authorised person" means a person specified in subsection (1) of section {data2} (subject to subsection (2) of that section);
"child" means a person aged under 16;
"agreement" means that the user has confirmed explicitly and unambiguously in writing that they agree to (i) provide their device; and (ii) the extraction of specified data from that device. Such an explicit written confirmation can only constitute agreement for these purposes if, in accordance with the Code of Practice issued pursuant to [relevant clause], the user:
(i) has been provided with appropriate information and guidance about why the extraction is considered strictly necessary (including, where relevant, the identification of the reasonable line of enquiring relied upon);
(ii) has been provided with appropriate information as to: (i) how the data will or will not be used in accordance with the authorized person(s) legal obligations; (ii) any potential consequences arising from their decision;

(iii) has confirmed their agreement in the absence of any inappropriate pressure or coercion.
"electronic device" means any device on which information is capable of being stored electronically and includes any component of such a device;
"enactment" includes— (a) an Act of the Scottish Parliament, (b) an Act or Measure of Senedd Cymru, and (c) Northern Ireland legislation;
"information" includes moving or still images and sounds;
"offence" means an offence under the law of any part of the United Kingdom;
"user", in relation to an electronic device, means a person who ordinarily uses the device.
(10) References in this section and sections {data1a} to {data2} to the extraction of information include its reproduction in any form.
(11) This section is subject to sections {data1a} (children, and adults without capacity) and {data1b} (persons who have died etc).

1 Application of section {data1} to children and adults without capacity [data1a]

(1) A child is not to be treated for the purposes of section {data1} (1) as being capable of—
(a) voluntarily providing an electronic device to an authorised person for those purposes, or
(b) agreeing for those purposes to the extraction of information from the device by an authorised person.

(2) If a child is a user of an electronic device, a person who is not a user of the device but is listed in subsection (3) may—
(a) voluntarily provide the device to an authorised person for the purposes of section {data1} (1), and
(b) agreement for those purposes to the extraction of information from the device by an authorised person.

(3) The persons mentioned in subsection (2) are—
(a) the child's parent or guardian or, if the child is in the care of a relevant authority or voluntary organisation, a person representing that authority or organisation,
(b) a registered social worker, or
(c) if no person falling within paragraph (a) or (b) is available, any responsible person aged 18 or over other than an authorised person.

(4) The agreement of persons listed in subsection (3) further to subsection 2(b) should only be accepted where, if it is appropriate, the child has been consulted on whether such agreement should be provided and the authorised person is satisfied those views have been taken into account.

[NB: Children under the age of 16 may still have valid views as to whether their information should be provided – and should at least be consulted before this step is taken].

An adult without capacity is not to be treated for the purposes of section {data1}(1) as being capable of—
(a) voluntarily providing an electronic device to an authorised person for those purposes, or
(b) agreeing for those purposes to the extraction of information from the device by an authorised person.

(5) If a user of an electronic device is an adult without capacity, a person who is not a user of the device but is listed in subsection (6) may—

(a) voluntarily provide the device to an authorised person for the purposes of section {data1}(1), and

(b) agreement for those purposes to the extraction of information from the device by an authorised person.

(6) The persons mentioned in subsection (5) are—

(a) a parent or guardian of the adult without capacity,

(b) a registered social worker,

(c) a person who has a power of attorney in relation to the adult without capacity, or

(d) if no person falling within paragraph (a), (b) or (c) is available, any responsible person aged 18 other than an authorised person.

(7) The agreement of persons listed in subsection (6) further to subsection 5(b) should only be accepted where, if it is appropriate, the adult without capacity has been consulted on whether such agreement should be provided and the authorised person is satisfied those views have been taken into account.

[NB: Adults without capacity may still have valid views as to whether their information should be provided – and should at least be consulted before this step is taken].

(8) Nothing in this section prevents any other user of an electronic device who is not a child or an adult without capacity from—

(a) voluntarily providing the device to an authorised person for the purposes of section {data1}(1), or

(b) agreeing for those purposes to the extraction of information from the device by an authorised person.

(9) In this section and section {data1b}—

"adult without capacity" means an adult who, by reason of any impairment of their physical or mental condition, is incapable of making decisions for the purposes of section {data1}(1);

"local authority"—

(a) in relation to England, means a county council, a district council for an area for which there is no county council, a London borough council or the Common Council of the City of London,

(b) in relation to Wales, means a county council or a county borough council, and

(c) in relation to Scotland, means a council constituted under section 2 of the Local Government etc (Scotland) Act 1994;

"registered social worker" means a person registered as a social worker in a register maintained by—

(a) Social Work England,

(b) the Care Council for Wales,

(c) the Scottish Social Services Council, or

(d) the Northern Ireland Social Care Council;

"relevant authority"—

(a) in relation to England and Wales and Scotland, means a local authority;

(b) in relation to Northern Ireland, means an authority within the meaning of the Children (Northern Ireland) Order 1995 (S.I. 1995/755 (N.I. 2));

"voluntary organisation"—

(a) in relation to England and Wales and Scotland, has the same meaning as in the Children Act 1989;

(b) in relation to Northern Ireland, has the same meaning as in the Children (Northern Ireland) Order 1995.

(10) Section {data1}(9) and (10) also contains definitions for the purposes of this section.

1 Application of section {data1} where user has died etc [data1b]

(1) If any of conditions A to C is met, an authorised person may exercise the power in section {data1}(1) to extract information stored on an electronic device from that device even though—

(a) the device has not been voluntarily provided to an authorised person by a user of the device, or

(b) no user of the device has agreed to the extraction of information from the device by an authorised person.

(2) Condition A is that—

(a) a person who was a user of the electronic device has died, and

(b) the person was a user of the device immediately before their death.

(3) Condition B is that—

(a) a user of the electronic device is a child or an adult without capacity, and

(b) an authorised person reasonably believes that the user's life is at risk or there is a risk of serious harm to the user.

(4) Condition C is that—

(a) a person who was a user of the electronic device is missing,

(b) the person was a user of the device immediately before they went missing, and

(c) an authorised person reasonably believes that the person's life is at risk or there is a risk of serious harm to the person.

(5) The exercise of the power in subsection (1) of section {data1} by virtue of this section is subject to subsections (2) to (x) of that section.

(6) Sections {data1}(x) and (x) and {data1a}(x) contain definitions for the purposes of this section.

1 Code of practice [data1c]

(1) The Secretary of State must prepare a code of practice containing guidance about the exercise of the power in section {data1}(1).

(2) In preparing the code, the Secretary of State must consult—

(a) the Information Commissioner,

(b) the Scottish Ministers,

(c) the Welsh Government,

(d) the Department of Justice in Northern Ireland,

(e) the Victims Commissioner,

(f) the Domestic Abuse Commissioner,

(g) any regional Victims Champion including the London Victims Commissioner,

(h) persons who appear to the Secretary of State to represent the interests of victims, witnesses and other individuals likely to be affected by the use of the power granted in section {data1}(1), and

(i) such other persons as the Secretary of State considers appropriate.

[NB: It is essential that representatives of victims, witnesses and other relevant groups are consulted on the code of practice, especially those that have been involved in engagement with the NPCC on its own efforts to develop procedures for obtaining agreement for data extraction.]

(3) After preparing the code, the Secretary of State must lay it before Parliament and publish it.

(4) The code is to be brought into force by regulations made by statutory instrument.

(5) The code shall address, amongst other matters:

(a) the procedure by which an authorised person must obtain and record confirmation that a device has been provided voluntarily;
(b) the procedure by which an authorised person must obtain and record confirmation that agreement has been provided for the extraction of specified information, including the information which must be provided to the user about:
(i) how long the device will be retained;
(ii) what specific information is to be extracted from the device and why, including the identification of the reasonable line of enquiry to be pursued and the scope of information which will be extracted, reviewed and/or retained;
(iii) how the extracted information will be kept secure;
(iv) how the extracted information will or may be used in a criminal process;
(v) how they can be kept informed about who their information is to be shared with and the use of their information in the criminal process;
(vi) their right to refuse to agree to provide their device and/or to the proposed extraction in whole or in part and the potential consequences of that refusal; and
(vii) the circumstances in which a further extraction may be required, and what will happen to the information after the case has been considered;
(c) the different types of extraction processes available, and the parameters which should be considered in defining the scope of any proposed extraction from a user's device;
(d) the circumstances in which the extraction of information should and should not be considered strictly necessary and proportionate;
(e) the considerations to be taken into account in determining whether there are less intrusive alternatives available to extraction for the purposes of section {data1(x)};
(f) the process by which the authorised person should identify and delete data which is not responsive to a reasonable line of enquiry and/or has been assessed as not relevant to the purposes for which the extraction was conducted; and
(g) the records which must be maintained documenting for each extraction or proposed extraction, including:
(i) the specific information to be extracted;
(ii) the reasonable lines of enquiry pursued;
(iii) the basis upon which the extraction is considered strictly necessary, including any alternatives considered and why they were not pursued;
(iv) confirmation that appropriate information was provided to the user and, if applicable, agreement obtained;
(v) the reasons why the user was not willing to agree to a proposed extraction.

[NB: There are core matters which must be addressed by the Code of Practice to address the concerns raised by the Information Commissioner in her report on mobile data extraction, as well by relevant stakeholders in engagement with the NPCC, CPS and College of Policing on this issue. A core problem is that different police forces are using different means to obtain agreement – if any proper procedure is in place at all. It is also essential that the Code of Practice ensures that blanket, unwarranted requests for all information on the device do not continue to be a problem.

This provision is modelled on section 66 PACE]

(5) A statutory instrument containing regulations under subsection (4) is subject to annulment in pursuance of a resolution of either House of Parliament.

(6) After the code has come into force the Secretary of State may from time to time revise it.

(7) References in subsections (2) to (6) to the code include a revised code.

1 **Effect of code of practice [data1d]**

(1) An authorised person must in the exercise of the power granted under section {data 1} have regard to the code of practice issued under {data1c} in deciding whether to exercise, or in the exercise of that power.

(2) A failure on the part of any person to comply with any provision of a code of practice for the time being in force under section {data 1c} shall not of itself render him liable to any criminal or civil proceedings.

(3) A code of practice in force at any time under section {data 1c} shall be admissible in evidence in any criminal or civil proceedings.

(4) In all criminal and civil proceedings any code in force under section {data1c} shall be admissible in evidence; and if any provision of the code appears to the court or tribunal conducting the proceedings to be relevant to any question arising in the proceedings it shall be taken into account in determining that question.

[NB: this new proposed provision is modelled on section 67 PACE and section 72 of the Regulation of Investigatory Powers Act 2000. It should be made clear that the Code of Practice is relevant and admissible in legal proceedings.]