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. 'On the ground' it has become practically routine for rape complainants to be asked to hand over phones and other digital devices and for most, or all, of the material held therein to be trawled. Through my recent survey of rape complainants and my network of stakeholders, I am told that the CPS frequently seek this level of material and a complainant's refusal will simply result in a refusal to charge.[1] There is clear evidence from the CPS themselves that this is their approach. At page 51, the Government Research Report which underpin its End-to-End Rape Review published in June, CPS survey participants are reported describing:

'The importance of obtaining as much digital and third-party evidence as possible in all cases to ensure prosecutors could make robust charging decisions'

This is highly troubling for victims, has a chilling effect on their confidence in reporting crimes, and can persuade people who have reported to withdraw.

My office analysed a Rape Crisis administrative dataset which showed that one in five victims withdrew complaints, at least in part, due to disclosure and privacy concerns. [2]

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

Many senior police chiefs agree that there has been a fall in public and victim confidence in them in relation to rape cases and that digital data extraction plays a big role in this.

In Northumbria, the Home Office funded a pilot of legal advice for rape complainants in the police station. The advice was mainly about this area of digital download and championed complainants' rights to privacy under Article 8 of the European Convention on Human Rights.[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 their own concern about the current disclosure 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*

[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

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 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 on complainants dropping out after reporting, my survey of rape complainants showed that, for some, scrutiny of their personal lives and digital lives was a consideration in deciding not to report in the first place. [5]

For those who did report, the experience was felt to be invasive and traumatic and 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]

Many respondents felt they had no choice but to hand over devices for scrutiny.

"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 said that the way that police were operating did not comply with data protection legislation in a number of ways in particular that the gateway of 'consent' was not open to them for a number of reasons.[8] They expressed concerns about others' right to privacy, such as family and friends whose data may also be on a complainant's mobile but whose consent is never sought.

What is the need for digital material to be downloaded at all from the phone and other devices of a rape complainant?

It is the case that a complaint of for instance burglary is not met with a requirement that the victim's mobile phone and other devices are handed over to police/CPS to be scrutinised, so why should it be different in rape cases? The answer is that is shouldn't be different save that if the complainant and the defendant have been involved in an intimate relationship, the details of their communication and what they have said to others about what happened are likely to be on mobile phones and are likely to be relevant to what each of them says happened at the time of the alleged offence. The police therefore ask for that kind of material from mobile phones since it may be evidence either for the complaint or against it. That would be done following a 'reasonable line of inquiry' as required by the

[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

Criminal Procedure and Investigations Act 1996 before any evidence is pursued. In many such cases that limited level of request for digital download may, indeed, be reasonable. However, as set out above the experience of victims and the stated position of the CPS is that ALL material from digital devices is demanded as the price for CPS considering a charge. There is evidence from the frontline that even in stranger rapes the complainant's mobile phone is often required and downloaded. This leads complainants quickly to conclude that it is they who are being investigated for their suitability as a victim and not the defendant being investigated for what he has done

This is the kind of behaviour for which the Government has recently apologised. In particular, the Lord Chancellor, Robert Buckland said, in answer to a question from Harriet Harman MP about the use of a victim's previous sexual history in trials, when making a statement on the End-to-End Rape Review in the House of Commons on 21st June 2021:

'I think undue focus on the victim begins right from the initial investigation and I think that that is wrong. I think that the proper emphasis in this report is about looking at the person who is alleged to have done it, rather than constantly focussing as she rightly says, on irrelevant previous sexual matters that have nothing to do with the case and are an unwarranted intrusion into the private life of victims.'

And in answer to David Davies MP …….

'We need to move away from the fixation with the credibility or believing of the victim and be much more about the perpetrator. If someone's house is burgled they do not expect to have a long trawl into their personal history and if they had a window unlocked or whether they had been drinking: it is about trying to find out who did it and who is responsible for the crime. It is that sort of approach that is needed in rape and serious sexual offending'

Consequently, the Rape Review Action Plan sets out to be put in place already:

'Victims are not asked for information unless it is necessary and proportionate in pursuit of a reasonable line of inquiry' (at page 7)

The new legislative proposals, which are a green light for CPS and police to continue the current appalling practices, are totally inconsistent with the ministerial apology, with their rejection of the current culture of investigating the complainant rather than the defendant's behaviour and inconsistent with the action strictly to limit digital download demands in a fair way. While the End-to-End Rape Review is pointing in one direction these proposals are set to turn the clock back and go in the reverse direction.

Why is this legislation being proposed?

The police quite separately from these considerations 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 that it contains relevant evidence with a request that the officer looks at it. This could be for instance where someone is being stalked and abusive messages have been sent to their phone. These 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 if they did so they would fall foul of the rules against unauthorised interception of messages which are set out in the Investigatory Powers Act 2016 (IPA)[10]*

[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

Even though this is its purpose, the power is not limited to that use and will be applicable to every situation where the phone's owner agrees that the police can take the phone and download it. The word 'agreement' is not defined in these clauses and is currently often obtained by reference to the CPS refusing to charge if a rape complainant will not agree to hand over their phone in this way. The complainant is faced with 'agreeing' or seeing their case abandoned. So, at a time when the End-to-End Rape Review is determined to see download kept to what is fair and proportionate, these provisions are a green light to those who behave in this way, legitimating the current excessive and over-intrusive digital download practices

I was consulted on these proposals at an early stage when it became very clear that the power required by the police to avoid falling foul of IPA could be combined with protections for the privacy rights of complainants against the provision's over-use in rape cases. My office, with legal advice, therefore drafted some clauses which would accomplish both purposes. The representative of the National Police Chiefs' Council who attended the same consultation meetings and the Information Commissioner's Office both accepted that our amended drafts successfully fulfilled both purposes. The NPCC lead on these matters was and still is of the view that either the Home Office drafts or ours would meet their needs in full. The ICO would prefer different legislation entirely but accepted too that our drafts would give protection for rape complainants which is missing from those of the Home Office.

Bizarrely, the Home Office, while accepting one or two of our more minor amendments refused to accept most of those which would give real protection to victims while giving police the powers they need. A minister has spoken of a Code of Practice to be drafted to give some protection in some ways to some people in unspecified situations. No draft of any such Code of Practice has been made available. No Code of Practice can counteract what is clearly set out in legislation. The nature of this legislation is such that it will not just legitimatise current practices but will empower them and no Code of Practice will be able to limit or control that position. Additionally, police will not be conversant with the contents of a detailed Code as they will be trained to be about new law. And victims are entitled to know what law will be applied to investigations in their case and not to have to search for an obscure Code to seek to protect their rights to privacy against over-intrusive demands apparently licenced by law.

How do the clauses drafted by OVC differ from the Home Office clauses?

The two sets of clauses are set out in the appendix and we have highlighted some of our concerns with the drafts in text boxes alongside the Home Office clauses. The main differences are set out in the text below and some are technical but the importance of using the right phrases to give the protections needed is fairly clear.

What are the problems with these clauses?

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

   'Agreement' has a normal meaning, but in practice 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 as set out above by the circumstances they are in. It is therefore a vital safeguard 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 requests being specific that the data owner can give informed agreement to extraction.

I have been advised that a Code of Practice will be produced and may cover agreement but the legislation takes primacy over anything else. Further the legislation as drafted precludes an 'authorised person', usually a police officer, from being prosecuted or sued if they fail to adhere to the Code of Practice and so there is no penalty for a failure to abide by it and no remedy for a victim whose material is wrongly demanded or wrongly coerced from them

2. **Reasonable line of enquiry**

The legislation refers to the need for 'a reasonable belief' that material to be downloaded is 'relevant'

However, the proper test set out in other legislation (Criminal Procedure and Investigations Act 1996) is that for purposes of investigating and prosecuting crime, material sought from a suspect or complainant must be part of a reasonable line of enquiry. '*Reasonable belief*' in relevance is a far wider definition. This is especially the case given the current culture of being suspicious of the complainant and requiring to investigate her, as set out by Robert Buckland. Thus, a case where a letter to school in which a rape complainant had forged her mother's signature to get out of a lesson she did not like was considered by police to be 'relevant' disclosed to the defence and used in cross examination. There would be no place for such material in a test of what was a reasonable line of inquiry into the rape of which she complained ten years later. Thus, this wrong phraseology risks further embedding a culture of wholesale downloads and intrusion into privacy and gives no protections against that.

3. Strict Necessity

The test for police should be that the exercise of the power is strictly necessary and proportionate. This is because statute[11] and case law[12] 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 information about others. A complainant's phone will nearly always contain such information and so will automatically require sensitive processing. The Government clauses remove 'strictly' from the test, which creates a far lower threshold than the one which the Data Protection Act intended for processing this type of material and means that victims' Article 8 ECHR rights are less protected.

4. Reasonably practicable

In order to comply with the 'strictly necessary for the law enforcement purpose' test under the Data Protection Act police need to demonstrate that they have considered other, less privacy-intrusive means of getting the material and have found that they do not meet the objective of the processing. In the Home Office clauses there is a test that having considered alternative means it is not practical to get the information that way. Obviously, due to current culture and to police operational constraints the most practical way to obtaining the information on the complainant's phone will be to take it from that phone. So, the requirement to consider an alternative will not be 'practical' and the protection intended in the DPA is deliberately excluded.

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

5. Other issues

Whilst not referenced in the legislation, there are what are called 'digital processing notices' (DPNs) or consent forms provided by police to complainants[13] which it is said will deliver protection by setting out terms on download. Whilst it is important that those forms conform with the law, they are of even less legal relevance than a Code. Additionally, their status is merely as an available document. Neither the College of Policing nor NPCC has any power to compel their use across forces whose practices are dictated by their Chief Constables. Experience shows that many forces do not use any national form of DPN.

In short, these clauses should be removed from the Bill and replaced with the ones drafted by OVC with legal advice and which we are clear will give complainants whose data is sought the protections they need and which the police lead on digital download is satisfied will provide the power required by police.

[13] 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.

Appendix

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.

(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.

(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.

(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.

(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).

(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,

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

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

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

The test in law is strict necessity.

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.

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.

conferred by an enactment or rule of law.

How do our proposed clauses 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 Government have used	*(4) Condition B for the exercise of the power in*	Although we have used reasonable

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 relevant information but have failed to define that relevant for a purpose outlined in subsection 2(a) must mean relevant to a reasonable line of enquiry	*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.*	belief here too, this is defined in sub-section 5 below as only 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*	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	*(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*	Our clauses here mirror the strictly necessary for law enforcement provisions in the DPA 2018.

(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 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 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.	*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*	
(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		*(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

power in subsection (1).			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—* *(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*	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 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*	We have extensively defined agreement.

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.*		*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.*	