Response from the Victims' Commissioner, Dame Vera Baird QC, on the Authorised Professional Practice: The extraction of digital data from personal devices consultation

Victims Commissioner

Overview

As Victims' Commissioner for England and wales, although I appreciate this guidance relates to both victims, witnesses and suspects I will limit my comments in this response to reflect the needs of 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 complainants' of rape 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 [1] and through my network of stakeholders, I hear that the CPS will frequently seek this level of material and refusal to submit will result in the case not proceeding to charge. This is highly troubling for victims and ultimately will have a chilling effect on reports as well as having a direct impact on victim attrition.

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

The Northumbria sexual violence complainant's advocacy scheme pilot (SVCAS)[2], which engaged local solicitors to provide legal advice and support to rape complainants in Northumbria primarily related to complainants' Article 8 rights to privacy, 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. As discussed in more detail below, the scheme proved to be useful for all the participants including the Police and CPS and I would urge the College to back it publicly.

Police, complainants and support workers who participated in the scheme[3] expressed concerns about the current situation:

"I think a lot of things are asked for when we, the police in general in the past, not so much now, they just kind of hand it over without questioning it and I don't think that's, that's

[1] Rape survivors and the criminal justice system, Victims' Commissioner, Oct 20 https://victimscommissioner.org.uk/published-reviews/rape-survivors-and-the-criminal-justice-system/

[2] FINAL REPORT: Evaluation of the Sexual Violence Complainants' Advocate Scheme, Dec 20, Olivia Smith & Ellen Daly https://needisclear.files.wordpress.com/2020/11/svca-evaluation-final-report-1.pdf

[3] Ibid.

sometimes the best way. 'Cos there doesn't really seem to be any, there's not any of that for the suspect, let's just say. So I think, you know, we need to have some sort of, some form of protection for the complainant as well." (Police Officer 11)

"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 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)

"I have had conversations with people in that sort of they are, they don't want to give up their phone and that sort of thing. And I know that that's been a bit of a barrier [to reporting]." (Support Worker 1)

"I would have to hand my phone over to the police. I had minimal contact with my abuser - maybe 2 texts - but I was promiscuous with others and knew that I would probably be questioned about that and judged for it." (did not report)

"The first responders were good, however after that the whole process really stressed me out (having my medical records accessed and phone gone through), this had a negative impact on my mental health and felt like a massive intrusion… The impact on my mental health and being signed off work - I almost lost my job… The criminal justice process caused me more harm than good." (reported 2019, withdrew)

The new guidance is an opportunity to re-balance this situation by ensuring victims' Article 8 rights are considered and upheld. This will go a long way to minimising the re-traumatisation many experience in the system and restoring confidence in the police.

This new guidance has been drafted in part in response to the ICO report on digital disclosure[4] and does, make attempts to address some of the concerns raised in that report. However, I remain concerned there are/ have been various pieces of work in this area[5] again triggered by that report and that without a more joined up approach, those on the ground may be at best confused or at worst operating in a contradictory manner. This is of particular concern as it applies to cross-agency working, with the recently consulted upon CPS RASSO[6] guidance, the Attorney General's guidance[7] and this guidance not always well aligned. This should be addressed with urgency.

[4] 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

[5] The Attorney General's disclosure guidelines, the new CPS RASSO guidance, the new interim DPN, the rape review, new powers under consideration for the Police and Public, Courts and Sentencing Bill and accompanying statutory guidance are just a few examples.

[6] https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-overview-and-index-2020-updated-guidance

[7] https://www.gov.uk/government/publications/attorney-generals-guidelines-on-disclosure-2020

I understand the issue of 'consent' in data protection law as raised by the ICO report, and whilst we are less concerned about how it is named it is vital that a complainant's digital devices and the 'specific' sought material within are only accessed when that complainant has given free informed agreement. Where that complainant does not have capacity to agree and thus someone else is asked to agree on their behalf (a parent/ carer etc.) their views are sought and recorded. The NPCC has requested a statutory power which deals with the issues arising from the ICO report with the common law gateway of consent and I anticipate this guidance will form a stop-gap because once that is in place the guidance will need to be re-written.

I am concerned to see mention of warrants being used in the guidance and would argue that such a coercive power should never be used on a victim/ complainant. In fact, the NPCC has been clear that the power in section 19 of PACE should never be used with victims precisely because it is coercive. As mentioned above, the new statutory power should help overcome some of the confusion and provide a clear power upon which the guidance can build.

I believe the steps outlined below would be in accordance with case law[8] and will satisfy the ICO report[9]. They also reflect a draft statutory provision currently being considered for inclusion in the Protection of the Police and Public, Courts and Sentencing Bill:

1. A police officer can if certain conditions are met extract information stored on an electronic device if the user has voluntarily provided the device and agreed to specified information being extracted from it.

2. The conditions are as follows:

    i) The above (1) can only be exercised for preventing, detecting, investigating or prosecuting an offence, locating a missing person or protection of a child or 'at risk' adult from harm.

    ii) The above (1) can only be exercised if the police officer believes that the information stored is relevant (relevant to a reasonable line of enquiry) to one of the above purposes (i) and it is strictly necessary and proportionate to achieve that purpose.

    iii) Where there is a risk that 'other' information i.e. not that information necessary for one of the purposes above (i) the police officer must in order to demonstrate what they are doing is strictly necessary and proportionate and be satisfied that there are no other less intrusive means available.

When I say "consent" or "agreement" in relation to the extraction of information from a user's device I mean a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the extraction of information from the device which has been

[8] Bater-James & Mohammed v R [2020] EWCA Crim 790,
[9] Ibid. 4

specifically identified in the request made to them by an authorised person. Agreement remains freely given in this context if the user is properly advised as to the potential implications of any refusal for a criminal investigation or prosecution if it has implications for compliance with an individual's right to a fair trial.

This is broadly what is set out in your introductory paragraphs to the document:

"The powers to acquire a device are different to those that apply to device. Acquisition of the device would be under common law consent. In most investigative circumstances, officers or staff will be intending to take the device for the purposes of extracting data. Investigators should be considering and explaining the power to acquire the device and the power to acquire the data at the same time, therefore officers and staff should apply both the common law consent to the physical device and DPA 2018 requirements for the data.

Consequently officers and staff will:

- *seek consent for the acquisition of the device*

and

- *believe acquisition of the data to be **strictly necessary** to satisfy a reasonable line of enquiry*

and

- *consider all other less intrusive means and decide that they are not able to provide the evidence in a way that will support the investigation of a reasonable line of enquiry*

and

- *seek informed, freely given permission to acquire the data*

However, I have concerns that the process is not clear, the different powers and legal basis are confused, and the guidance is at times too contradictory and so it is entirely possible officers will stray from this stepped approach and this may lead to regional variation and some bad practice.

I am also concerned this guidance alone will not change the culture which currently sees routine disproportionate downloads. So, whilst it is good to see the 'safety net' of an inspector authorising a download, this is unlikely to bring about the needed culture change. Instead, good practice guidance should ensure that a paper record of the thought process of the officer seeking the data is recorded, so that at each stage of the above conditions the reasoning is recorded and can be scrutinised at a later point.

Finally, I have been unable to view the PSED assessment for this consultation but submit this guidance is likely to disproportionately impact certain groups with protected characteristics under the Equality Act. I would like to see discussion of this in the guidance and mitigating actions.

Questions

1. *Are the guidance principles clear and easy to understand?*

Principle 1 – Strictly necessary and avoiding unnecessary intrusion.

This principal reflects case law[10] and the Attorney General's guidance[11] that there should be no speculative searches and that **specific** material can be sought if it is necessary to serve a reasonable line of enquiry, indeed, the ruling in Bater-James[12] stated that:

"It is not a 'reasonable' line of inquiry if the investigator pursues fanciful or inherently speculative researches…There is no presumption that a complainant's mobile telephone or other devices should be inspected, retained or downloaded." (para.70, 78)

I am pleased to see it reflected in the guidance. However, in practice, as has been well publicised complainants are frequently subject to background trawls which largely focus on their credibility.

A police officer interviewed as part of the Northumbria pilot[13] stated:

"…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." (Case 27, Case Files, emphasis in original)"

Complainants told my survey[14] about this experience, mentioning that they felt 'under investigation' and that they found it hugely intrusive:

"I don't really understand the need to do this, are they trying to ensure I fall under the category of a 'good survivor'? Are they assessing my sexual history and preferences because they know this can be used against a survivor in court? Are they trying to prove I wasn't lying? It felt like the investigation was more about me than the perpetrator at this point! They didn't look at his phone!
Female, White, straight/heterosexual, aged 25 to 34, reported in 2018"

"I felt anxious, confused and infuriated. I was under far deeper investigation than the rapist (who I have no doubt would have had questionable material had they searched the same). They had refused to take physical evidence - my clothing from the night of the attack - but wanted to investigate my private life. I asked them to justify each request but they could not, so I did not provide it.
Female, White, straight/heterosexual, aged 25 to 34, reported in 2017"

[10] Ibid. 8
[11] Ibid. 7
[12] Ibid. 8
[13] Ibid. 2
[14] Ibid. 1

The guidance alone, will not change practice, but it is helpful in setting standards. Most of the terms used, i.e. 'strictly necessary', 'reasonable line of inquiry' etc. are not defined and this will undermine the effectiveness of the guidance.

I hear from stakeholders including police there is a big push from the CPS to the police to obtain as much 'credibility' evidence about the complainant as possible. Some police cannot get the CPS to consider a charge unless there has been a whole phone download (along with non-digital evidence such as medical records not covered by this guidance) without a definition of strict necessity then it is easy to foresee a scenario where everything the CPS demands is 'strictly necessary' for the purposes of the investigation.

This 'relationship' between the police and CPS was well evidenced in the Northumbria pilot[15] with several police recounting the demands they are asked to meet:

> *"In terms of the 3rd party material: I have obtained as much as I need from her phone. I have just received her Local Authority Records from [Council] and I am awaiting her 21 | Page medical records and school records. Once I have reviewed this material, I will be able to go to the CPS for a decision. Unfortunately, as you are no doubt aware, the CPS will not entertain any files for charging decision unless this material is reviewed without exception regardless of the circumstances." (Case 18, Case files)*

> *"We have never asked for anything like that [consent for 3rd party material] in the past… If we don't get 3rd Party information the CPS won't charge any cases." (Case 18, Case files)*

I am troubled that there is no mention of proportionality anywhere in the guidance and this surely is key when considering 'strict necessity'. We would like to see proportionality included as a consideration with clear definitions and examples.

Whilst I accept 'reasonable lines of enquiry' will vary from case to case and that there should be a degree of investigator discretion on what forms a reasonable line in each case, there will be a finite number of common reasonable lines of enquiry in rape cases. I don't wish to be prescriptive but would like to see some examples in the guidance, which would not only serve to clarify what might be considered reasonable and what might not, but which would more importantly provide officers with a clear 'tool' to be able to resist unreasonable requests from the CPS should they arise.

The case of Bater-James[16] provides some solid examples of when it may be reasonable to seek digital data. The court stated: *'there will be cases where there is no requirement for the police to take the media devices of a complainant or others at all…Examples of this would include sexual offences committed opportunistically against strangers, or historic allegations where there is considered to be no prospect that the complainant's phone will retain any material relevant to the period in which the conduct is said to have occurred and/or the*

[15] Ibid. 2
[16] Ibid. 8

complainant through age or other circumstances did not have access to a phone at that time.'

The guidance is contradictory on the point about what will be extracted it states as an overarching principle that '*Only the minimum data that is strictly necessary will be extracted.'* But it also discusses what officers should do where material extracted is not relevant to the search i.e. that it should not be examined and deleted without delay. This, I assume, is because from a technological viewpoint there is a disconnect between a desire to only extract specific material and the technical capability of different forces to achieve this type of very specific download? I believe this issue should be addressed elsewhere as it is predominately a resourcing issue and the guidance should be clear and unequivocal that only specific defined material is sought and downloaded.

I am pleased to see consideration should be given to less intrusive means of obtaining material but if this is to translate to a change in practice, there needs to be clear guidance from the College that this is the 'gold standard' i.e. screen shots over a whole phone download and that police will be backed if and when the CPS insist on whole phone download.

Police have the power under PACE to seize and scrutinise a suspect's phone (when he is under arrest), which is done almost routinely in other offence types such as drug dealing. I am concerned this power is rarely used in rape cases as obtaining and scrutinising a complainant's phone is probably seen as an easier option. Presumably this is because so many suspects are now invited for a voluntary interview which means they are not under arrest and will often attend the station without their phone. A less intrusive (to the complainant) means of obtaining material might be to obtain it from the suspect's phone particularly where the suspect relies on text messages or previous interactions in interview and it is wholly reasonable for police to use a more coercive power in relation to a suspect.

I mention above but reiterate here that the guidance should also advise officers to keep a record of their process in deciding to ask for and obtaining permission for download of material. This should include why it is strictly necessary, proportional and forms a reasonable line of enquiry. Firstly, it will more likely illicit a culture change, as if officers know their decision making can be scrutinised, they are more likely to follow the guidance. Secondly, it will ensure they are having to think about the steps rather than just 'doing what we've always done'. Thirdly, in relation to the relationship with the CPS and cross-agency working, it again provides police a means to resist the wholesale download culture that pervades currently (see quote from Police Officer 10 in the Northumbria pilot under Prinicple 2 below).

Principle 2 – Provision of information & Principle 3 – Requesting permission.

These are heavily interlinked and as such I will discuss them together.

Principle 2 outlines that victims should be given full and clear details of the proposed data extraction. Respondents to our survey[17] reflect that current practice does not adhere to this principle.

"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."

"*I was happy to provide my mobile phone for them to download all the vile messages that supported my assaults. The police said they would download all messages between me and my ex-husband but they actually downloaded all of my phone every message, [G]oogle search and all my privacy was gone.*
Female, White, straight/heterosexual, aged 35 to 44, reported in 2019"

The Northumbria pilot[18] also demonstrates this:

"We weren't getting, not getting informed consent, and we were just asking people to sign bits of paper where they don't really know what we're asking for, and data protection is obviously quite a big thing and we shouldn't really be asking people for consent for things that they don't understand." (Police Officer 13)

"I wish they told me that signing a form to give the police access to my phone meant they would be examining my consensual sexual relationships and sexual history. I didn't realize my relationships with my ex's, how many friends I have, how often I go out, is relevant to being raped by a school teacher." (752, reported 2018, police NFA)

Many victims and witnesses are unclear about the reasons that they are being asked for data and although the new temporary DPN's are a great improvement on previous notices, we think the guidance should be more explicit about what information needs to be provided to a victim.

In addition to the list of information to be provided to victims in the guidance we think the following should also be included:

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

How the extracted information will be kept secure

How the extracted information will or may be used in a criminal process

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

[17] Ibid. 1
[18] Ibid. 2

The circumstances in which a further extraction may be required

What is key here is that agreement is informed which is why it is imperative that victims are told explicitly about what is being sought and why. The best way to ensure informed agreement would be for victims to be given free independent legal advice as per the Northumbria pilot[19] and as such we would like to see the College of Policing supporting this call.

Many of the police involved in that scheme[20] saw the benefit it brought to their process and in terms of being able to push back to the CPS:

"I think that did make a difference, and I think it's a learning curve with it anyway but I definitely think the fact that instead of just doing a blanket application it makes you sit down and look at what's actually going to be relevant a lot more and in detail… Not to protect the complainant but just to assist… It makes you look at your investigation in more depth and actually think well yeah we do need that and we don't need that and I'm not gonna apply for that. And it kind of makes you stand up to the CPS a little bit more, which is not a bad thing, 'cos I think they just want everything, so you've just gotta be able to say no." (Police Officer 10)

I welcome the suggestion victims be provided with an alternative device but additionally it is essential that as much notice as possible is given to victims, so they have opportunity to download sentimental or important material from their phones such as photographs etc. prior to handing the device to police.

In relation to information on the time a phone may be retained for, I welcome police giving an estimate to victims but assert that there should be a check and balance in the form of a formal review process after a specified period of a month, details of which should also be provided to victims.

I welcome the mention of capacity and consideration of trauma. PTSD and severe trauma are commonplace amongst survivors of sexual violence and will often impact their ability to give informed consent to some degree. It is important officers dealing with these complainants are trauma-informed and take appropriate approaches, but I accept this is outside the scope of this guidance. What is vital is that even where capacity is an issue, the views of that person i.e. the victim are still sought. Even if someone is lacking in capacity to give agreement, they may still have a view and their right to refuse should still be given consideration. This applies to children also. It is imperative that due to capacity issues the wishes of a victim are not circumnavigated by police.

Whilst I am pleased to see reference to sensitive processing of sexuality data, the way in which data extraction and potential disclosure relates to sexual history is a vitally important consideration here and needs delineating in the guidance. One example I have heard of is a dating app history being sought by police. This clearly falls into sexual history territory and

[19] Ibid. 2
[20] Ibid. 2

is arguably never appropriate unless it relates very specifically to the suspect. This needs further consideration in the guidance.

Principle 4 – The right to refuse.

It would be useful to see further guidance about what may happen if someone refuses and greater discussion of the exceptions that apply i.e. when data can be extracted even when someone refuses.

I am very concerned to see the suggestion a warrant may be sought in circumstances where a victim refuses. This would override all the checks and balances this guidance and the new DPN's etc. seeks to put in place as such this should be revised. The NPCC advise that a coercive power should never be used on a victim and the guidance should reflect this.

Principle 5 – Deletion of irrelevant material.

As mentioned above, I assert that only specific relevant material should be sought. I understand from an operational perspective there will be variation in technological capability from force to force which will impact the ability of some investigators to be specific in their downloads. However, the principle should still be specificity. This then becomes resourcing issue to ensure that all forces have parity in their ability to scrutinize devices in a specific and targeted manner.

As the current circumstances mean that material will inevitably be downloaded which is non -relevant it should be deleted immediately with only as much scrutiny as is necessary to determine it is non-relevant. However, I would like to know what efforts are being made to update force technology so that victims can be assured that only specific data will be obtained.

In relation to material which evidences criminal activity by victims/ complainants, I am pleased to see the guidance state *'it is unlikely to be proportionate…to investigate references to drug use, when dealing with a victim of serious sexual assault'.* However, I fear discovery of criminal activity such as drug use or of being an immigration over-stayer or someone without legal basis to be here are serious concerns for victims and have a chilling effect on reporting and cause fear in terms of handing over devices. It would be good to see a bit more explicit guidance here on what 'unlikely' means.

Additionally, given that we know that much digital evidence is (inappropriately) used by the CPS to assess the credibility of a complainant, I would like to see more discussion about what uncovering evidence of drug use may otherwise do to the investigation as this would usually mean that a prosecution wouldn't follow. It would be good to see some discussion about how this should not mean that a prosecution cannot continue.

Principle 6 – Safeguarding

I am pleased to see the police should consider how loss of a device could put a victim in a potentially harmful situation and it would be good to see this covered more broadly. For some categories of victim their phone may be a literal life-line to the outside world (current context excepted).

The list of examples 'confidential private information' is odd as it includes both private information like sexuality and criminal offences such as HBA and threats. This is confusing and conflates risk to the victim with privacy issues and needs re-drafting so for example someone subject to HBA may be a safeguarding risk if their phone is taken (and in any event).

Principle 7 – Updating, reviewing and managing.

I welcome reference to victim's being able to retract agreement at any time but the guidance is scant on details about how this is possible or what effect this would have. This needs to be covered in the final version. Additionally, as agreement will be sought on the basis of agreement to specific information being downloaded, the guidance should make clear that further specific agreement for any new lines of enquiry that occur will be needed, if they weren't covered in the original agreement or have arisen at a later point in the investigation.

Principle 9 – Recording actions

Although the guidance mentions logging of agreement from victims it does not go into further detail about how decisions and processes should be logged. As outlined above I would like to see a clear process that is properly recorded in writing.

2. *Are the conditions in the guidance that set out the police procedures governing the taking possession of personal digital devices and extracting the data clear?*

No, not in respect of victims at least, as I have outlined above it should be an iterative process.

Identification of a reasonable line of enquiry, is it strictly necessary and proportionate? Specification of what is sought, obtaining informed agreement from the victim (which includes outlining what is being sought, explaining how it is a reasonable line of enquiry and outlining their rights).

This process should be clear and easy for police to follow and should be evidenced (over and above the DPN).

3. *Is the legal basis under which the police will act clear?*

I do not think it is sufficiently clear or outlined fully enough to be of any meaningful use to officers on the ground. What is being proposed in part to address the concerns of the ICO in their report is a more thoughtful approach to data processing which includes consideration

of different powers in different circumstances and the balancing of different actors' human rights. In order for this to work the different powers need to be properly outlined. There is confusion even within the language used in the guidance with consent and agreement confused in places. I note that there may in due course be a statutory power which will address some of this confusion and at that point this guidance will need to be rewritten.

4. *Do the principles set out the legal safeguards to prevent the unnecessary intrusion into personal and family life?*

There is a lack of exploration of privacy concerns which some groups have raised about the process. I have outlined this below.

The permission of an inspector, although welcome, will not bring about needed culture change and we assert that there should be greater need to document decision making thought processes which can be scrutinised leading to greater accountability.

The distress of victims at intrusion into their privacy is not really well covered here and there is limited reference to their article 8 rights. It is vital this is addressed. This quote from the Northumbria pilot demonstrates that police know that this is important but just hasn't been a consideration in the past:

"I would love to see a document where somebody who has looked at third-party material has actually considered the Article 8 rights of the victim. 'Cos I don't think you'll find that anywhere." (Police Manager 1)

In the ICO report reference is made to the Bank Mellat[21] test as a useful way of assessing intrusion into article 8 rights but it is not referenced here.

5. *Do the principles address concerns of groups who could be unfairly or disproportionately affected by the implementation of this guidance?*

The concerns are not well discussed in the body of the guidance; indeed, they are mentioned almost in passing. It would be far better if the concerns were outlined and then the mitigating provision placed alongside them.

There is no consideration of how certain groups may be disproportionately affected, for example, there is one mention of interpreters under capacity but nothing more, there is no mention of disabled victims and the impact of losing a phone on a victim for whom that may be a life-line to the outside world. There is nothing about black and minoritized people's historic mistrust of police or about immigration concerns which could impact a victim's decision making in this area. This is particularly prudent as the recent super-complaint

[21] Bank Mellat v Her Majesty's Treasury (No 2): SC 19 Jun 2013

report outlines these issues fully and recommended a firewall between police and immigration enforcement[22].

This would help inform force equality impact assessments and give a clear steer as to the types of considerations they should include.

[22] Safe to Share? Report on Liberty and Southall Black Sisters' super-complaint on policing and immigration status, Dec 20,
https://www.gov.uk/government/publications/police-data-sharing-for-immigration-purposes-a-super-complaint