Briefing: Data extraction clauses (Part 2, Chapter 3: Police Crime Sentencing & Courts Bill)

Victims Commissioner

Summary

- Victims of rape are being forced to choose between justice and their right to a private life. Rape victims are facing unjustified demands for downloads of personal data and cases are frequently dropped if victims do not sign over their data.
- Faced with handing over their personal devices and data, many victims drop their complaints, leaving them with no resolution and the public with the risk of a criminal free to offend again, this is a particular risk in sexual offending as research suggests that most offenders do so serially.
- The PCSC Bill affords police and the Crown Prosecution Service (CPS) through the police wide-ranging powers to wholesale access of victim data. Any safeguards for victims are relegated to guidance, which current practice demonstrates is largely ignored.
- These provisions run in the complete opposite direction to the government's end-to-end rape review (E2ERR) and its commitments to victims of rape. If passed in its current state, these clauses are likely to only worsen the situation for victims.

Tabled Amendments

"It is my assertion that the only way to bring about a much-needed change in practice is to ensure that the framework in place to protect victims' Article 8 rights is embedded in the legislation itself." – Dame Vera Baird QC

- The Victims' Commissioner asks you to consider supporting the tabled amendments tabled by Lord Rosser (754 (parliament.uk) pages 21 - 23 (Clause 36.)
- As a further safeguard, victims should be afforded free and independent legal advice to help them assess if information requests are necessary and proportionate to the investigation. The Victims' Commissioner asks you to consider supporting the tabled amendment (754 (parliament.uk) on page 20 (clause 36).
- A detailed briefing is available on my website.

Background

- It has become routine for rape complainants to be asked to hand over excessive personal information. Requests can be in the form of both digital data (from personal devices) and 'third party material' (official records kept by others, including medical records).
- Data requests are frequently disproportionate to the investigation and have had a chilling effect on victim confidence. Refusal of these demands frequently leads to cases being dropped ('no further actioned').
- Guidance and case law prohibit the download of an individual's entire personal history; it is not relevant to a reasonable line of enquiry and is not strictly necessary or proportionate (the 'tests' laid down in 'law').
- The Information Commissioner's Office (ICO) found that demand for this material is principally driven by the Crown Prosecution Service (CPS). The E2ERR references CPS lawyers who *"described 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 will include stranger rapes where this information cannot possibly be said to be relevant to a reasonable line of enquiry.

The current legal framework

- Existing case law, legislation and guidance makes clear that an officer is only entitled to ask for digital data if s/he believes that it is material relevant to a **reasonable line of enquiry**. In the case of Bater-James, judges were clear that this means no speculative searches, and data protection legislation only allows for extraction of specific information insofar as it **is strictly necessary** and **proportionate** for the investigation. The officer must also be satisfied that there are no less intrusive means of getting the information.
- Whilst data protection legislation allows police to access material under the strictly necessary for law enforcement 'gateway', it is vital that victims are asked to agree to the download free of pressure or coercion and that they fully understand what is being sought from them and the implications of providing information.

What led to Government's proposed clauses in the Bill?

- The digital extraction clauses in the PCSC bill were initially sought by police for an entirely separate purpose delineated fully in my longer briefing.
- The Victims' Commissioner (VC) was consulted on draft clauses and raised concerns that this power would also have implications for victims of crime, particularly victims of rape. With agreement from the National Police Chiefs Council (NPCC) and the ICO the Commissioner proposed amendments to the clauses, which the government chose not to incorporate.
- The government asserts that the statutory guidance will ensure safeguards for victims. However, the current safeguards are largely contained in guidance, which has been shown by current practice to be ineffective. In any event, the guidance is without teeth: legislation takes primacy over guidance and the current clauses specifically limit liability for failure to follow the guidance.
- **The power in the bill is wide-ranging and will effectively provide a legal basis for intrusive and excessive download of personal information, with any safeguards for victims of crime relegated to guidance.**

What are the problems with these clauses?

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

- 'Consent/agreement' is often sought by police from complainants of sexual violence in circumstances where they are not fully informed or are being coerced. To safeguard against this and to make clear that agreement means informed and freely given consent, 'agreement' should be defined in legislation.
- Police (and others) need to be specific about what data they are seeking. It is only through specifics that the data owner i.e. victim can give informed consent to extraction.

2 Reasonable line of enquiry

- Without 'reasonable line of enquiry' clearly defined in legislation, the 'legal' hoop for police is merely *reasonably belief* in relevance, which risks embedding a culture of wholesale downloads and intrusion into privacy. Reasonable line of enquiry needs to be clearly defined and an audit trail for the decision-making process should also be mandated, so that decisions can be scrutinised at a later date.

3	**Strict Necessity** • A complainant's personal device can be expected to contain 'sensitive data' within the meaning of the data protection legislation (e.g. health and sexuality data, and/or such information pertaining to others). Statute and case law insist on 'strict necessity' as the only appropriate test in circumstances where sensitive data will be processed. The modifier 'strictly' has been removed from the test, creating a far lower threshold for processing of this type of material than the Data Protection Act intended. This means that victims' Article 8 ECHR rights are less protected.
4	**Reasonably practicable** • The Data Protection Act places a high threshold for processing data in this context: 'strictly necessary for the law enforcement'. In order to comply with the legislation, the police 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 use of the phrase 'reasonably practicable' is a problem both because it is incompatible with data protection legislation and because of concerns that this gives police a means of easily dismissing other options. • The risk for rape victims is that the most practical - or easiest path - to obtaining the information sought will nearly always be the victim's personal device, with limited safeguards for victims.
5	**Other issues** • The authorised person has no obligation to obtain views of children and those without capacity when seeking to obtain information from their phones. A duty to explore their views should be included to safeguard their human rights. It is wholly inappropriate that an unknown adult can give consent in these circumstances – this should be removed. • Immigration officers can be an authorised person under the draft clauses. There is obvious potential for a conflict of interest – this power should not be extended to them. • 'Emotional harm' as a ground for extraction is far too vague and open to wide interpretation. This should be limited to physical and mental harm. • Victims should be granted the option of free and independent legal advice in circumstances where they are required to give consent to police to access their digital data or third-party materials.