Committee Stage Briefing on digital extraction powers in the Police, Crime, Sentencing and Courts Bill

Big Brother Watch, Amnesty International UK, Centre for Women's Justice, defenddigitalme, End Violence Against Women, Fair Trials, JUSTICE, Liberty, Rape Crisis England & Wales, The Survivors' Trust

May 2021

CONTENTS

12th May 2021

Contact: silkie.carlo@bigbrotherwatch.org.uk

Introduction

This Committee Stage briefing concerns Part 2, Chapter 3 of the Police, Crime, Sentencing and Courts Bill: "Extraction of information from electronic devices".

We are concerned that this Chapter of the Bill significantly rolls back vital data, privacy and equality protections our groups have fought to be put in place to better uphold the rights of complainants of rape and sexual offences who report offences to police.

On the whole, this Bill presents some of the most profound and varied threats to human rights in the UK of any Bill introduced for decades, from the right to privacy to the right to freedom of expression and freedom of assembly. We support calls for the Bill to be revoked or voted against in its entirety. However, in this briefing we make a series of vital recommendations for amendments to protect rights and justice, should Part 2 Chapter 3 of the Bill proceed through Committee Stage.

Background

The widespread use of mobile phones and other digital devices in people's everyday lives means we increasingly leave a data trail everywhere we go. Our digital footprints can reveal where we have been and when, who we have spoken to, the content of our private conversations and, via our internet history, even some of our innermost thoughts.

More and more, such data is being sought in criminal investigations. Clearly, data from devices can be highly relevant to investigations, particularly if the offence involves digital communications. But police are seeking masses of personal data by default that is not relevant to an investigation at all, and may not be lawful. Our groups have found that this practice is used almost exclusively in relation to complainants of rape, sexual offences and domestic violence, who are overwhelmingly women. Further, an investigation by Big Brother Watch found that female victims of rape and sexual offences also face demands for digital strip searches more often than male victims.[1]

The scale and depth of the police's mobile phone searches are incomparable with the police's legislative powers to carry out physical searches. It would amount to police searching someone's property and taking copies of all photographs, documents, letters, films, albums, books and files. Some phones can contain over 200,000 messages and over 100,000 photos. [2] This information can run to many thousands of pages. An average individual's mobile phone can contain the equivalent of 35,000 A4 pages of data.[3]

Much of this information is incredibly personal, including private conversations with friends, family members and partners; personal and potentially sensitive photographs and videos; personal notes; financial information; and even legally sensitive work-related information such as in emails. Most people's phones and communications contain sensitive information classed as 'special category data' under data protection law: information about an individual's race,

ethnic origin, politics, religious or philosophical beliefs, health, sex life or sexual orientation, and as such data extraction from phones requires robust safeguards.

These would be intrusive searches even for most suspects of crime. But now, police are carrying out these intrusive digital searches against victims of crime.

In recent years police, pressured by the Crown Prosecution Service, have been demanding victims give blank cheque "consent" allowing access to their digital lives, warning them that the investigation will likely be discontinued if they refuse. The National Police Chiefs' Council (NPCC) formalised a policy for digital extractions in April 2019 in the form of a 'Digital Processing Notice' to be used across England and Wales, and given to individuals where a digital extraction was sought.[4] The Notice specifically stated that more data than necessary may be extracted from the device: "even though we may only consider a limited number of messages relevant to the investigation, the [extraction] tool may obtain all messages." The Notice also stated that, to the extent that the extraction would be specified, it would be specified according to entire categories of data to be extracted from devices: "In order to investigate the crime you are involved in, the police intend to extract the following data categories from the device e.g. call data, messages, email, contacts, applications (apps), internet browsing history etc." Big Brother Watch subsequently published a report in July 2019 titled "Digital Strip Searches: The police's data investigations of victims".[5]

In our experience, these demands are often made in absence of any strong necessity or sometimes even relevance of data that may be on the device. The police use mobile phone extraction tools to download the contents of victims' mobile phones and digital devices. These digital strip searches are not only cruel, invasive and causing major delays to investigations - they breach victims' fundamental rights and obstruct justice. These invasive practices are highly likely to infringe victims' data protection and privacy rights protected by the Data Protection Act and the Human Rights Act.

The searches appear to be driven by a generalised suspicion of complainants, and mobile data trails are increasingly being seen as character references. By analysing victims' digital lives, police attempt to infer "evidence" from information spanning years, analysing what kind of person they are, examining who they have relationships with, and even speculating about their state of mind.

Victims are faced with an impossible choice – the pursuit of justice or the protection of their privacy. No one should be faced with such a choice.

This creeping norm of using data trawls to treat victims like suspects marks a disturbing, radical change within our criminal justice system. Anyone of us could become a victim of a crime and suddenly find our private lives subject to intense digital scrutiny. Those who refuse will be exempt from justice.

Campaign for change

Big Brother Watch initiated a coalition of women's, victims' and rights groups to call for change, namely: Big Brother Watch, Amnesty International, Centre for Women's Justice, End Violence Against Women Coalition, Fawcett Society, JUSTICE, Liberty, Privacy International, Rape Crisis England and Wales, Southall Black Sisters and The Survivors Trust. We called for urgent reform that:

- Protects victims' consent to proportionate data requests and doesn't require a choice between privacy and justice;
- Brings police tech up to date to support proportionate investigations;
- Rejects police fishing expeditions through private data, including by using artificial intelligence.

Over 37,000 people signed Big Brother Watch's petition calling on the police and the Crown Prosecution Service to stop forcing sexual assault survivors to hand in their phones in investigations. 15,000 signatories also sent emails in protest to the NPCC and Minister for Policing.

The Centre for Women's Justice represented two survivors of rape to initiate a legal challenge against the NPCC's April 2019 digital extraction policy, which our groups supported. On our analysis, the digital strip search policy breached the right to privacy protected by Article 8 of the European Convention on Human Rights; the Data Protection Act 2018; and since an equality assessment was not conducted (and women are adversely affected), it failed to uphold the public sector equality duty as required by the Equality Act 2010, and Article 14 (read together with Article 3). The parties engaged in pre-action correspondence and entered Alternative Dispute Resolution.

Bater-James & Anor v R.

In June 2020, the Court of Appeal handed down a judgment in another case involving digital extraction, *Bater-James & Anor v R.*, which was clear that the increasingly default practice of bulk digital extraction is disproportionate and unjustified. The judgment was the first to closely analyse digital extraction practices and therefore we quote it here at length.

The judgment said that digital extraction must not be the default or assumed approach:

> "There is no presumption that a complainant's mobile telephone or other devices should be inspected, retained or downloaded, any more than there is a presumption that investigators will attempt to look through material held in hard copy." [77]

And that lines of inquiry must be specified:

> "There must be a properly identifiable foundation for the inquiry, not mere conjecture or speculation." {77}

And that if there are reasonable lines of inquiry regarding data stored on a device, less intrusive methods than looking at, taking possession of, or extracting data from a device should be considered:

> "Furthermore, as developed below, if there is a reasonable line of enquiry, the investigators should consider whether there are ways of readily accessing the information that do not involve looking at or taking possession of the complainant's mobile telephone or other digital device." [77]

The judgment expanded on alternative methods to digital extraction, including examination of the suspect's phone:

> "If a reasonable line of inquiry is established to examine, for example, communications between a witness and a suspect, there may be a number of ways this can be achieved without the witness having to surrender their electronic device. The loss of such a device for any period of time may itself be an intrusion into their private life, even apart from considerations of privacy with respect to the contents. Thus the investigator will need to consider whether, depending on the apparent live issues, it may be possible to obtain all the relevant communications from the suspect's own mobile telephone or other devices without the need to inspect or download digital items held by the complainant. (...) Consideration should, therefore, be given to whether all the relevant messages or other communications in this context are available on the suspect's digital devices, within the witness's social media accounts or elsewhere, thereby potentially avoiding altogether the need for recourse to the witness's mobile telephone etc." [78, emphasis in original]

> "(...) Instead, putting focussed questions to the witness together with viewing any relevant digitally recorded information, and taking screen shots or making some other suitable record, may meet the needs of the case." [79]

The judgment concluded with a relatively prescriptive set of recommendations about the requirements for a digital extraction policy to be in accordance with the law:

> "In conclusion on the second issue and answering the question: "how should the review of the witness's electronic communications be conducted?", investigators will need to adopt an incremental approach. First, to consider with care the nature and detail of any review that is required, the particular areas that need to be looked at and whether this can happen without recourse to the complainant's mobile telephone or other device. Second, and only if it is necessary to look at the complainant's digital device or devices, a critical question is whether it is sufficient simply to view limited areas (e.g. an identified string of messages/emails or particular postings on social media). In some cases, this will be achieved by simply looking at the relevant material

> and taking screenshots or making some other record, without taking possession of, or copying, the device. Third, if a more extensive enquiry is necessary, the contents of the device should be downloaded with the minimum inconvenience to the complainant and, if possible, it should be returned without any unnecessary delay. If the material is voluminous, consideration should be given to appropriately focussed enquiries using search terms, a process in which the defendant should participate. It may be possible to apply data parameters to any search. Finally, appropriate redactions should be made to any disclosed material to avoid revealing irrelevant personal information."

As well as recommendations about the information that should be provided to the complainant:

> "(...) in particular, there needs to be clarity as to i) the length of time the witness will be without their digital device; and ii) what areas will be looked at following the copying of the contents of the device." [91]

> "In conclusion on the third issue and answering the question: "what reassurance should be provided to the complainant?", the complainant should be told i) that the prosecution will keep him or her informed as to any decisions that are made as to disclosure, including how long the investigators will keep the device; what it is planned to be "extracted" from it by copying; and what thereafter is to be "examined", potentially leading to disclosure; ii) that in any event, any content within the mobile telephone or other device will only be copied or inspected if there is no other appropriate method of discharging the prosecution's disclosure obligations; and iii) material will only be provided to the defence if it meets the strict test for disclosure and it will be served in a suitably redacted form to ensure that personal details or other irrelevant information are not unnecessarily revealed (e.g. photographs, addresses or full telephone numbers)." [92]

Revocation of the NPCC's digital extraction policy

The NPCC's Digital Processing Notice, encapsulating the policy set for digital extractions in England and Wales, was revoked in July 2020. As a result, the two survivors represented by Centre for Women's Justice were able to bring their legal challenge to a resolution.

An interim Digital Processing Notice that, whilst not perfect, better respects complainants' data protection and privacy rights was introduced in September 2020 and remains in place. The forms require far more specificity and necessity of data requested from victims and witnesses and are clearer about their rights in relation to their data. However, the revised policy is not being put into practice effectively by police forces. Many of our groups are still being contacted by distressed complainants of rape and sexual offences who tell us they have been told to hand over their mobile phones for full data extraction after making a report, in absence of any clear necessity, or police will not investigate the offences.

It is clear that a robust, legally binding policy needs to be put in place to protect the rights of victims and survivors of rape, sexual offences and domestic violence, to ensure there are no

unnecessary and harmful obstructions to justice, and to enable offenders to be held to account.

Many of our groups have been involved in an ongoing consultation regarding a permanent replacement policy with the Attorney General's Office, the Home Office, NPCC, and the CPS. However, we are disturbed to find that our recommendations and expertise shared in that process is not reflected in the relevant provisions in this Bill.

Survivors' accounts

Due to the sensitivity of the crimes to which this issue primarily applies, victims and survivors whose lives have been affected by excessive digital extraction are rarely heard. However, we believe it is vital that parliamentarians hear their voices in order to understand the seriousness of inadequate rights protections in relation to digital extraction. We include three cases here.

Anonymous

A woman who reported being violently sexually assaulted had her case dropped because she refused to hand over the entire contents of her mobile phone.

"A few years ago I was violently sexually assaulted by a "friend" on a night out. It was a sustained and sadistic attack that in no way began with consent. I made the incredibly difficult decision to report it to the police because I needed to take power back.

"Even though some time had elapsed between the assault and my reporting of it, there was evidence that the police acknowledged as compelling. Despite this, my case was dropped not because of an unlikely prospect of conviction, but because I refused to hand over my mobile phone to be downloaded in its entirety.

"I consider that request to be a gross violation of my human rights. What is on my phone is private and irrelevant to the crime that was committed."

"The way I have been treated by the Crown Prosecution Service has affected me deeply. In the years of dealing with intrusive requests from the police, such as asking for my counselling or medical records, I have been a shadow of my former self. They would tell me I had to supply this information or they wouldn't pursue my case. I was diagnosed with PTSD, not from the assault but from how I was treated by the authorities after reporting it. Over the course of the investigation, when a new request for deeply personal information would come in, I had panic attacks that resulted in 999 calls.

"Unable to think properly or function for months at a time, I felt betrayed by the people who should have been there to help."

"Imagine your most private thoughts and feelings from counselling held in your phone being seen by anyone, let alone your rapist."

"And imagine having no guarantee about how in the future this data may be used or stored. The decision to have my case dropped was a no-brainer for self-preservation, but I now feel that the requirement to surrender one's data is the same as being raped with impunity.

"The optimism I had at the beginning of this process of "taking power back" has been replaced with a feeling of absolute helplessness. Why would other victims of rape or sexual assault come forward to make complaints knowing all their past emails, messages and photographs, however irrelevant to the case, would be subjected to similar scrutiny under this policy? "[6]

Jane*

Police demanded Jane's mobile phone and personal records after she was raped by a stranger eight years ago, even after identifying the attacker using DNA evidence. She told police she had no contact with the man other than when she was raped, but she was told that unless she gave over her mobile phone, the Crown Prosecution Service might refuse to charge.

"I literally had no idea who the suspect was and it was DNA that linked him to me.

"They asked me at one point whether I had the same mobile phone that I had at the time and I said no. Otherwise they said they would have asked for my phone and wanted my messages.

"I'm sure this is a pretty standard experience. As a victim, you are the one under suspicion. You are the one who has to prove your good character."[7]

Olivia*

Olivia* reported being drugged and then attacked by a group of strangers. Despite being willing to hand over relevant information, police asked for 7 years worth of phone data, and her case was then dropped after she refused.

"The data on my phone stretches back seven years and the police want to download it and keep it on file for a century. My phone documents many of the most personal moments in my life and the thought of strangers combing through it, to try to use it against me, makes me feel like I'm being violated once again."

"This isn't about trying to stop the police from putting together the facts of the case. This isn't about objecting to the police downloading information from the time that it happened. This is about objecting to the police downloading seven years of information that pre- dates the event and therefore has zero relevance."

"I kept trying to ask them if the data that they took could be restricted just to the period of time of relevance to what actually happened, and they said no."

"They told me that if I didn't consent that they may just drop the case and may not proceed with it. They have now dropped the case citing one of the reasons being that I have not handed over seven years of my personal life which is of complete and utter irrelevance to that one night.

"I am willing to hand over the information that is relevant to what happened - I'm not willing to hand over seven years worth of information that is totally and utterly irrelevant."[8]

AMENDMENTS

Amendment to prevent digital extraction by immigration officers

Amendment:

Schedule 3, page 198, line 29, leave out "A person appointed as an immigration officer under paragraph 1 of Schedule 2 to the Immigration Act 1971."

Effect:

This amendment would remove immigration officers from the list of authorised persons who may carry out a digital extraction.

Briefing:

Clause 36 permits an "authorised person" to extract information from electronic devices. "Authorised persons" for these purposes are defined in clause 42 and Schedule 3 and include a police constable, any other member of staff appointed by a chief police officer, an immigration officer or a person engaged to provide services including digital extraction by any other authorised person. As Privacy International wrote:

"Including immigration officers is concerning, as the Bill could potentially lead to misuse of their powers enabling immigration officers to gather and analyse all devices from asylum seekers. As currently drafted, the PCSC Bill can be interpreted to treat all asylum claimants as either witnesses or victims of smuggling to justify the taking of their devices and gathering of all of their data."9

Digital extraction is a particularly serious privacy interference that requires a high bar of necessity to be reached in order to justify the intrusion. Whilst immigration officers may be involved in a case in which digital extraction requests are made, we believe it would be inappropriate for those officers to be conducting the digital extraction. Immigration officers should be removed from the "authorised persons" who are permitted to extract information from electronic devices.

Amendments to define "agreement"

Amendments:

Clause 36, page 28, line 26, after 'person' insert 'and,'

Clause 36, page 28, line 27, insert -

(c) that user has confirmed explicitly and unambiguously in writing that
(i) they agree to provide that device,
(ii) they agree to the extraction of limited data that has been specified to the user from that device,
(iii) they agree in the absence of any inappropriate pressure or coercion.

Clause 36, page 28, line 28, insert subclause 2A -

(2A) In order for an agreement to be made in subsection (1), the user must be provided with -
(a) information about why the extraction is considered strictly necessary, and
(b) information about the reasonable line of enquiry pursued by the authorised person, and
(c) information as to what information stored on the electronic device the authorised person reasonably believes to be relevant to the purpose within subsection (2), and
(d) an explanation of what less intrusive methods to obtain the information referred to in paragraph (c) were considered before the request for extraction was made and why no less intrusive means are possible, and
(e) information as to how the data will or will not be used in accordance with the authorised person's legal obligations, and
(f) information about any potential consequences arising from the user's decision, and
(g) the length of time for which the device may need to be in the possession of the authorised person, and
(h) information about the user's ability to obtain a review of the request for the extraction or information

in writing and in accordance with the code of practice issued pursuant to section 40.

Effect:

These amendments would provide a definition of a user's "agreement" to digital extraction, which relies on the necessary provision of information for an agreement to be made, and for that agreement to be made in writing.

Briefing:

An authorised person can extract information from an electronic device if the user of the device has (a) voluntarily provided it and (b) "agreed to the extraction of information from the

device by an authorised person" (Clause 36 (1)). The language used in this clause deliberately avoids use of the word "consent" to evade the legal rights afforded by the consent process as provided by the Data Protection Act 2018, including the ability to give specified and limited consent to data use and the ability to withdraw consent at any time.

However, the term "agreed" is given no further explanation or definition.

Clause 40 requires the Secretary of State to prepare a code of practice containing guidance about the exercise of digital extraction powers. The code is to be brought into force by statutory instrument, and may be changed from time to time. It is possible that a code will contain further guidance on what constitutes an agreement - but whilst a code will provide important and valuable guidance, it would be inappropriate for it to contain the vital protections and definitions required to safeguard individuals' protected rights. These safeguards, which are absent in the current provisions, are required on the face of the Bill. Further, a failure of an authorised person to act in accordance with the code does not render the person liable to criminal or civil proceedings (Cl. 40(7)). Provisions to protect individuals' privacy rights in the course of digital extraction must be on the face of the Bill rather than a code of practice.

The absence of a definition of an agreement and vagueness of this construct contradicts the Government's stated aim for these provisions – that is to ensure this is a "non-coercive power"10 that provides "additional safeguards (...) needed to protect privacy and to support victims of crime (...)".11 The safeguards are notably absent. We believe this is a grave oversight that risks reinstating a system whereby victims' agreement is not reliably informed, meaningful, or given in the framework of a clearly defined statutory process that allows their rights to be duly protected. A definition of "agreement" is paramount.

Further, the addition of paragraph (h) would notify the user of their right to obtain a review of the request for digital extraction. See below, 'Amendment to permit a user to obtain a review of the request for digital extraction'.

Amendment to remove non-criminal "emotional harm" as a purpose for digital extraction

Amendment

Clause 36, page 28, line 30, after 'physical' insert 'or mental harm'.

Effect

This amendment restricts the non-criminal purposes for which an authorised person may extract digital information to protection from neglect or physical or mental harm, removing the purpose of emotional harm.

Briefing:

Digital information may only be extracted for the purposes of preventing, detecting, investigating or prosecuting crime; to help locate a missing person; or to protect a child or an at-risk adult from neglect or "physical, mental or emotional" harm (Clause 36(2)). The broad concept of "emotional harm" (Cl. 36(2)(c)) is without definition, untethered from the investigation of criminal offences, and as such is open to interpretation and possibly abuse. We recommend that the purpose of "emotional harm" is removed as a legitimate purpose for digital extraction from the Bill.

Amendment to ensure digital extraction is only permitted where strictly necessary

Amendment:

Clause 36, page 29, line 4, after 'power is' insert 'strictly'

Effect:

This amendment would make clear that the necessity test to extract digital information is one of strict necessity.

Briefing:

It is important to make clear on the face of the Bill that the threshold to justify a digital extraction is one of strict necessity. 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. The Bill must make clear that a test of strict necessity applies to digital extraction.

Amendment to ensure less proportionate means than digital extraction are used where possible

Amendment:

Clause 36, page 29, line 17, leave out paragraph (b)

Effect:

This amendment would prevent excessive, disproportionate digital extractions where other more proportionate means are possible.

Briefing:

An authorised person may only extract digital information if the person "reasonably believes that information stored on the electronic device is relevant" to the purpose for which the device is being examined (Cl. 36(5)(a)) and if they are "satisfied" that it is "necessary and proportionate" to achieve that purpose.

If there is a risk of obtaining information other than that which is necessary to achieve the purpose, an explicit proportionality test is set out, creating a threshold that there are no other means of obtaining the information sought which avoid that risk, or that there are such means but it is not "reasonably practicable" to use them. This could mean that the entire contents of a victim's phone could be downloaded if an officer reasonably believes there is information on the device relevant to their investigation of the allegation – a very low and vague bar – if, for example, the police force does not have software capable of specifying and limiting the data extraction, although it may exist (i.e., if it is not reasonably practicable to use more proportionate means). This risks a continuation of the types of practices and justifications around digital strip searches that campaigners have fought to end, and that have been found to be unlawful.

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

The use of less proportionate means was explored at length in the Bater-James & Anor v. R judgment, and nowhere in this judgment was 'practicability' set out as a legitimate reason for excessive privacy intrusion:

" (...) if there is a reasonable line of enquiry, the investigators should consider whether there are ways of readily accessing the information that do not involve looking at or taking possession of the complainant's mobile telephone or other digital device." [77]

This point is critical to protect complainants' privacy and data rights and maintain confidence that their rights are appropriately valued. If less intrusive means of obtaining data are available, they must be used, or the extraction is unlikely to meet the test of strict necessity and proportionality.

Amendment to permit a user to obtain a review of the request for digital extraction

Amendment:

Clause 36, page 29, line 19, insert subsections (8A) to (8C) -

(8A) A user may obtain a review of the strict necessity and proportionality of a proposed agreement referred to in section 36(2A).

(8B) A review of a proposed agreement referred to in section 36(8A) must be conducted by a person listed in Schedule 3 who is independent of the investigation (the 'Reviewer') and returned in writing to the user and authorised person within 30 working days.

(8C) In conducting a review of a proposed agreement, the Reviewer must consult with
(a) the user, which may include representatives appointed by the user,
(b) the authorised person,
(c) the Crown Prosecution Service,
(d) the Information Commissioner's Office,
(e) the Victims' Commissioner, and
(f) such other persons as the Reviewer considers appropriate.

Effect:

The effect of these amendments is to create a mechanism by which to review requests for digital extractions.

Briefing:

We believe a review mechanism is an important process to ensure that the requesting individual has correctly analysed the complex factors of necessity and proportionality, accounting for multiple factors such as less intrusive methods, technical capabilities and the user's legal rights, among others.

At present, if a complainant is met with an unreasonable or excessive request for digital information they have no recourse – they can only comply or refuse, and in the latter case, the

investigation is invariably dropped.12 Further, there is a significant culture change needed in police forces as demonstrated by the continuation of excessive digital extraction requests even after the revocation of the April 2019 Digital Processing Notice and the introduction of the interim policy in September 2020. In order to ensure complainants' rights are protected, they must be able to obtain a review of the request for digital extraction.

Amendment to prevent unknown adults agreeing to extraction on behalf of children and adults without capacity

Amendment:

Clause 37, page 30, line 18, leave out paragraph (b)

Clause 37, page 31, line 12, leave out paragraph (f)

Effect:

These amendments would remove unknown adults from agreeing to extraction on behalf of children and adults without capacity.

Briefing:

Clause 37 provides that a responsible person may agree to digital extraction on behalf of a child (aged under 16) or adult without capacity. Clause 37(3) confers this power a parent, guardian, or if they are not available then "any responsible person who is aged 18 or over other than a relevant authorised person". In the latter case, the parent or guardian need only then be informed of the agreement if the authorised person considers that it is "appropriate to do so" (Cl. 37(5)). This construct deprives vulnerable individuals of adequate protection, effectively allowing any adult to negotiate their privacy and data rights regardless of their relationship to or knowledge of the individual or their complaint. Further, such an entitlement could be easily abused, risking power being unfairly tilted towards those with more power whether investigators or even abusers. It is vital that the ability to agree to an invasion of privacy on a vulnerable person's behalf is only afforded to those in a position of trust, who can be reasonably expected to represent the person's best interests. Only parents, guardians, or a person representing an authority or organisation in the care of the individual, must be able to agree on behalf of children or adults without capacity.

Amendments to limit police possession of a device

Amendments:

Clause 36, page 29, line 25, insert subclause 10A -

(10A) The user may choose to be in the presence of the authorised person during the extraction unless either the user or the authorised person deems it impracticable or inappropriate, in which case an explanation must be set out in writing in the agreement referred to in subsection (1).

Clause 36, page 29, line 25, insert subclause 10B -

(10B) If it is necessary for the authorised person to take possession of the device and extract data in absence of the user, the authorised person must
(a) explain why possession of the device is necessary in the agreement referred to in subsection (1),
(b) retain the device no longer than is strictly necessary,
(c) return the device to the user within 30 working days.

Effects:

These amendments would permit the user to choose whether to be present during the digital extraction, unless deemed impracticable or inappropriate; and create a statutory time limit for the authorised person's retention of the device in the event that it is necessary to take possession of it.

Briefing:

It has been common for police digital extractions to result in lengthy delays to investigations, and for complainants to be left without their phones for months and even years. A Freedom of Information investigation by Big Brother Watch in 2019 found that average wait times for devices to be examined varied across forces from 3 weeks to 5 months.13 However, our groups are also aware of cases where a phone has been retained for over 2 years, as in some cases devices may be retained until the end of criminal proceedings or when the case is closed.

This lengthy retention of devices can take away a lifeline from complainants, who may be in a state or trauma and are likely to be in particular need of social support. It particularly disadvantages poorer complainants who may be unable to replace the device and be made unable to easily communicate, socialise or even work without an electronic device such as a phone or laptop. It could also disadvantage complainants who are reporting an offence without the knowledge of their friends or family as it may be difficult to explain why they no longer have a device such as a phone. As such, the risk of losing possession of a device for a prolonged

period of time will prevent many individuals from pursuing the complaint or even reporting an offence in the first place.

The digital extraction technology available today, including mobile extraction kiosks which are now commonly possessed by police forces, mean that these delays and lengthy retention of devices are not strictly necessary and therefore cannot be justified. It is possible for specified data to be extracted rapidly and we believe that it is paramount that police forces are given the right funding and training to make this capability possible nationwide.

Further, to give complainants reassurance and foster trust, they should be given the option of being present during the digital extraction in the same way that an individual reporting a home invasion or burglary would be present during a search of their home. It is important to remember that complainants agreeing to a digital extraction are assisting police with an investigation of a crime – they are not suspects, in which case the use of an agreement would be unlikely to be appropriate. Police possession of a device constitutes a serious privacy intrusion and must be limited to that which is strictly necessary.

Amendment to ensure affected groups are consulted on the code of practice

Amendment:

Clause 40, page 33, line 36, insert -

(DA) the Welsh Government,
(e) the Victims Commissioner,
(f) 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 36, and

Effect:

This amendment would expand the list of stakeholders the Secretary of State must consult when preparing the code of practice, including those with expertise on victims' experiences in the criminal justice system.

Briefing:

After many years of serious policy failure around digital extraction and half of rape victims dropping their complaints even after the suspect is identified,14 it is clear that consultation with groups and individuals with expertise on these matters is vital to provide critical insights that appear to be consistently missing among policy-makers. We note that a consultation process had begun with some of our groups, but that our recommendations are missing from this Bill. Therefore, a verbal assurance that we will be consulted is likely to be inadequate;

consultation with expert groups should be afforded the importance required by way of inclusion on the face of the Bill. Affected groups must be consulted on the code of practice.

Endnotes

1 Rape cases dropped over digital strip search refusals – Big Brother Watch, 18 June 2020: https://bigbrotherwatch.org.uk/2020/06/rape-cases-dropped-over-digital-strip-search-refusals/

2 NPCC and CPS evidence to the Justice Committee Inquiry into Disclosure in Criminal Cases (http://data.parliament. uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in- criminal-cases/written/80778.pdf)

3 Office of the Police and Crime Commissioner Northumbria, Written evidence to the Justice Committee, 24 April 2018 (data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/ disclosure-of-evidence-in-criminal-cases/written/80665.pdf)

4 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 [no longer available online]

5 Digital Strip Searches: The police's data investigations of victims – Big Brother Watch, July 2019: https://bigbrotherwatch.org.uk/wp-content/uploads/2019/07/Digital-Strip-Searches-Final.pdf

6 https://www.theguardian.com/commentisfree/2019/apr/29/sexual-assault-case-dropped-refused-police- phone-rape

7 https://www.independent.co.uk/news/uk/crime/rape-victims-phones-medical-records-met-police- cps-a8949636.html

8 https://www.lbc.co.uk/radio/presenters/eddie-mair/rape-victim-says-complaint-dropped-phone-data/

9 The new Policing Bill fails to provide sufficient safeguards around extraction of victims' data – Privacy International, 17th March 2021: https://privacyinternational.org/news-analysis/4465/new-policing-bill-fails-provide-sufficient-safeguards-around-extraction-victims

10 Police, Crime, Sentencing and Courts Bill: Explanatory Notes - Home Office, Ministry of Justice and Department for Transport, 9th March 2021, p.13: https://publications.parliament.uk/pa/bills/cbill/58-01/0268/en/200268en.pdf

11 Police, Crime, Sentencing and Courts Bill 2021: data extraction factsheet – Home Office, updated 16th April 2021: https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-data-extraction-factsheet

12 Rape cases dropped over digital strip search refusals – Big Brother Watch, 18 June 2020: https://bigbrotherwatch.org.uk/2020/06/rape-cases-dropped-over-digital-strip-search-refusals/

13 Digital Strip Searches: The police's data investigations of victims – Big Brother Watch, July 2019, p.18: https://bigbrotherwatch.org.uk/wp-content/uploads/2019/07/Digital-Strip-Searches-Final.pdf

14 Half of rape victims drop out of cases even after suspect is identified – Owen Bowcott and Caelainn Barr, the Guardian, 10th November 2019: https://www.theguardian.com/society/2019/nov/10/half-of-victims-drop-out-of-cases-even-after-suspect-is-identified