PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

POLICE, CRIME, SENTENCING AND COURTS BILL

Seventh Sitting

Thursday 27 May 2021

(Morning)

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Monday 31 May 2021

The Committee consisted of the following Members:

Chairs: † Steve McCabe, Sir Charles Walker

† Anderson, Lee *(Ashfield)* (Con)
† Atkins, Victoria *(Parliamentary Under-Secretary of State for the Home Department)*
† Baillie, Siobhan *(Stroud)* (Con)
† Champion, Sarah *(Rotherham)* (Lab)
† Charalambous, Bambos *(Enfield, Southgate)* (Lab)
† Clarkson, Chris *(Heywood and Middleton)* (Con)
† Cunningham, Alex *(Stockton North)* (Lab)
Dorans, Allan *(Ayr, Carrick and Cumnock)* (SNP)
† Eagle, Maria *(Garston and Halewood)* (Lab)
† Goodwill, Mr Robert *(Scarborough and Whitby)* (Con)
† Higginbotham, Antony *(Burnley)* (Con)
† Jones, Sarah *(Croydon Central)* (Lab)
† Levy, Ian *(Blyth Valley)* (Con)
† Philp, Chris *(Parliamentary Under-Secretary of State for the Home Department)*
† Pursglove, Tom *(Corby)* (Con)
Wheeler, Mrs Heather *(South Derbyshire)* (Con)
† Williams, Hywel *(Arfon)* (PC)

Huw Yardley, Sarah Thatcher, *Committee Clerks*

† attended the Committee

Public Bill Committee

Thursday 27 May 2021

(Morning)

[Steve McCabe *in the Chair*]

Police, Crime, Sentencing and Courts Bill

11.30 am

The Chair: Good morning. Before we begin, there are a few preliminaries. Can you switch your phones and electronic devices to silent please? The Speaker does not permit food or drink to be consumed during Committee. Please make sure you are observing social distancing and sitting in the appropriate places as marked. People should wear face masks when they are not speaking, unless they are medically exempt. *Hansard* would be grateful if you could email your speaking notes.

We will now resume line-by-line consideration of the Bill. The selection list for today's sitting is available in the room. I remind Members wishing to press a grouped amendment or new clause to a Division that they should indicate that intention when speaking to their amendment. The temperature is wonderful in here, so feel free to remove your jacket if you so wish.

Clause 23

Duty to arrange a review

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss clauses 24 to 35 stand part.

Sarah Jones (Croydon Central) (Lab): It is a pleasure to be back here today. Before I get into the detail of the clauses, I want to put some questions to the Minister, to reflect on the importance of reviews when there have been homicides or unexplained deaths and to give an example.

I was reading the serious case review about Child Q, who was aged 16 when he died following a moped crash. One might think, "There's a child who died following a moped crash. End of story." but because he was a vulnerable adolescent there was a comprehensive serious case review into his life, his death and what happened.

At the time of his death, he was a looked-after child in children's services and was living in the midlands with members of his extended family. On the day of the collision, he had been released on conditional bail from a remand court for breach of his court order. Family members and professionals had requested that he be made the subject of a curfew and tagging, but that, for whatever reason, was not put in place and he returned to London, where the fatal accident occurred.

He started his life as an aspirational boy and had wanted to be a professional footballer. His first conviction ended those aspirations and the motivation to play football. Throughout his life he lived with various family members and foster carers. He was often missing and was both a victim and a perpetrator of various offences. He was involved in high-risk behaviour and believed to be a gang member. When interventions were made, he appeared to understand that his life was very high risk, but seemed almost resigned to the inevitable risks that he was facing. During the latter stages of professional involvement, Child Q asked the professionals, "Where were you when I was six?"

This 16-year-old died because of a moped crash, but because of this review we can learn that bail conditions and tagging would have helped him to make the decision not to travel to London. We have learned that this child was in and out of care and often went missing, that interventions were not made and that the problems started very early. Although that could not in itself have prevented that death, there is a story behind that child that we can learn from.

Sarah Champion (Rotherham) (Lab): My hon. Friend may not know that I used to run a children's hospice. Child deaths are very rare, but a review such as this enables the family to have the closure that they need to move on, enables the lessons to be learned and enables the whole community to grieve and draw a line under something. Of course it is important to understand the failings that occurred so that they never happen again, but also in the broader context, conducting a review is a really important thing to do. In terms of costs and resources, these deaths are not that common; this does not happen that often, but when it does, it destroys a community, not to mention the family.

Sarah Jones: I thank my hon. Friend for that intervention. She speaks with great experience, and she is absolutely right: doing these reviews has wider benefits. Reading the review on Child Q and hearing the stories from the father, mother and family members about him, we can see, hopefully, some form of the beginnings of closure from the review. Therefore we are very much in favour of extending homicide reviews in the way provided for under the Bill. We have some amendments, but they come later, so I will not speak to them now.

To do the victims and their families and friends justice, we need to ensure that the lessons are learned. Part 2, chapter 2 of the Bill will require police, local authorities and clinical commissioning groups to conduct offensive weapon homicide reviews when an adult's death involves the use of an offensive weapon. Police recorded 625 homicide offences in the year ending December 2020. Of all homicides recorded in the last year—the latest year that we have information for—37% were knife-enabled crimes. A large proportion of homicides involve offensive weapons. In the year ending March 2020, 275 homicides involved a sharp instrument, 49 involved a blunt instrument and 30 were homicides involving shooting. It is therefore absolutely right that the Government look to learn the lessons from those homicides not currently reviewed by multi-agency partners.

In my constituency, there have been incidents in which adults have been killed and an offensive weapon was involved. In one instance, there were incidents in the same area within weeks of each other. Those cases were not linked together, but actually, when people looked into the background and how those murders occurred, it turned out that they were linked.

It is therefore important that the pathways that lead people to be involved in homicides, whether as victims or perpetrators, can be understood and the knowledge

can be shared. Offensive weapon homicide reviews will be similar to the domestic homicide reviews that already take place. Domestic homicide reviews are carried out when someone over the age of 16 dies as a result of domestic violence, abuse or neglect. The Government have committed to taking action to address homicide, but have not previously committed to introducing offensive weapon homicide reviews specifically.

Clause 23 will require an offensive weapon homicide review to be carried out when a qualifying homicide has taken place. A qualifying homicide occurs when an adult's death or the circumstances or history of the person who has died meet conditions set by the Secretary of State in regulations. In accordance with clause 27, the purpose will be to identify lessons to learn from the death and to decide on actions to take in response to those lessons.

Clauses 24 to 35 do a number of things, including giving the Secretary of State the power to specify the relevant review partners in regulations and which of the listed public bodies will need to carry out the review in these circumstances, and to clarify when offensive weapon homicide reviews do not need to be carried out. Importantly, review partners must report on the outcome of their review to the Secretary of State. In addition, there are other key regulations about the obligations of offensive weapon homicide review partners.

Clause 33 is important, as it will require offensive weapon homicide reviews to be piloted before they are brought into force. The Secretary of State will be required to report to Parliament on the pilot. It is vital that offensive weapon homicide reviews are piloted before being rolled out nationally, but the provisions are fairly light on detail. It would be helpful if the Minister could provide any further information on the piloting. Can she clarify how many local authorities or police forces they will work with to pilot the reviews?

Standing Together, a domestic abuse charity, recently reviewed domestic homicide review processes in London boroughs. Its 2019 report identified several areas for improvement, including how domestic homicide reviews are stored and retrieved, how chairs are appointed, and how appropriate funding is secured. It also highlighted that not enough sharing of knowledge is happening.

We are glad that the pilot partners will report on these reviews before they are implemented, but could the Minister explain in a bit more detail what those reports will include? Will there be regular reporting and evaluation of these offensive weapons homicide reviews once they are implemented? Where there is an overlap, and a homicide fits into two different categories—for example, if there is a domestic homicide review and an offensive weapons homicide review—how will the lessons be learned? Will there be two reviews, or just one? I am also keen to hear how the lessons from all existing homicide reviews can be better understood and shared between partners to ultimately make our streets safer and save lives.

The Secretary of State is given the power to make regulations on offensive weapons homicide reviews, to provide information on how to identify which local services are relevant to the review and how local services can negotiate who carries out the review when the circumstances are not clear. This is defined in regulatory powers, not on the face of the Bill; perhaps the Minister could explain why, and also explain what her expected timeframe is for these powers. If the duty to conduct these reviews will not be carried out until the criteria are defined in regulation, will there be a delay? What period of time is the Minister expecting that to be—because those regulations will need to go through Parliament—and what will happen after the regulations are published? Can she provide any data on how many more homicide reviews this change will actually bring; what expected number of reviews will need to be undertaken? Finally, what are the plans for budgets to cover local safeguarding partners' costs for the delivery of these reviews? That question was raised in evidence from the Local Government Association, so will the Home Office be submitting a case to increase the funding for local authorities? If not, how does it envisage that these reviews will be funded? I will leave it there.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): It continues to be a pleasure to serve under your chairmanship, Mr McCabe. I am very grateful to the hon. Member for Croydon Central for setting out some of the background to these clauses. Through the clauses relating to offensive weapons homicide reviews, we want to tackle the growing proportion of homicides that involve offensive weapons, for all the reasons that one can imagine: for communities, and for the families affected. As the hon. Lady has set out, there is at the moment no legal requirement to review such homicides unless they are already subject to review: if, for example, the victim is a child or a vulnerable adult, or the homicide has happened in a domestic setting. As such, we want to introduce these offensive weapons homicide reviews to ensure that local agencies consider the circumstances of both victims and perpetrators, and identify lessons from these homicides that could help prevent future deaths.

Taking a step back and looking at the Bill as a whole, this work will form part of the local authorities' work on the serious violence duties. I hope there will be much cross-learning between those duties and the homicide reviews that may occur in local areas, as part of a joined-up approach to tackling such homicides. All persons, bodies and organisations with information relevant to the decision to conduct a review or to identifying lessons, such as schools and probation services, will be legally required to provide information deemed relevant to the review.

The hon. Member for Croydon Central has understandably asked where these reviews fit in with existing homicide reviews: child death and adult safeguarding reviews in England, and their equivalents in Wales, as well as domestic homicide reviews. To avoid duplication of work, the Bill provides that these new offensive weapons homicide reviews will be required only where there is not an existing statutory requirement to review the homicide, which I hope answers her question.

11.45 am

Existing reviews can also take place in certain cases where a death was caused by a person receiving or who had received mental health care, so the Bill provides powers to disapply the duty to conduct an offensive weapons homicide review in such cases.

We want to ensure that these reviews have the most effective impact on tackling homicide, so we anticipate developing a review process that is swift and does not

place an undue burden on partners, but that is also robust and produces meaningful recommendations that can be shared and acted upon to save lives. We want to co-design the process with local partners to ensure that we take account of the expertise and experience of those who will be required to deliver and act on the reviews, and to ensure that they address the limitations of existing homicide reviews.

Again, we want to provide the legal framework for these reviews in the Bill, but we are very much in listening mode, and we want to work and collaborate with local agencies to ensure that the reviews are as effective as possible. To that end, the Committee will notice that the Bill includes regulation-making powers to define in greater detail how the reviews will work in practice. That enables us to agree the details and processes at the design stage, and to give effect to them in secondary legislation. The regulations will be dealt with by way of affirmative procedure, so the scrutiny of the House will be necessary and indeed welcome.

Although it is not covered in the Bill itself, it may be helpful to outline the role that the Home Office will play in overseeing these reviews. We are mindful that recommendations in the reports of existing reviews are not always acted on or given the attention they deserve. There may be many reasons for that, but we want to ensure that the recommendations from offensive weapons homicide reviews are properly shared, considered, debated and—where appropriate—implemented, locally and nationally, in England and Wales.

We will therefore establish a new Home Office homicide oversight board to oversee the introduction of the offensive weapons homicide reviews, to monitor and implement any of the findings, and to support dissemination, both locally and nationally. More information on this board will be provided in due course.

Maria Eagle (Garston and Halewood) (Lab): Given that the Minister is determined to learn the lessons of these reviews and given the importance of properly funding local agencies to carry out any such improvements, can she confirm today that additional resource will go along with this additional focus from the Home Office on implementation?

Victoria Atkins: I am very pleased to confirm that the Home Office will provide funding for the relevant review partners to cover the costs of the reviews during the pilot stage, and will meet the cost of the Home Office homicide oversight board. If the policy is rolled out nationally, funding arrangements will be confirmed after the pilot, but in that initial period that is certainly the approach.

I am trying to see whether I have further details about the pilots that I can assist the Committee with. Clause 33 requires that a pilot of the reviews takes place for one or more purpose, or in at least one area. We intend to pilot reviews in at least three areas and are currently in discussions to enable that to happen. We will announce the pilot areas in due course. We want to pilot the reviews in areas that have high levels of homicide and in areas that have low levels, and that represent regions in both England and Wales.

We will also specify in regulations the length of time that the pilot will last. We currently intend to run the pilot for 18 months to ensure that the review process can be tested properly in each of the pilot areas, but clause 23 allows us to extend the length of the pilot for a further period, which may be useful if further test cases are needed. Our approach is to ensure that the pilot provides us with the greatest insight and information as to how the reviews would work if we roll them out across the whole of England and Wales. In the interests of transparency, clause 33 also requires the Secretary of State to lay before Parliament a report on the operation of the pilot before the reviews can come fully into force across England and Wales.

Question put and agreed to.

Clause 23 accordingly ordered to stand part of the Bill.

Clauses 24 to 35 ordered to stand part of the Bill.

Clause 36

Extraction of information from electronic devices: investigations of crime etc

Sarah Jones: I beg to move amendment 94, in clause 36, page 29, line 5, at end insert—

"(c) the user who has given agreement under subsection (1)(b) was offered free independent legal advice on issues relating to their human rights before that agreement was given."

This amendment would ensure that users of electronic devices were offered free independent legal advice before information on their device could be accessed.

The Chair: With this it will be convenient to discuss the following:

Clause 36 stand part.

Government amendment 63.

Clauses 37 to 42 stand part.

Amendment 115, in 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."

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

That schedule 3 be the Third schedule to the Bill.

New clause 49—*Extraction of information from electronic devices—*

"(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.

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

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

(b) helping to locate a missing person, or

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

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

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

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

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

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

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

(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.

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

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

(8) Condition D is that an authorised person must have regard to the code of practice for the time being in force under section [Code of practice] in accordance with section [Effect of code of practice] below.

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

(10) In this section and section [Application of section [Extraction of information from electronic devices] to children and adults without capacity]—

'adult' means a person aged 18 or over;

'authorised person' means a person specified in subsection (1) of section [Application of section [Extraction of information from electronic devices] to children and adults without capacity] (subject to subsection (2) of that section);

'child' means a person aged under 18;

'agreement' means that the user has confirmed explicitly and unambiguously in writing that they agree—

(a) to provide their device, and

(b) to 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 section [Effect of code of practice], the user—

(a) 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);

(b) has been provided with appropriate information as to (a) how the data will or will not be used in accordance with the authorized person's legal obligations and (b) any potential consequences arising from their decision;

(c) 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.

(11) References in this section and sections [Application of section [Extraction of information from electronic devices] to children and adults without capacity] to the extraction of information include its reproduction in any form.

(12) This section is subject to sections [Application of section [Extraction of information from electronic devices] to children and adults without capacity] and [Application of section [Extraction of information from electronic devices] where user has died etc]."

New clause 50—*Application of section [Extraction of information from electronic devices] to children and adults without capacity*—

"(1) A child is not to be treated for the purposes of subsection (1) of section [Extraction of information from electronic devices] as being capable of—

(a) voluntarily providing an electronic device to an authorised person for those purposes, or

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

(2) If a child is a user of an electronic device, a person who is not a user of the device but is listed in subsection (3) may—

(a) voluntarily provide the device to an authorised person for the purposes of subsection (1) of section [Extraction of information from electronic devices], and

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

(3) The persons mentioned in subsection (2) are—

(a) the child's parent or guardian or, if the child is in the care of a relevant authority or voluntary organisation, a person representing that authority or organisation,

(b) a registered social worker, or

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

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

(5) An adult without capacity is not to be treated for the purposes of section [Extraction of information from electronic devices] as being capable of—

(a) voluntarily providing an electronic device to an authorised person for those purposes, or

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

(6) If a user of an electronic device is an adult without capacity, a person who is not a user of the device but is listed in subsection (7) may—

(a) voluntarily provide the device to an authorised person for the purposes of subsection (1) of section [Extraction of information from electronic devices], and

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

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

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

(b) a registered social worker,

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

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

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

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

(a) voluntarily providing the device to an authorised person for the purposes of subsection (1) of section [Extraction of information from electronic devices], or

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

(10) In this section and section and [Application of section [Extraction of information from electronic devices] where user has died etc]—

'adult without capacity' means an adult who, by reason of any impairment of their physical or mental condition, is incapable of making decisions for the purposes of subsection (1) of section [Extraction of information from electronic devices];

'local authority'—

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

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

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

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

(a) Social Work England,

(b) the Care Council for Wales,

(c) the Scottish Social Services Council, or

(d) the Northern Ireland Social Care Council;

'relevant authority'—

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

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

'voluntary organisation'—

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

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

(11) Subsections (10) and (11) of section [Extraction of information from electronic devices] also contain definitions for the purposes of this section."

New clause 51—*Application of section [Extraction of information from electronic devices] where user has died etc*—

"(1) If any of conditions A to C is met, an authorised person may exercise the power in subsection (1) of section [Extraction of information from electronic devices] to extract information stored on an electronic device from that device even though—

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

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

(2) Condition A is that—

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

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

(3) Condition B is that—

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

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

(4) Condition C is that—

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

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

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

(5) The exercise of the power in subsection (1) of section [Extraction of information from electronic devices] by virtue of this section is subject to subsections (2) to (8) of that section.

(6) Subsections (10) and (11) of section [Extraction of information from electronic devices] and subsection (9) of section [Application of section [Extraction of information from electronic devices] to children and adults without capacity] contain definitions for the purposes of this section."

New clause 52—*Code of practice*—

"(1) The Secretary of State must prepare a code of practice containing guidance about the exercise of the power in subsection (1) of section [Extraction of information from electronic devices].

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

(a) the Information Commissioner,

(b) the Scottish Ministers,

(c) the Welsh Government,

(d) the Department of Justice in Northern Ireland,

(e) the Victims Commissioner,

(f) the Domestic Abuse Commissioner,

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

(h) persons who appear to the Secretary of State to represent the interests of victims, witnesses and other individuals likely to be affected by the use of the power granted in subsection (1) of section [Extraction of information from electronic devices], and

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

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

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

(5) The code must address, amongst other matters—

(a) the procedure by which an authorised person must obtain and record confirmation that a device has been provided voluntarily;

(b) the procedure by which an authorised person must obtain and record confirmation that agreement has been provided for the extraction of specified information, including the information which must be provided to the user about—

(i) how long the device will be retained;

(ii) what specific information is to be extracted from the device and why, including the identification of the reasonable line of enquiry to be pursued and the scope of information which will be extracted, reviewed and/or retained;

(iii) how the extracted information will be kept secure;

(iv) how the extracted information will or may be used in a criminal process;

(v) how they can be kept informed about who their information is to be shared with and the use of their information in the criminal process;

(vi) their right to refuse to agree to provide their device and/or to the proposed extraction in whole or in part and the potential consequences of that refusal; and

(vii) the circumstances in which a further extraction may be required, and what will happen to the information after the case has been considered;

(c) the different types of extraction processes available, and the parameters which should be considered in defining the scope of any proposed extraction from a user's device;

(d) the circumstances in which the extraction of information should and should not be considered strictly necessary and proportionate;

(e) the considerations to be taken into account in determining whether there are less intrusive alternatives available to extraction for the purposes of subsection (7) of section [Extraction of information from electronic devices];

(f) the process by which the authorised person should identify and delete data which is not responsive to a reasonable line of enquiry and/or has been assessed as not relevant to the purposes for which the extraction was conducted; and

(g) the records which must be maintained documenting for each extraction or proposed extraction, including—

(i) the specific information to be extracted;

(ii) the reasonable lines of enquiry pursued;

(iii) the basis upon which the extraction is considered strictly necessary, including any alternatives considered and why they were not pursued;

(iv) confirmation that appropriate information was provided to the user and, if applicable, agreement obtained;

(v) the reasons why the user was not willing to agree to a proposed extraction.

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

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

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

New clause 53—*Effect of code of practice*—

"(1) An authorised person must in the exercise of the power granted under section [Extraction of information from electronic devices] have regard to the code of practice issued under section [Code of practice] in deciding whether to exercise, or in the exercise of that power.

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

(3) A code of practice in force at any time under section [Code of practice] shall be admissible in evidence in any criminal or civil proceedings.

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

Sarah Jones: As more and more crimes take place online or are enabled through digital devices and the internet, the extraction of information from electronic devices has increasingly become a routine part of criminal investigations, but the way in which such information can be made available to law enforcement, prosecutors and the defence has rightly received a great deal of attention and scrutiny in recent years, particularly in rape cases. It has become the norm for rape complainants to be asked to hand over digital devices and for most or all of the material to be checked through in detail. The Victims' Commissioner said in her excellent evidence to the Committee last week that, through her recent survey of rape complainants and her network of stakeholders, she had heard that

"the CPS frequently seeks a level of material straight away, before it charges, and if a complainant refuses, the case just does not get considered for charge. That is very, very troubling, and it has a chilling effect not only on current victims, but on reporting, and it could impact victim attrition."—[*Official Report, Police, Crime, Sentencing and Courts Public Bill Committee,* 20 May 2021; c. 110, Q174.]

I will give some examples that have come to light and that reflect many people's experience. These are the words of Courtney:

"After a two-and-a-half-year investigation into my sexual assault case, which had witnesses and a potential second victim, the police told me the CPS was going to drop my case if I didn't give them a download of my phone. When I asked them what was the reasonable line of inquiry, they told me that I could be lying. There could be something that discredits me on there. I could be hiding something. And to me, that's not reasonable. I was asked why I was concerned, but actually it's totally rational to fear giving your phone over to the police. I think most people would not want to give the contents of their phone to their mother"—

I certainly would not—

"let alone the government or the person who attacked them who may, because of rules around disclosure, get access to it. When I refused my case was immediately dropped.

The CPS turned its back on me and treated me as a suspect—they made it so clear that I was alone and I was powerless. That anyone can rape me with impunity unless I submit to the court's illegal demands.

And it became clear to me that I needed to work to change that, because it can't go on. I had my power taken away from me from the assault, I had my power taken away from me from the criminal justice system. I was left in a really bad place. There were times, you know, I didn't want to be here anymore. But taking up this case, working with the Centre for Women's Justice, it's been so important for my mental wellbeing. I feel like, for the first time in a while, I'm coming to terms with everything that happened to me."

A woman who was raped by a stranger in London told *The Independent* newspaper that she dropped her case after the police demanded access to her mobile phone. She said:

"It made me very angry, it made me feel like I was the one on trial and they were trying to seek out ways it was my fault."

She added that she was concerned that evidence of past one-night stands could be used against her in court. Another woman who faced the same demand after the Metropolitan police had identified her attacker using DNA told that paper that the investigation felt like "one intrusion after another". She said:

"I'm not actually sure I would have gone ahead with the case if I'd known what was part of the process."

In another case, the CPS demanded to search the phone of a 12-year-old rape victim despite the fact that the perpetrator had admitted the crime. The case was delayed for months as a result. Finally, a different woman

[Sarah Jones]

reported being drugged and then attacked by a group of strangers, but the case was dropped after she refused to hand over seven years of phone data.

Analysis of a rape crisis administrative dataset conducted by the office of the Victims' Commissioner showed that one in five victims withdrew complaints at least in part because of disclosure and privacy concerns. Victims in 21% of cases had concerns about digital downloads, about disclosing GP, hospital, school and employment records, and about a combination of negative press coverage. Home Office data also shows an increase in pre-charge withdrawal of rape complaints. In the year ending December 2020, 42.8% of rape offences were closed as part of what is called the "evidential difficulties" category—where the victim did not support further police action against a suspect—compared with 25.6% in 2015. As we know, the charge rate for sexual offences is just 3.6%, and for rape it is 1.6%.

Such stark figures will not help with the concerns of many senior police chiefs that there has been a fall in public and victim confidence in the police in relation to rape cases, in particular. The issue of digital data extraction plays a big role in that, which is why we have tabled amendments. I am sure the Minister will say that clause 36 is required to tidy up the law so that it is clear about what the police can and cannot do, but with our amendments we are seeking to define and improve the rights of victims so that it is clearer to them when data should and should not be extracted.

Amendment 94 would ensure that users of electronic devices are offered free, independent legal advice before information on their device could be accessed, and it was recommended by the Victims' Commissioner. It is vital that victims understand their rights so that they can make an informed decision on whether to agree to handing over their device for digital download.

Sarah Champion: I can only speak from my constituency experience, but many women have come to me having gone to report offences against them in childhood or rape offences against them. They are not in a position to give consent; they are not even in a position to understand what is going on—they are in a highly traumatised state. Walking into a police station is a very shocking thing. They go up to the front desk, get a meeting—one hopes—with an officer, and they are then told to hand over their phones or the police cannot proceed. Will my hon. Friend comment on that inherent power imbalance and the vulnerability of people in that situation—they were all women in those cases—who are expected to make an informed choice?

Sarah Jones: My hon. Friend makes an excellent point about that power imbalance. I have not been in that situation myself, but I can only imagine the bravery that it would take for someone just to take those first steps into a police station and recount what has happened to them, given how awful that would make them feel, let alone potentially handing over everything on their phones.

We were all watching Dominic Cummings yesterday—well, some of us were. [*Interruption.*] Whatever we think of him, right or wrong, he commented, "Well, I would not just hand my phone over so you could look, just to fish to see if there was anything on it that you thought might be relevant." It is the same situation here. If people have past sexual history, which most people have, the idea that that would be used against someone in that vulnerable position—

Maria Eagle: My hon. Friend referred to a fishing expedition. Generally speaking in the criminal law, fishing expeditions are not encouraged, and court rules generally seek to discourage them and to prevent information gathered in that way from being used at trial. Is this any different?

12 noon

Sarah Jones: That is completely right and why we think that having some advice would help in both directions. It would help be clear about when a phone should or should not be handed over, but it would also hopefully help give people confidence when handing it over is the right thing to do, because it is reasonable and proportionate for the police to ask for it, for whatever reason they have given. We hope that that legal advice and support at that stage would help stop anything from being just a fishing expedition, while also giving people confidence to hand over their phones when that is the appropriate thing to do.

I am grateful to the Home Office for funding a pilot of independent legal advice for rape complainants dealing with digital download in Northumbria. The Sexual Violence Complainants' Advocate scheme pilot engaged local solicitors to provide legal advice and support to rape complainants in Northumbria, related to the complainants' article 8 rights to privacy. The pilot demonstrated what was happening in practice and found that about 50% of requests were not strictly necessary or proportionate. Some police officers who participated in the scheme expressed concern about this culture. One said:

"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."

They go on:

"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 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."

Another contributor said:

"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."

Furthermore, another said:

"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 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."

Sarah Champion: I think we all—well, most of us—got a fantastic briefing from Big Brother Watch, Amnesty, End Violence Against Women and so on. Within that, they refer to these things as digital strip searches, which tend to be carried out more often on women than men.

Perhaps I can read something out and ask for my hon. Friend's opinion:

"The scale and depth of the police's mobile phone searches are incomparable with the police's legislative powers to carry out physical searches."

An average phone

"would amount to police searching someone's property and taking copies of all photographs, documents, letters, films, albums, books and files."

Furthermore, some

"phones can contain over 200,000 messages and over 100,000 photos",

and the 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."

Will my hon. Friend, and indeed the Minister when she speaks, comment, first, on the relevance of that; secondly, on why, digitally, police have so much further reach, without the necessary applications to court in place; and, thirdly, on the impact—my hon. Friend rightly mentioned this—that that is having on court and CPS time, and the costs associated with it, in an already highly clogged-up court system?

Sarah Jones: My hon. Friend has made a series of correct points. Across the board, in the digital and the online worlds, when it comes to laws, we are behind what is happening in the real world. A significant number of changes need to be looked at to come up to date with what is already happening. We would argue that this is one of those examples.

As well as impacting victim attrition, this issue is a factor in deciding whether to even report a rape or a crime in the first place. The Victims' Commissioner survey of rape complainants showed that, for some, scrutiny of their personal lives—including their digital lives—was a consideration in their decision not to report. For those who did report, the experience was felt to be "invasive" and "traumatic", with many feeling that the process was not properly explained. The survey stated:

"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."

A female is quoted as saying:

"I was also reluctant to do so because I felt my [F]acebook data and mobile phone information would not have supported my account as I had been friendly with the perpetrator before the incident."

Another said:

"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…and all my privacy was gone."

Many respondents felt that they had no choice but to hand over devices for scrutiny, and that raises issues around what is meant by "voluntary" in the context of a police power. Arguably, it confirms the need for safeguards in legislation, which speaks to what my hon. Friend the Member for Rotherham said about the power balance and what "voluntary" means. The Victims' Commissioner said:

"Many survivors said 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 request was simply part of normal investigation procedures. However, most survivors had concerns around the disclosure of personal data and access to records."

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

A great deal of work has been done at policy level to address some of the issues, but none of the work to date has sought to alter police powers to obtain and scrutinise a digital device. Existing case law legislation and guidance make it clear that agreement to digital extraction can be sought only if the officer believes that relevant material can be extracted from a phone for criminal investigations—that means that it is relevant to a reasonable line of inquiry.

Sarah Champion: My hon. Friend would be making an incredibly powerful argument if she was making it on behalf of the criminals, but she is actually making it on behalf of the victims of crime. Surely, this level of invasive behaviour as regards their most private and personal things, after they have been the victim of a crime, is truly shocking.

Sarah Jones: I completely agree. The issue of people having things on their phone that relate to their family or friends, which they feel it would be terrible for others to see, has not been thought through.

In the Bater-James Court of Appeal judgment, the judges were clear that there should not be speculative searches, and that there must be specificity based on a reasonable line of inquiry. The information should be extracted only in so far as it is strictly necessary and proportionate to the investigation, and the officer must be satisfied that there are no other, less intrusive means available to them of pursuing that line of inquiry. It is vital that the police can rely on "strict necessity" for law enforcement purposes from the perspective of data protection, but it is also vital that the victims agree to the download, meaning that they fully understand what is being sought, and that the agreement is freely given.

In an evidence session last week, we heard from Martin Hewitt of the National Police Chiefs' Council that there is an ever-increasing

"volume of digital evidence that is required for almost every investigation."

He said:

"That has created real pressure on the time limits of investigations and our ability to gather the evidence that we need to take an investigation forward. We have increased the capability. It is partly about equipment and having the right equipment to be able to extract digital evidence. It is also about having officers and staff who have the right capabilities to assess that evidence and produce it in an evidential form…However, the flip side and the really important point is making sure that what is being done is lawful, proportionate and necessary. Again, that side of the work is equally important…So we need the legal framework to allow us to do that properly and we then also need the resourcing and the

[Sarah Jones]

capabilities to do it within the right time limits."—[*Official Report, Police, Crime, Sentencing and Courts Public Bill Committee,* 18 May 2021; c.16, Q21.]

Alex Cunningham (Stockton North) (Lab): My hon. Friend is making a very clear argument. She will recollect clause 36(10), which relates to the age of an adult. It suggests that in the context of extraction for information, an "adult" is someone who is 16 years old. Is it not all the more important that we have legal protections for children, if the Government insist that they are adults at the age of 16?

Sarah Jones: My hon. Friend makes a very good point, which was raised last week, and which I know the Minister has clocked. We have an amendment to shift the age from 16 to 18, but my hon. Friend is absolutely right to say that if the age remains that low, we need to make even more sure that we protect victims.

Police forces carry out digital data extraction from victims' phones in kiosks. In the police forces that have kiosks—not all of them do—the police often have to queue and wait to download their information. Martin Hewitt's point about time limits is crucial; the police clearly do not have the right equipment for the new power to be used in the way that the law says it should be used. The police do not have the technology to draw out specific information from people's phones, and the risk of incriminating family or friends can prevent cases from going ahead. I know that the guidance from the College of Policing says that police must immediately delete all data that are not relevant, but there is a big problem, in that so many cases brought to them do not go ahead. Will the Minister provide assurances as to how the Government will provide the police with the resources and capacity that they need to enforce what they need to do with digital extraction?

In the evidence sessions, we also heard from Dame Vera Baird that

"The police have now done a lot of work to try to shift policy backwards, and this new power—which has no obvious nod, even, in the direction of the protection of complainants—came out of the blue from a different Department of the Home Office, and has absolutely none of the protections that, in policy terms, the police have been looking towards for quite some time."—[*Official Report, Police, Crime, Sentencing and Courts Public Bill Committee,* 20 May 2021; c.111, Q174.]

New clauses 49 to 53, on the power to extract data from electronic devices, would protect the rights of complainants under article 8 of the European convention on human rights, particularly in sexual assault and rape cases. They would more clearly define that "agreement" in the legislation means informed and freely given agreement, to avoid abuse of this power. The new clauses would ensure that alternatives were considered before a request was made to a victim, and that only specified persons could agree and provide a device on behalf of children, who must be consulted before a decision is made. The same would apply to adults without capacity. The new clauses would oblige the code of practice to address a number of points about exercising the power, in order to better protect the rights and experience of victims.

I will run through the issues that we are seeking to correct through the new clauses. The first is that there is no definition of "agreement" in the legislation. As we have said, police all too often seek the agreement of complainants of sexual violence in circumstances where they are not fully informed—sometimes they are being coerced—so it is really important that the primary legislation defines "agreement", which means agreement that is informed and freely given. Linked to agreement is the need for the police to be specific about what data they are seeking. Only if the police are specific can the data owner give informed agreement to extraction.

The second issue is that a reasonable line of inquiry is not clearly defined in the legislation. It nods to that by using the word "relevant", but material sought from a suspect or complainant for the purposes of investigating and prosecuting crime will be relevant only inasmuch as it is part of a reasonable line of inquiry. It is vital that that be clearly defined in the legislation. Without a clear definition, the legal hoop for police is merely reasonable belief and relevance. This risks further embedding a culture of wholescale downloads and intrusion into privacy.

12.15 pm

Sarah Champion: My hon. Friend talks about the being able to access the device only if there is a reasonable line of inquiry. Should the police or investigating body also look to follow that reasonable line of inquiry through other methods, rather than automatically making a call on that digital device?

Sarah Jones: My hon. Friend is absolutely right: other means of investigating should be pursued before there is that intrusion of taking people's phones. The Victims' Commissioner has recommended that guidance be issued mandating that a record be made of the decision-making process of the authorised person in identifying a reasonable line of inquiry, so that it can be scrutinised at a later date.

The next problem is that clause 36(5)(b) states that an authorised person using the power should be

"satisfied that exercise of the power is necessary and proportionate to achieve that purpose."

The Victims' Commissioner advises that the test should be that the authorised person is satisfied that exercise of the power is strictly necessary and proportionate to achieve that purpose, and we have incorporated that language into our new clauses. Statute and case law insist on strict necessity as the only appropriate test in circumstances where sensitive data—such as health data, sexuality data, or information about others—will be processed. A complainant's phone will nearly always contain such information, and as such will automatically require sensitive processing. In their clauses, the Government have removed "strictly" from the test, creating a far lower threshold than the one that the Data Protection Act 2018 intended for processing this type of material, and meaning that victims' article 8 rights are less protected.

The next problem is that the phrase "reasonably practicable" in clause 36(7)(b) is incompatible with the data protection legislation, and there are concerns that this gives police a means of easily dismissing other options. The term

"strictly necessary for the law enforcement purpose"

under the Data Protection Act places a higher threshold on processing based on this condition. As my hon. Friend the Member for Rotherham said, controllers

need to demonstrate that they have considered other, less intrusive means, and have found that they do not meet the objective of the processing. The test does not ensure that. Under the clauses, police could decide, having considered alternative means, that it is not practical to get the information via those means. The risk for rape victims is that, both culturally and due to operational constraints, the most practical or easiest path to obtaining the information sought will nearly always be the victim's phone. Again, normal practice is being bolstered by this legislative power, and there are limited safeguards for victims.

The final point of concern for the Opposition is that in the clauses, as my hon. Friend the Member for Stockton North said, the authorised person has no obligation to obtain the views of children and those without capacity when seeking to obtain information from their phones. Neither the police nor the person giving agreement in those people's stead is obliged to ensure that their views are considered.

Sarah Champion: This relates to amendments of mine that will be debated later. I wonder whether something needs to be inserted about language competency. My amendments deal with asylum seekers who do not have English as their first language. Should language competency also be a consideration, so that we ensure that people actually understand their rights?

Sarah Jones: Yes. Whenever people hand over personal information, they need to know why they are doing so, and the implications. That is as important for a child as for an adult, and we need to make sure that principle is enshrined properly in law.

It is important to safeguard the human rights of children, and to ensure that only specified persons can agree to handing over information and providing a device on behalf of children, who must be consulted before a decision is made. The same should apply to adults without capacity, and we have effected this principle in our new clauses.

Another issue—the Minister was looking at this last week—is that for the purposes of this chapter, clause 36(10) defines an adult as a person aged 16 or over, and a child as a person under 16. Hazel Williamson, chair of the Association of Youth Offending Team Managers, said in evidence to us last week:

> "We should treat children as children until they are 18 and they should be sentenced as a child until they reach the age of 18. In an ideal world, we would look beyond that, because many people do not develop fully, in terms of brain development, until they are in their mid-20s."—[*Official Report, Police, Crime, Sentencing and Courts Public Bill Committee,* 20 May 2021; c.136, Q223.]

Our amendments would change the age from 16 to 18. I would like to learn from the Minister why the Government chose to define "adult" in that way.

While we welcome the code of practice attached to this legislation, there is no detail yet about what it may contain, and there is no duty on the Secretary of State to consult victims' representatives or champions in creating it. Our new clause would require the Secretary of State, when preparing the code of practice, to consult a range of parties, including the Information Commissioner, the Victims' Commissioner, the Domestic Abuse Commissioner and other regional and national bodies.

Our new clauses also list matters that the code of practice should address, because protection for victims should be in the Bill. Clauses 36 to 42 provide the police with a wide-ranging power to obtain and scrutinise victims' phones, with virtually no safeguards for victims. It is said that some protections are intended to be put into the code of practice, but the police will not be obliged to follow it. There are concerns that the clauses will provide the police—and the Crown Prosecution Service, via the police—with a legal basis for carrying on as they have been. The police accept that the Victims' Commissioner's proposals are appropriate for their purpose, and would give a better balance as regards victim protection. I thank the Victims' Commissioner and her team for all their work to guide us though this tricky area of law. I hope that the Minister will listen to the concerns we have raised.

Sarah Champion: I thank my hon. Friend for all the points she made, which, to be quite honest, are common sense, but would cause a huge shift in victims' and survivors' perceptions of their rights. I have questions for the Minister.

On data storage and security, I am sure we were all pretty shocked and disgusted to hear that images relating to Sarah Everard were not secure in the police system. While I have a very high regard for the police, they can be a leaky sieve—let us be honest. Why do we not simply clone phones at the point of taking them? Why is it months, or usually years, before the victim gets their phone back? Would it be possible to put in legislation or guidance a timeframe on how long that phone can be held for? Having spoken to officers, it seems that cloning a phone is complicated and geeky; it tends to be put in a back drawer until they absolutely have to do it. A timeframe would give a lot of comfort to victims and survivors; they would know it was only a week until they got their photos back, for example.

Finally, a myth has been perpetuated that victims and survivors have to hand over their phone or mobile data to the police or their case will not be taken forward. I have heard examples of victims and survivors being told expressly that if they do not hand it over, they are withholding evidence and could be prosecuted. At that point, unfortunately, a number of survivors drop out of the process and withdraw their charges altogether. If the Minister is able to give reassurance on that, that would be hugely appreciated.

I turn to amendment 115, on the list of people who may extract data. The list is pretty extensive, but one group stood out: immigration officers may request a mobile phone. A few months ago, I went to a large asylum hospital in my constituency, where there were 50 to 100 men—I do not know how many—and what concerned them most was that, literally as they entered the country, their mobile devices and indeed clothes were taken off them. There was no debate or explanation; it is just part of the process.

I completely understand the argument that very bad people, such as gangmasters, who come into the country may have a lot of contacts that are relevant to police inquiries. The police and transport police are already on the extensive list of people who may access electronic devices, so if an immigration officer was concerned, they could get a police officer to take the digital device away. That is not a problem. Extracting data is a complex

[Sarah Champion]

process that requires specialist experience, and it ought to be managed under the law. I am concerned that we are asking immigration officers to be incredibly mindful, and to be trained and resourced, and to have all the skills, to request that device.

The people I met fell into three camps: economic migrants, who have paid to come over here; people who have been trafficked over here; and those brought in specifically for modern slavery. All the men I spoke to wanted to see pictures of their loved ones. They wanted those memories from home, and a mobile phone may be the best way to hold those memories and connections.

I do not know anyone's telephone number aside from my parents'—it was the one I grew up with. I can call the police, the NHS helpline and my mum, but everything else is stored on my phone. If I lost it, I would not know how to respond—and I have back-ups that I can access, and English as my first language. When I changed phones, I did not download properly and lost five years of photos. That was so painful. Imagine someone being trafficked into this country, and probably horrifically abused on the way in. The one thing they can hold on to is their memories on that digital device, but that is taken away. They have no information about why it was taken, or when it will be returned, and all their contacts have been lost.

All the points that my hon. Friend the Member for Croydon Central made apply in this case. Immigration officers are one of the groups who may take these devices—this is not a dig against immigration officers, who do a difficult job—but in any other situation a police officer or a court order would be required to take such detailed data. I ask the Minister please to remove immigration officers from the list.

Victoria Atkins: I welcome the discussion about this chapter of the Bill, because the framework we are setting out is a really important step forward in improving the expectations about and management of digital data that victims and complainants may have on their digital devices. Of course, completely understandably, the focus has been on complainants in sexual violence cases—I will go into some detail on that in due course—but the chapter applies across the board. If, for example, in cases that do not relate to sexual violence, a mobile phone is deemed to be relevant and the authorised person is satisfied that the exercise of the power is necessary and proportionate, this chapter will apply.

12.30 pm

A detail that perhaps needs to be drawn out in Committee is that this chapter does not apply just to police investigations or, in other words, to somebody coming to the front desk of the police station, as the hon. Member for Rotherham described. It also applies in circumstances in which the police need help to locate a missing person or to protect a child or vulnerable person from neglect or harm—those harms are set out in the Bill. It is not simply for police investigation from the moment of reporting; it can also involve those very difficult cases in which the police perhaps have only hours to act to protect a child or locate a missing person.

Against that context, I will focus for the time being on victims of rape and other sexual violence. We know that conviction and charge rates in sexual cases have fallen dramatically over the last few years. From conversations with victims, as well as with charities that work with victims, we know that one of the barriers to victims reporting to the police or, once they have reported, to continuing all the way through to trial, is how their mobile phones are dealt with—we absolutely understand that. I do not pretend for a moment that it is the only barrier, but it is a significant one.

Over the last couple of years, we have had some awful examples of the system clearly not working well, some of which the hon. Member for Croydon Central set out. It has not been working well for victims, and it has not been working well for defendants or suspects either—I know that we are all seeking to keep that balance between the rights of victims and the convention that a person is innocent until proven guilty. There have been problems with the CPS and the police issuing guidance in the past. There is a huge groundswell of support—I would hope so, anyway—for clarifying the law on this, because it has clearly caused problems. As mobile phone usage has increased exponentially, and as what we use our phones for has changed over the last five years—let alone the last decade—it is critical that we get the legal framework in place. That is what the Bill will achieve.

I would not want anyone to think that this framework is the Government's only answer to the far wider problem of conviction and charge rates in rape cases, or that this is the work to ensure that victims feel supported in their journey through the criminal justice system—it is not. It is but one step in our work on that. Colleagues will know that only this week there was an urgent question directed towards my hon. Friend for one of the Hampshire seats—I cannot remember whether it is north, south, east or west.

The Parliamentary Under-Secretary of State for the Home Department (Chris Philp): North West.

Victoria Atkins: Thank you. The Minister for Crime and Policing, my hon. Friend Member for North West Hampshire (Kit Malthouse) answered the urgent question on the timing of the rape review. Colleagues will know that for the last two years, the Government have commissioned intensive research into each stage of the process within the criminal justice system of a rape case or a sexual violence investigation, from the moment of reporting through to the moment when the case finishes, whether by way of a verdict or if a trial does not go ahead for any number of reasons. We had very much hoped to publish that review by the end of last year. However, we were very understanding of the fact that the Victims' Commissioner and women's charities wanted to make representations, in particular looking at the shadow report by EVAW—End Violence Against Women. We were mindful that there was a super-complaint under way as well. Therefore, we have paused publication in order to take into account some of those factors.

The Minister for Crime and Policing informed the House this week that we plan to publish the review after the Whitsun recess. It will show the Government's intentions in relation to this particular category of cases, sexual violence cases, and will of course sit alongside this Bill, but will go much further than the Bill. On some of the situations, scenarios and experiences that were described today and last week in evidence, I just urge caution until the rape review is published, because there may be answers in that document.

In terms of the legal framework, I think it is really important that we have this in the Bill and that the rights of victims and of suspects and defendants are set out and clarified and that we introduce consistency where that has been alleged in the past to be missing.

I note just as an example that one of the other ways in which we are really trying to help victims of sexual violence is through support for independent sexual violence advisers. We already have ISVAs working with victims across the country. This year, we have been able to announce the creation of 700 new posts, with some £27 million of funding. I give that just as an example. This is an important part of our work, but it is not the only piece of work that we are doing to address some of these very genuine concerns.

Sarah Champion: I am hearing everything that the Minister is saying. Knowing that the review is coming out—I assume it is something that she has been working on or very closely with, because of her intense involvement and support in this area—does she feel that the measures in the Bill are proportionate or are they something that, once the review comes out, she may look at changing, to ensure that the safeguards that she speaks of are embedded in the final Act that we see?

Victoria Atkins: We have been working together on this. We must not not forget that the background to the legal framework has to take into account the Criminal Procedure and Investigations Act 1996 and the more general disclosure rules, for example. But this has been very much a piece of work across Government, because we want this framework to give confidence and clarity to victims and to suspects, but also, importantly, to the police and the Crown Prosecution Service, because they are the ones who must administer and work within the legal framework and the code of practice.

If I may, Mr McCabe, I will take a bit of time, because this is such an important measure and I am mindful that there are questions about it, to set out some of the detailed thinking behind the way in which the clauses have been drafted. The current approach to the extraction of information from digital devices has indeed been criticised by some as feeling like a "digital strip-search" where devices have been taken as a matter of course and where, in many cases, all the sensitive personal data belonging to a device user was extracted and processed even where it was not relevant to the offence under investigation. We absolutely understand the concerns that have been raised in relation to that.

Alex Cunningham: I think this is an appropriate point for me to lay the challenge on the Government about the decision to classify children as adults at the age of 16 in clause 36(10). The Minister has just used the expression "digital strip-search". Is it really appropriate for a 16-year-old girl, or boy for that matter, to have a digital strip-search, giving up all their little secrets and everything else, because the Government think that they should be classified as an adult and that adult factors should be applied directly to them?

Victoria Atkins: I will deal with that in detail in due course. Just so that colleagues understand how that age was settled upon, in the drafting we carefully considered people's views, including the Information Commissioner, about the freedoms and the feelings of power and authority that users of devices have. We settled on the age of 16 because we understand that a 16-year-old is different from a 12 or 13-year-old, if their parents have allowed them mobile phones, although I am banning my son from having a mobile phone until he is at least 35, but there we go. A moment of lightness, sorry.

I will deal with the point in more detail later, because it is important, but there is a difficult balance to maintain between rights of victims, suspects and defendants but also rights of users, particularly under the European convention, so that has been the Government's motivation in this. However, we are alive to scrutiny.

Sarah Champion: I think this involves the focus that I hope the Minister is going to come to. I hear everything she has just said about the justification and I am going along with that, but it is clear in subsection (10):

"In this Chapter—

'adult' means a person aged 16 or over".

Why was that specific wording chosen rather than "the remit of the clause covers people from the age of 16 onwards", for example?

Victoria Atkins: I will come to that later, but the hon. Lady knows that I am in listening mode on this. The Bill includes requirements to obtain agreement to extract information; to ensure there is reasonable belief that the required information is held on the device; and, before using this information, to consider whether there are less intrusive means of obtaining it. That is an important point that I know hon. Members have focused on. The clauses will ensure that the victim's right to privacy will be respected and will be at the centre of all investigations where there is a need to extract information from a digital device.

The Bill also includes a new code of practice. This will give clear guidance to all authorities exercising the power. It will address how the information may be obtained using other, less intrusive means; how to ensure that agreement is freely given, and how the device user's rights are understood. All authorised persons will have a duty to have regard to the code when exercising or deciding whether to exercise the power. The clauses are also clear that the code is admissible in evidence in criminal or civil proceedings and that a failure to act in accordance with it may be taken into account by the court. It will give up-to-date, best practice guidance for selectively extracting data considering existing technological limitations. That will be updated as and when further capabilities are developed and extended to all authorities able to use this power.

Sarah Jones: The Minister is outlining how important the code of practice is. Is she therefore sympathetic to the view that we have put forward in our new clauses that that code of practice should be pulled together with a list of eminently sensible and professional organisations and people, and that we should define in the Bill some of what that should include because it is so important?

Victoria Atkins: We are going to be even more ambitious than that. We aim to publish a draft on Report, which means the House and the other place will be able to scrutinise the draft code of practice during the scrutiny of the Bill as a whole. Once the Bill receives Royal Assent, we will consult formally on the code of practice, including with the relevant commissioners, to enable a

[Victoria Atkins]

more detailed draft to be laid before the House. Again, we are in listening mode on the ways in which the code of practice should be drafted, because we understand how important it is and how important it is that victims, the police and the Crown Prosecution Service, among others, have confidence in the document.

12.45 pm

Last week, we heard evidence from the Victims' Commissioner, who argued that the provisions do not go far enough in protecting the privacy of victims and witnesses. Those concerns are captured in the new clauses put forward by the hon. Member for Croydon Central. I assure the Committee that we have considered Dame Vera's points very carefully. In a letter of 7 May, the Home Office director of data and identity set out in detail our response to each of her points. I will deal with each one in turn.

Clause 36 confers a power on an authorised person to extract information stored on an electronic device where the user has volunteered the device and has agreed to the extraction of information from the device. New clause 49 narrows this second test so that the device user agrees to the extraction of "specified information".

The police and other agencies that will need to use this power extract information from electronic devices using a range of different tools and techniques. Not all such tools have the ability to extract only specified information. The extraction process is complex and dependent on the device type. In some cases, the applications being used will determine what level of information can be extracted. For example, the information may be held in a database that needs to be fully extracted to process just one message or photo from it. These complications apply particularly in cases where there are allegations that the digital device—the mobile phone, for example—contains images of child sexual abuse. Some people who are accused of such offences are very sophisticated users of technology. That is one example of where the complexities of downloading the material are not perhaps as simple and clear as one would ideally like.

I have asked about cloning phones and I am told that the risk is that not all the data is copied exactly. Information could be lost and there are concerns that it may not be able to be used in court proceedings.

The wider picture is that extracting evidence or information from a phone is not a uniform process and there are different tools that the police must use. That is why we have drafted the clauses we have, so that the authorities are able to use the power now, rather than depending on some future technology that we hope and expect will be developed in years to come.

We are also mindful that technological developments, and with it the capabilities of the police and others, are fast-moving. While we are keen to see the adoption of new tools by police officers, we also need to ensure that the legislation reflects current capabilities and does not require amendment as each development in technology occurs.

Sarah Champion: I hear what the Minister says about cloning and the risk that it is not suitable for admission in court. Will the Minister comment on a kindness that could be done—giving a clone of photos to an asylum seeker, for example?

Victoria Atkins: I am so sorry—I have not quite understood the hon. Lady. On the taking of a phone, if I have just been told that we are concerned about the ramifications of cloning it, I do not see why we would clone it despite those reservations in order to provide photographs. I would be very uneasy about having differences in how the police handle digital data depending on the personal circumstances of the person from whom they have taken a phone, including nationality. I would be very cautious about going down that road.

Sarah Champion: I did not mean to be used in court. I meant for the individual who has lost their one contact with home—that they could get a copy or a print-out of photos, rather than the device just being taken away with no explanation of when they are going to get it back again.

Victoria Atkins: I am very cautious about distinguishing between different victims. Perhaps the hon. Lady is alleging that the person she is talking about is a victim. The framework is about consistency and clarity, and I would be concerned about having caveats here and there in order to fit individual facts. Part of this test is about relevance, necessity and proportionality. Those are the tests that we are asking officers to apply, and we would have to apply them across the board.

There are situations within the framework whereby the power can be used without agreement, such as to locate a missing person where the police reasonably believe that the person's life is at risk. Under clause 36, the police may have good reason to believe that a device has information that will help to locate the person. In such circumstances, clearly the person is not available to give their consent, so clause 36 ensures that officers can extract data, if it is necessary and proportionate, to protect the privacy of the user. That also applies in relation to children who need to be protected.

New clause 49 raises the bar for the exercise of the power in clause 36(1). The necessity test under new clause 49 is one of strict necessity. I am not persuaded that adopting the phrase, "strictly necessary and proportionate", instead of "necessary and proportionate", will make a material difference. This phrase is well used in the Bill. I note that article 8.2 of the European convention on human rights—the very article that people are relying on in relation to the framework—permits interference with the right to respect for private and family life. Such interference is permitted where it is necessary to achieve various specified objectives.

Sarah Jones: I understand what the Minister is saying. The review in Northumbria showed that about 50% of requests were not strictly necessary and proportionate. That must be wrong, and we are trying to make sure that people know what they are giving over, that they do it voluntarily and that it is absolutely necessary that such information is requested. Apart from trying to be clear about what is proportionate and necessary, what solution can the Minister put in place to make sure we do not have 50% of cases involving asking for information where it is not necessary and proportionate?

Victoria Atkins: On what the hon. Lady has described, I am not sure what difference it would make. I am trying to put myself in the boots of a police officer. Would a police officer ask for data if they read the words, "strictly necessary", but not if they read the word,

"necessary"? Actually, the problem that has been identified by the figure quoted by the hon. Lady is police officers' understanding of the legislation, which comes back to training. Article 8, on which many rely in this context and in this part of the Bill, refers to "necessary" interference, and I am not clear what "strictly necessary" would add to that.

New clause 49 seeks to provide that information may be extracted only for the purpose of a criminal investigation

"where the information is relevant to a reasonable line of enquiry."

There are safeguards within the clauses to ensure that information is not extracted as a matter of course, and they have been drafted with respect for victims' privacy in mind. They include a requirement that the authorised person has a reasonable belief that the device contains information that is relevant to a purpose for which they may extract information, and that the exercise of the power is necessary and proportionate to achieve that purpose.

Sarah Champion: I hear everything the Minister is saying and it is very plausible, but I want to challenge her assertions on necessary, proportionate and clear lines of inquiry, based on the answer I received to a written question to the Home Office on 11 November. I asked about the process of extracting mobile phones. The Under-Secretary of State for the Home Department, the hon. Member for Croydon South replied:

"Immigration Enforcement search all migrants"—

at this point, "all migrants", so we do not know yet whether they are an asylum seeker, being trafficked or are here for nefarious purposes—

"upon arrival at the Tug Haven at Dover. In the event that a mobile phone is discovered it will be seized as part of an investigation into the organised crime group involved in the facilitation."

Again, we do not know if they are a criminal or a victim at this point, but the phone will be seized regardless.

"The migrant will be informed verbally that the phone will be kept for evidential purpose for three to six months. They are provided with a receipt and contact details. Attempts will be made to communicate this in their first language, although this can be challenging due to external factors."

So people arrive here, immediately their phone is taken away from them and they might not even know why. It is great that within "three to six months", they are meant to have that response—

Chris Philp: Because they are here illegally.

Sarah Champion: Sorry, Minister? I do not think that the reality on the ground—the reality that the Home Office acknowledges—backs up what the other Minister is saying about reasonable, proportionate and lines of inquiry, because it is happening to every migrant coming into this country.

The Chair: I know this is important detail, but I remind the hon. Lady that interventions should not be too long.

Victoria Atkins: I cannot hope to do justice to a parliamentary question answered by my hon. Friend the Member for Croydon South, the Immigration Minister, because I know the care and attention he gives to answering such PQs. However, over lunch, I will attempt to extract an answer that will do justice to his response. I make the point that the hon. Member for Rotherham is referring to practice at the moment. Again, the point of this legal framework is to ensure that we have consistency and clarity of approach. I will try to do my hon. Friend justice when we return at 2 o'clock.

I will now move on to the Criminal Procedure and Investigations Act 1996 and its code of practice, because those provisions on "reasonable lines of inquiry" will continue to apply to the investigation of criminal offences in England and Wales. We cannot—must not—view the extraction of digital data in a vacuum, apart from the rest of the powers of, and duties on, police officers and the CPS when it comes to a criminal trial.

In the context of mobile phones, iPads and so on, police forces will continue to use the digital processing notice developed by the National Police Chiefs' Council for this purpose. It explains in lay language how the police extract the information, which information might be extracted, how long the device might be retained for and what happens to irrelevant material found on the device or devices. The notice makes it clear that investigators must respect an individual's right to privacy and must not go beyond the reasonable lines of inquiry. That is the golden thread that runs throughout the Act.

It is imperative that the existing procedures for investigations set out in the 1996 Act are followed. Although the clauses in the Bill concern a broader range of activity than just criminal investigation, helping as they do in investigations for missing persons or to protect children, we do not want to introduce any ambiguity. I will therefore reflect on that, but we are clear that the CPIA provisions must continue in the context of criminal investigations.

I note that new clause 49 would omit subsection (7)(b) of clause 36. We are clear that police officers and others using the extraction power should always seek to obtain the information required in the least intrusive way possible. There are situations in which it may not be reasonably practicable to utilise the least intrusive means of obtaining information, and this clause ensures that authorised persons may make that judgment. That could be because the time it would take to gather the information might affect the investigation or increase the risk of harm to an individual, or because those methods would mean intruding on the privacy of a wider number of people.

I will give one example and then I will sit down. When searching for a missing person, information such as an image on a witness's device might also be captured on CCTV. Identifying all cameras, and downloading and reviewing many hours of CCTV footage is a time-consuming process. The authorised person may decide that it is more appropriate to extract the information from the device in order to speed up the inquiry and to try to locate the missing person before they come to harm.

1.1 pm

Ordered, That the debate be now adjourned.—*(Chris Philp.)*

Adjourned till this day at Two o'clock.