Privacy International response to documents disclosed in advance of External Reference Group meeting which took place on 21 November 2019

TO: External Reference Group & Police Scotland

Privacy International make these submissions in relation to the following documents that we have received. If any documents not listed below were discussed, we kindly request a copy:

- Chair's summary of Police Scotland's Cyber Kiosk (digital triage) External Reference Group members' views July 2019
- Complete – Consent Leaflet v2.1
- Police Scotland / SPA Equality and Human Rights Impact Assessment
- Digital Device Consent Capture Flow Process
- Digital Device Consent Withdrawal Flow Process
- Digital Device Examination Request Form Flow Process
- Digital Device Examination – Principles
- Digital Device Journey Request Flow Process

Table of Contents

Summary concerns ***3***

Introduction ***6***

Questions for Police Scotland ***14***

Submissions on the documents ***15***

Consent Leaflet v2.1 ..... **15**

Police Scotland / SPA Equality and Human Rights Impact Assessment **21**

Digital Device Consent Capture Flow **23**

Digital Device Consent Withdrawal Flow Process **23**

Digital Device Examination Request Form Flow Process **24**

Digital Device Examination - Principles **24**

Digital Device Journey Request Flow Process **24**

Data Protection Impact Assessment – Cyber Kiosks **25**

Audit ***26***

Selective Extraction ***26***

Internet of things ***27***

Summary concerns

Consent

1. Police Scotland state in the disclosed documents listed above that seizure of a phone can be based on consent. This consent is unrelated to the Data Protection Act 2018. This consent must be voluntary, informed and with capacity. Given the power imbalance between the police and the individual it remains unclear how such consent can ever be 'free'.

2. The lack of information provided to the individual regarding extraction, examination, retention, deletion, sharing and search parameters undermines that any seizure which is for the purpose of examination can be informed.

3. We further question, if the victim or a witness is not provided with legal advice or other independent support in reaching a decision whether to consent and is likely to be in a state of distress, whether they can truly have capacity to make an informed decision free from pressure and influence.

4. The use of 'consent' as a legal basis for seizure can be nullified by the use of another power i.e. consent only relates to the seizure of the device and not examination, how is such consent then meaningful?

5. Police Scotland have not stated the legal basis for using 'consent' to seize the device.

6. Police Scotland's focus on seizure and 'consent' gives an illusion of involvement and empowerment of the victim or witness, when in reality, withdrawal of consent may have little or no impact apart from being noted on a form. This is because the police have seized the phone for the purpose of examination and either intend to or have sent the phone for examination, regardless of withdrawal.

Failure to provide sufficient information on cybercrime hubs, despite being intrinsically relevant to the victim consent forms and associated literature.

7. It is clear from the documents that devices seized, whether by consent or otherwise, are seized for the purpose of examination. There are numerous references not just to 'examination' but to 'extraction' of data in the documents, created to be provided to victims and witnesses. This indicates very clearly the intention to use the cybercrime hubs i.e. to extract the data. Yet Police Scotland have failed to provide any transparency to the Justice Sub-Committee on Policing and the External Reference Group [ERG] in relation to cybercrime hubs.

8. Police Scotland have insufficiently clarified whether they will extract all data and then apply search parameters. They have not stated whether or not selective extraction is possible. If a full extraction is attempted, Police

Scotland have not said in any detail how search parameters protect victims' rights. They have failed to clarify whether they will collect and retain all data that can be extracted, even if this is not relevant to the investigation. They have not said whether once the data that is strictly necessary and proportionate to the investigation has been identified, whether the rest can be deleted.

9. Police Scotland have provided insufficient information to reassure the ERG that search parameters will be strictly enforced and independently audited. They have also not specified how they will be formulated e.g. if the victim says there are relevant text messages, on what basis can Police Scotland go beyond this data type and date range.

10. Police Scotland have stated in the disclosed documents and previously[1] the device will not be connected to the internet at cyber kiosks, there is no such assurance in relation to the cybercrime hubs. Therefore, it is unclear whether cloud extraction is possible at the examination stage, especially if digital devices includes 'internet of things' devices.

Data Protection Act 2018 & confusion relating to lawful basis for examination

11. There appears to be confusion in the documents when referencing the Data Protection Act 2018 and the lawful basis for examination.

12. The lawful basis under the Data Protection Act 2018 and the relevant statutory and common law powers remains unclear and still fails to satisfy the concerns raised by the ERG.

Internet of things

13. Police Scotland refer to 'digital devices' in the disclosed documents which appears to include not only mobile phones but internet of things devices, which could include for example, an Amazon Echo, Google Home, fitbit, smart lightbulbs, connected toys, smart TV, smart fridge and the plethora of other devices that could fall under this term. Yet no information has been provided in relation to 'internet of things'; no definition has been provided as to what this encompasses; and there has been no consideration as to how these devices differ from mobile phones and present a further challenge to the ability to obtain 'consent' to seize these devices, that is voluntary, informed and with capacity.

14. For example, whilst an individual may understand that their phone holds relevant messages, it is questionable what an individual may understand is held on an internet of things device and what can be obtained from extracting data from an internet of things device, as opposed to going to the relevant company to obtain cloud stored data.

[1] https://www.theguardian.com/society/2019/nov/10/half-of-victims-drop-out-of-cases-even-after-suspect-is-identified

15. The inclusion at this late stage of 'digital devices' to refer to undefined internet of things, appears to be expanding what Police Scotland seek to do without sufficient transparency and scrutiny.

Flawed definition of digital devices and comparison with a briefcase

16. Police Scotland seek to compare examination of extracted data from a digital device to examining a briefcase that has a lock. This is an extremely problematic comparison and wholly inaccurate. For example, there is no way a briefcase could contain all your browsing history, emails, text messages, photographs, location data, calendar entries, Bluetooth devices you had connected to, wifi connections, voice requests to Alexa or Siri and so forth, stretching back many years and relating to many individuals. You cannot store the entirety of someone's life in a briefcase.

Introduction

17. We support the Chair's summary of Police Scotland's Cyber Kiosk (digital triage) External Reference Group, updated November 2019. We do not repeat these submissions in detail. However, we do expand on the submission regarding the use of 'consent' as a legal basis for seizure and how this can be nullified by the use of another power i.e. at the point of examination. We agree this affirms the view set out in the Chair's summary that the current legal framework is inadequate. We further note the recommendation for a Standard Operating Procedure and our suggestions below in relation to information that should be provided to individuals who have their phones examined.

18. We believe that insufficient procedures, checks, independent audit requirements and transparency exist in the current proposed scheme to protect the rights of victims, witnesses and suspects. A Standard Operating Procedure, guidance or policy is needed which addresses issues we raise below under 'What is needed to inform an individual'.

What is consent?

19. Privacy International understand from the disclosed documents and the discussion at the External Reference Group meeting in November 2019 that Police Scotland are now using 'consent' in a way that has two separate interpretations.

20. Firstly, they are using it in relation to the 'seizure' of a phone from a victim or witness and secondly, they refer to 'consent' as a lawful basis in relation to the Data Protection Act 2018 ("DPA 2018"), notably in the 'consent Leaflet v2.1' (see below). This second reference is confusing and perhaps inadvertently so, given Police Scotland now accept that they cannot 'examine' or process the data from the phone using 'consent' as a lawful basis under the DPA 2018.

21. It was discussed at the External Reference Group meeting that since seizure does not involve the processing of personal data, the Data Protection Act 2018 has no bearing on this stage. The use of 'consent' to seize the phone has nothing to do with consent as understood under the DPA 2018.

22. Nevertheless, we reserve the right to assess whether, at the point of seizure of the phone, the examination of the phone is so inextricably linked to the processing of personal data, given the seizure of the phone is done explicitly for the purpose of examination (according to the documents disclosed by Police Scotland) that the DPA 2018 is relevant at the point of seizure. And thus, the use of 'consent' to seize and extract the phone is in breach of the DPA 2018.

23. Consent is not defined in Part 3 of the DPA 2018 and is not defined in the Law Enforcement Directive as it should not be a legal basis used by the police to process data. If it were a valid legal basis for the data processing then there would not be the same need to make this distinction. However, we will not make further submissions on this point in this document.

Digital devices

24. It should be noted that when discussing devices, based on the disclosed documents that refer to 'digital devices' and our correspondence with Police Scotland, Police Scotland are not only referring to mobile phones but to 'internet of things' devices. Therefore, when they refer in the documents to seizing devices from individuals based on 'consent' i.e. voluntary submission, this relates not just to phones but to any 'digital device'. As devices connected to the internet proliferate, this has very serious consequences for the rights of individuals. The concerns related to use of consent to take internet of things devices not only reflect those related to mobile phones which we raise, but there are additional serious concerns with this practice that are addressed at the end of this submission.

25. This appears to be the first time that Police Scotland have referred to 'digital devices' and 'internet of things' in documentation disclosed to the External Reference Group. We therefore believe that there has been a lack of transparency or openness in relation to the intention of Police Scotland to extract data from connected devices. This may also be the consequence of Police Scotland and the External Reference Group not discussing cybercrime hubs. The ERG has focused on cyber kiosks whose purpose is to triage mobile phones.

26. In the disclosed documents the fact that 'digital devices' is a broad term including internet of things, is given no prominence, which gives the sense that it is being treated by Police Scotland as a side note. This is extremely worrying and raises questions as to Police Scotland's understanding in relation to the complexities and risks relating to using connected devices within investigations and as a form of intelligence gathering.

27. It is strange that this has not been drawn to the attention of the External Reference Group until now. It appears to have come to light due to the welcome desire to discuss issues relating to victims and witnesses. It is through the disclosure of documents relating to extracting data from the phones of victims and witnesses that reference has been made to 'digital devices' and internet of things.

28. The extraction of data from digital devices beyond mobile phones is an issue that therefore appears more relevant to the cybercrime hubs than the kiosks. This may be why the External Reference Group have not discussed this. However, this feeds into concerns raised by a number of groups about the opacity and secrecy surrounding cyber crime hubs.

Cyber crime hubs

29. It is notable that Police Scotland have failed to answer the Justice sub-committee on Policing's questions regarding cybercrime hubs. Given the External Reference Group have repeatedly raised concerns about the lack of transparency relating to extraction, we question how the victim or witness will be 'informed' at this stage.

30. It is acknowledged that the Justice Sub-Committee and ERG's remit relates to cyber kiosks and not cybercrime hubs. However, this highlights the artificial nature of separating these, especially when much of the documentation the ERG are being asked to consider relating to victims and witnesses relates to extraction and examination which is done by hubs not kiosks.

31. The Sub-Committee questioned Police Scotland regarding cybercrime hubs and asked for the following information:

    - Copies of the formal proposal by Police to create the initial cyber hubs and then to extend the number to 5, the date/s that these proposals were considered and approved by the Scottish Police Authority Committees / Board
    - The location of the initial 3 hubs and then the additional 2 cyber hubs
    - Details of the equipment to be included in the hubs, the rationale for their use and the date/s when these proposals were considered and approved by the Scottish Police Authority Committees/Board. Also details of any contracts published following these decisions.
    - Details of the process and engagement undertaken by Police Scotland to ensure that the hubs were using processes and equipment that were legal and satisfied human rights, privacy, data protection and security requirements, including copies of any equalities impact assessments, and data protection impact assessments made at the time of approval etc.
    - Details of any equipment used in the hubs that can capture, access or download data from mobile devices.
    - Details of how the processes undertaken in the cyber hubs differs from practice prior to the establishment of Police Scotland to capture, access or download data from mobile devices.
    - Details of Police Scotland's consideration of informed consent from those whose phones etc. are to be sent to the hub, in particular, witnesses.

Legal basis and rights of the individual

32. Privacy International note that Police Scotland state in the disclosed documents that that the voluntary provision of devices by victims and witnesses (i.e. consent to hand it over) to the police is nothing new. However, they have failed to state the legal basis upon which this transaction takes place, which would inform the rights and protections

afforded to the victim or witness when they choose to hand over their device.

33. It is noted that consent is not used in relation to suspects. Thus, any reference to consent in this document relates only to victims and witnesses. In relation to suspects and indeed for examination of phones of victims and witnesses, Police Scotland rely on a patchwork of common law and statutory powers, which is in and of itself problematic. This has been highlighted by Privacy International in previous submissions to Police Scotland and the Sub Justice Committee on Policy of the Scottish Parliament.

34. Aside from keeping a record that an individual has 'consented' to hand over their phone i.e. done it voluntarily rather than the police using a power of seizure, it is unclear whether it gives the individual any rights.

Should the phone be the starting point

35. We are concerned that the starting point for Police Scotland is very much focused on taking a victim's phone and extracting all data with the potential of conducting a detailed examination. The intention, apparent from the documents disclosed, is not so much to use the kiosks but to extract data. This is demonstrated in all the disclosed documents and flow charts which indicate at the point of reporting, the phone will be sought, and consent information documents provided. Although Police Scotland do state the phone can be provided at any time.

36. It is suggested that this is the wrong starting point. The starting point is that a victim's phone is not relevant in every case. The issues in the case should be looked at and for example, the suspect interviewed. This will help ensure that only what is strictly necessary and reasonable is examined, should it be relevant. The focus on mobile phone evidence, particularly in cases where it is not clear why it is relevant, will only increase fear that the police and prosecution seek the phones of victims in order to discredit them, rather than to investigate the serious crimes they report.

37. In relation to Police Scotland stating that they are doing 'nothing new', again Police Scotland are failing to appreciate what makes handing over a smart phone today very different from even a few years ago and handing over a connected device equally novel. We have elaborated on this point in our previous submission[2] and do not repeat those submissions here. It is disappointing Police Scotland maintain this narrative despite critique not only from members of the External Reference Group, but Members of the Scottish Parliament.

Can consent be relied upon for seizure

[2] https://privacyinternational.org/report/3202/old-law-new-tech-and-continue-opacity-police-scotlands-use-mobile-phone-extraction

38. Police Scotland have stated in correspondence and at the External Reference Group that the use of 'consent' to seize a phone relates to 'policing by consent'. Police Scotland use this rather than 'voluntary' because of the three critical components of consent being voluntary, informed and capacity.

    - Voluntary: the decision to either consent or note must be freely made by the person and free of coercion, pressure or influence.

    - Informed: the person must be given information about what the process of taking and examination involves and their rights in terms of providing, refusing and withdrawing consent.

    - Capacity: the person must be capable of giving consent, which means they understand the information given to them and can use it to make an informed decision.

39. We do not accept that Police Scotland's use of consent to seize a phone meets the above critical criteria. Therefore, we do not accept they can rely on consent to seize the phone of a victim or witness.

40. In relation to 'voluntary', Police Scotland are seeking consent at a time when an individual is highly likely to be traumatised. We question whether an individual's consent to hand over their phone can be freely made, given the power imbalance between the police and a victim, particularly when the victim has not recourse to legal advice or support at the time of the decision.

41. We note the comments by Claire Waxman, London's first victims' commissioner, who stated recently that "People feel very pressured to consent. Victims don't want to share all their personal details even if it's only with the CPS and police. It's a risk they don't want to take."[3]

42. In relation to 'informed' we question what this means when Police Scotland have not disclosed any documentation which explains for example how the extraction works, what data may or may not be taken, what limits there are on what the Police will review, how retention and deletion operates. A more detailed list of the issues we believe should be discussed with victims and witnesses is below. As noted above, the need for more detailed information underlines the need for a Standard Operating Procedure, policy or guidance document.

43. There is an assumption that individuals will be able to understand or be aware of the volume of data that is on their phone and what can be extracted from their phone e.g. location data can be taken from photos, messages, cell towers and Bluetooth devices.

[3] https://www.theguardian.com/society/2019/nov/10/half-of-victims-drop-out-of-cases-even-after-suspect-is-identified

44. There is little to no consideration that individuals will not have any technical understanding of mobile phone extraction. The degree to which they are 'informed' apart from extremely basic information the police might provide is questionable.

45. We are unclear how Police Scotland intend to assess 'capacity' i.e. that an individual has understood the information that has been given to them. There is no indication of advocacy or support. There is no indication of access to legal advice at the time of signing over a device.

What is needed to inform an individual

46. To elaborate on the 'informed' aspect of consent, Police Scotland state that part of the 'consent' is that the individual is informed. i.e. they must be given information about what the process of taking and examination involved.

47. We suggest that if Police Scotland wish to truly protect the rights of victims and witnesses, there should be greater transparency around cybercrime hubs, which is where the extraction takes place, and greater transparency, information and involvement of the victim or witness throughout the process in relation to:

Extraction

- What data has been extracted (different from examination e.g. full physical extraction);
- Whether it is possible to selectively extract certain types of data i.e. extract via type;
- If yes, whether they will restrict the extractions to certain types of data;
- If no, and they have to extract all data, what limits exist in relation to the examination of the data i.e. how is the police officer who is viewing the data restricted to looking only at what is strictly necessary and proportionate.
- Whether it is possible to selectively extract data by type and time frame i.e. extract only messages relating to a certain period;
- If yes, whether they will restrict the extraction to this;
- If no, and they have to extract all data, what limits exist in relation to the examination of the data i.e. how is the police officer who is viewing the data restricted to looking only at what is strictly necessary and proportionate.
- Whether internet connection is disabled at the cybercrime hubs
- Whether cloud extraction is used at cybercrime hubs for mobile phones and/or other digital devices.

Examination

- What data will and has been examined e.g. provision of a list of data types, dates etc.
- How the police decide which data to examine;

- What independent checks exist to ensure that the police only examine what is strictly necessary;
- What auditing exists to ensure that Police Scotland only examine what is strictly necessary and reasonable in relation to the investigation;
- Is all extracted and examined data retained;
- On what basis is irrelevant data retained and not deleted.

Disclosure

- What data will the police disclose to the suspect;
- What details will be provided to the victim/witness in relation to a detailed description of the data provided to the suspect.

Legal advice and support

- what legal advice and support will be offered to a victim or witness prior to a discussion about handing over the phone.

48. The above is by no means an exhaustive list. We believe it should be the basis for a Standard Operating Procedure / guidance or policy

49. We are aware that the police have held focus groups where they have discussed the use of the term consent. Given the highly confusing use of consent in the documents disclosed, we do not accept the outcomes of these focus groups as supporting the way the police wish to use and document consent. The police's own documentation is misleading, particularly where data protection terminology is used, and reference is made to the Data Protection Act 2018. We note these in our comments below on the documents disclosed.

50. We are also concerned that it has not been adequately demonstrated that these focus groups have full understanding that once their phone is in the possession of the police, withdrawal request may have little impact apart from being noted on the file. This is supported by the evident confusion at the External Reference Group meeting in November at Police Scotland's approach.

51. Privacy International have repeatedly stated that the police should obtain a warrant if they wish to seize and examine a phone. We believe that there may be good reasons that Police Scotland should be required to obtain a warrant to seize and examine a phone or at the very least to examine the phone of a victim or witness. The requirement of a warrant would ensure independent oversight into what data is examined and provide a layer of protection to ensure that it is only that which is strictly necessary.

52. If Police Scotland maintain that a warrant would be impractical, we do not accept the alternative of consent. As stated above, given the consensus among the External Reference Group that the group has noted that the use of 'consent' as a legal basis for seizure can be nullified by the use of another power i.e. at the point of examination, we agree this affirms the

view that the current legal framework is inadequate. This particularly relates to the use of 'consent'. It is not fit for purpose.

Does withdrawal have any real impact?

53. Given that a phone is handed over for the purpose of examination, if an individual were to withdraw that consent:
    - Does withdrawal come with any legally enforceable rights for the phone to be returned? Police Scotland explicitly state in the disclosed documents (see below) that withdrawal of consent **does not** mean the police have to return the phone.
    - Thus, if the phone is taken for the very purpose of examination, the assumption must be that on most occasions the police would not return it. They state they have other powers to then keep the phone for examination, so it does not matter if consent is withdrawn.
    - If the phone is already being subject to examination, then withdrawing consent has no impact. Although if the data has been extracted the phone may then be returned but the collected data will be retained.
    - We suggest that there will be few instances where a phone taken 'by consent' will be returned if consent is withdrawn.

54. We believe that whether a phone is returned or no when consent is withdrawn, this should be an issue that is easily auditable i.e. in what number of cases where consent was the basis for seizure, has consent been withdrawn but the phone has not been returned. And then in what number of these cases (where they withdrew consent) has the victim dropped the prosecution if the police refuse to return the phone.

Is consent misleading

55. That Police Scotland are heavily focusing on the point at which the phone is handed over gives an illusion of involvement and empowerment of the victim or witness.

56. We therefore believe that use of the term consent and the added documentation behind it i.e. leaflets, forms, flow charts, is misleading as it gives the impression that the victim or witness is empowered by this process, when in fact, if they withdraw their consent, the police can continue to examine their phone, as the examination is carried out using separate powers and has nothing to do with the voluntary provision of the phone.

57. We are concerned that whilst the individual can 'withdraw' consent, the only real impact, as is clear from the documentation disclosed by Police Scotland, is that the withdrawal is noted on the file. The police keep the phone because they have taken it for the purpose of examination.

58. We are concerned in many cases this makes 'consent' meaningless and will undermine trust of victims in handing over their phone to Police Scotland. Since once the police have the phone, which they have explicitly seized for the purpose of examination, they are going to examine it, and there is nothing the individual can do about that. There may be rare occasions it is returned before examination, but we believe this will be the exception rather than the norm.

59. Furthermore and importantly the position of 'consent' for seizure of a phone does not resolve the discussion that has been ongoing for well over a year regarding clarification of Police Scotland's legal basis for processing personal data on mobile phones via the kiosks and then later the hubs (whether examination or extraction or any other processing operation). The deficiencies of the current legal framework taken together with the unsurmountable hurdles in overcoming the imbalance of power and relying on consent remain.

Questions for Police Scotland

1. What is the relevant statutory authority for the use of consent to seize digital devices?

2. Does Police Scotland have any projected statistics for the number of phones that are seized based on 'consent'; in how many of these cases will victims and witnesses withdraw consent; and in what number of cases the police will nevertheless examine the device despite consent being withdrawn?

3. Is there an intention to keep statistics in relation to the above and make these figures publicly available?

4. What information do Police Scotland intend to provide in relation to victims and witnesses in relation to:
    a. Cybercrime hubs;
    b. What data types and date range of data will be extracted from phone or other digital device;
    c. What data types and date range of data will be examined from the phone or other digital device;
    d. What search parameters will be applied to extracted data;
    e. Whether data examined went beyond the envisaged type and date range and what was actually examined;
    f. What data will be disclosed to the suspect;

5. Do Police Scotland accept that a briefcase is not an accurate comparison to the volume and types of data that are stored on a phone or internet of things device.

6. Do Police Scotland accept that if an individual consents to seizure of their phone, withdraws consent, but Police Scotland relies on legal basis to examine the phone, the only impact of withdrawal is that it is noted on the file.

7. It is understood that sim cards are removed, and mobile phones are not connected to the internet when examined at the cyber kiosks. Does the same apply when phones are examined at the cybercrime hubs?

8. At the cybercrime hubs can the phone be connected to the internet and is cloud extraction possible either for phones or internet of things devices?

9. What definition of IOT do Police Scotland rely on?

10. Once again, please can Police Scotland, with reference to Police Scotland's statutory and common law powers, confirm which legal basis under the Data Protection Act 2018 they are relying on for the data processing involved in examination and extraction of mobile phones and why this is considered sufficient?

Submissions on the documents

Consent Leaflet v2.1

Question 1:

60. Police Scotland state explicitly that taking a device from a victim or witness is 'for the purpose of examination'.

61. Police Scotland state that this requires 'lawful authority' but do not clarify the lawful basis for using 'consent.'

62. Police Scotland use the term 'consent' as a lawful authority to take the phone for the purpose of examination. However, this is different to the use of term 'consent' which is also referenced by Police Scotland when discussing the lawfulness of processing data. Consent in this context merely refers to 'Where a victim or witness is willing to provide their device voluntarily.' It has no relation to Data Protection Act 2018.

63. As noted above, we do not believe that relying on consent is appropriate given the requirements to be voluntary, informed and with capacity. The legal basis for seizure is still unclear.

64. Whilst we oppose the use of 'consent' to seize the phone, if Police Scotland do continue to rely on this, it should be made absolutely clear that this has no relation to consent as understood under the Data Protection Act 2018

(DPA). We further suggest that a separate term should be used, as is done in the Data Protection Impact Assessment, such as 'voluntary submission'.

65. Police Scotland needs to be more explicit that they believe there are two separate steps in relation to devices i.e. seizure and examination, whereby seizure, in the view of Police Scotland can include voluntary submissions.

66. Police Scotland need to be clear what the 'take' stage can relate to e.g. investigation, court proceedings, prosecution etc. It is unclear whether the phone is only taken from a witness in relation to court proceedings from the way the response is phrased.

67. The response on 'examine' is extremely confusing, unclear and we believe incorrect. It states:

    i. "The Data Protection Act 2018 allows police to keep and use information taken from a device for the investigation, even if you withdraw your consent for police to keep the device itself."

68. This gives the impression of referring to consent as defined under DPA 2018, whereby withdrawal of consent would mean the police cannot keep the device. It also reads, perhaps unintentionally, that it is the DPA that nullifies consent if withdrawn.

69. It is accepted now by Police Scotland that they cannot rely on consent as a basis for processing data obtained from mobile phones.

70. It is unclear why the Police are citing the Data Protection Act 2018 as a 'power' to examine the device i.e. the lawful basis for processing. This is the question that they state they are answering in Q1. Again this goes back to the point made from the beginning of the reference group that Police Scotland must be in a position to point to a clear and appropriate legal power.

71. The DPA 2018 requires that if the police are to process data:

    - It must be lawful and fair;
    - The purpose must be specified, explicit and legitimate
    - Personal data be adequate, relevant and not excessive
    - It be kept no longer than necessary
    - Processed in a secure manner.

72. Given that mobile phone and internet of things data will generally include sensitive personal data / special category data the processing must be strictly necessary for the law enforcement purpose and meet at least one of the conditions in Schedule 8.

35 The first data protection principle

(1)The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2)The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a)the data subject has given consent to the processing for that purpose, or

(b)the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3)In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4)The first case is where—

(a)the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5)The second case is where—

(a)the processing is strictly necessary for the law enforcement purpose,

(b)the processing meets at least one of the conditions in Schedule 8, and

(c)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(6)The Secretary of State may by regulations amend Schedule 8—

(a)by adding conditions;

(b)by omitting conditions added by regulations under paragraph (a).

(7)Regulations under subsection (6) are subject to the affirmative resolution procedure.

(8)In this section, "sensitive processing" means—

(a)the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b)the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c)the processing of data concerning health;

(d)the processing of data concerning an individual's sex life or sexual orientation.

73. If Police Scotland believe that the DPA 2018 gives them the 'power to examine the device', to keep and use the information taken from the device for investigation, they must elaborate on this and provide reference to specific sections of the DPA 2018 and as pointed out throughout this process be able to point to Police Scotland's specific powers that they are relying on.

74. Please note that we maintain our position in relation to the legal basis relied upon by Police Scotland as set out in our submissions dated September 2018[4]. In summary we believe that the legal basis relied upon by Police Scotland is deficient.

Suggested new Question:

75. If Police Scotland continue to rely on voluntary submission we believe greater clarity is needed. For example:

76. Q. If I agree to hand over my phone, can I withdraw my agreement?

- If you agree to hand over your phone to the police, whilst you can 'withdraw' your consent, this does not give you any right to get it back from Police Scotland. This is because once Police Scotland have your phone for the purpose of examination, they rely on the legal powers to examine the data on the phone that are not reliant upon your voluntary agreement.

- You can however inform them that you withdraw your agreement, which will be noted on the file. But that does not mean that you will get your phone back.

Question 2:

77. Question 2 asks 'If police ask for my consent, do I have to give it?

78. As we have set out we do not believe the criteria for consent can be met and Police Scotland have not stated the legal basis for 'consent'.

79. It should also be clarified that if the individual choses to withdraw consent or agreement to hand over their phone, this does not mean that it will be handed back and the examination will not take place.

Question 3:

80. The question should be redone to read: What happens if I refuse to hand over my phone?

[4] https://privacyinternational.org/report/3202/old-law-new-tech-and-continue-opacity-police-scotlands-use-mobile-phone-extraction

81. The answer should be improved e.g. It is your decision whether or not you decide to hand over your phone. You can decide whether you want to hand over your phone at any stage of the investigation and proceedings and you may want to discuss whether to do this with a legal representative or victims' rights charity (provide details). Your decision will not affect how we treat you or the enquiry and it will not stop us from investigating all other reasonable lines of enquiry.

    Please note that as the investigation progresses and particularly if it proceeds to prosecution, if we believe there is evidence on your device, we may use other powers to seize your phone without your voluntary agreement.

Suggested new Question:

82. It is suggested that a Q&A is needed as follows: 'If the police seize my phone without my agreement, how are my rights protected?

83. Police Scotland need to come up with an answer to this.

Question 4:

84. Question 4 asks: The police have my device, what happens now?

85. In the answer the police only say 'necessary'. However, they will be processing sensitive personal data so this should state 'strictly necessary'.

Suggested new Question:

86. It is suggested that a Q&A is needed as follows: 'The police have my phone, can they look at everything and will they keep everything?

87. Police Scotland need to come up with an answer to this.

Suggested new Question:

88. It is suggested that a Q&A is needed as follows: 'The police have my phone, will they give all my information to the suspect?'

89. Police Scotland need to come up with an answer to this.

Question 6:

90. No mention is made here of the defence / suspect or others who might examine and view the information. This needs to be reconsidered.

Question 9:

91. This is insufficiently clear as to what information the victim or witness will be told. It needs to be clarified whether they will be told e.g. which data types have been examined, from what time frames, whether system and deleted data has been recovered, the type of extraction performed etc.

92. It is necessary to provide this information for example, should the information extracted be disputed and the victim wish to instruct a separate forensic examination of the device.

Question 11:

93. To improve this question, we seek the following from Police Scotland:

94. **Please can Police Scotland confirm that you will attempt to conduct a full extraction.**

95. **Please can Police Scotland confirm whether or not you will retain the full extracted data rather than only that which is strictly necessary and proportionate.**

96. **Please can Police Scotland clarify how you will only look at information that is strictly necessary and proportionate and how this will be documented and subject to independent audit.**

97. The statement on page two 'Withdrawing your consent'. As explained earlier withdrawing consent is rendered meaningless as the phone will not be returned in every circumstances.

98. Please delete the section 'Your decision regarding consent' as given the concerns expressed above this risks being meaningless. Alternatively, it should be re-phrased.

100. It is notable that the stated purpose of this document is: 'The Service seeks the introduction of an enhanced practice for capturing consent from victims and witnesses when required for the purpose of digital device examination.'

101. This is confusing or misleading given all the concerns expressed by Privacy International and others in the ERG regarding consent and the difficulties with relying upon it as a legal basis for examination.

102. It is clear from this document that the seizure or 'voluntary' taking of the device, which is the subject of 'consent' is inextricably linked to 'examination' at which point the victim or witness has no power withdraw 'consent' (apart from the fact that it will be noted on a form) or stop the examination of the data on the phone.

103. It is therefore unclear what role 'consent' plays apart from providing the police with an easy way to seize the phone rather than the police using other powers to take possession.

104. It would be important to document and audit the statistical impact of the use of consent and relatively powerless nature of 'withdrawal' on the impact on victims. In particular whether it results in victims dropping prosecutions. i.e. a victim withdraws their consent, is told that it does not mean that they will be given their phone back, and so drops the prosecution of the accused.

105. As was recently reported in the Guardian[5], half of rape victims in England and Wales drop out of cases even after suspect is identified. It stated that "tens of thousands of women are reluctant to pursue their alleged attackers when faced with invasive disclosure demands" among other factors. It goes on to state that "One of the most concerning changes is the growing proportion of cases resulting in "outcome 16", whereby a suspect has been identified after a police investigation, but the victim does not support further action. The document reveals that from 2015 to 2018, the proportion of cases dropped owing to an outcome 16 rose from 33% to 48%."

106. In the first section of the impact assessment, in relation to 'how is consent from victims and witnesses captured' it states that 'When being asked for consent to provide their device(s) to police for the purpose of examination, a victim or witness should be made fully aware of what is being asked of them, what the process entails and their rights in terms of provision, refusal and withdrawal.'

[5] https://www.theguardian.com/society/2019/nov/10/half-of-victims-drop-out-of-cases-even-after-suspect-is-identified

107. In relation to 'what is being asked of them, what the process entails and their rights in terms of provision, refusal and withdrawal' we dispute that any of the disclosed document achieves this. We note our submissions above regarding the transparency needed in relation to extraction, examination and disclosure/sharing.

108. Police Scotland refer to refusal and withdrawal. It is unclear on what basis withdrawal is more than something theoretical given that once the phone is to be subject to examination, any withdrawal of 'voluntary agreement' has little to no bearing on what the police do.

109. The 'consideration section' is confusing.

110. Police Scotland say that obtaining consent is nothing new. Whilst that may be the case, they do not state the legal basis upon which this transaction takes place and how individual rights are protected or what is legally enforceable.

111. Further reference is made to 'withdrawal' of consent. We note our earlier comments that this is more a theoretical withdrawal and has no practical impact. From our understanding of Police Scotland's position, if the victim withdraws consent for 'seizure' it does not make any difference to examination taking place.

112. In relation to the 'examination' on page 4, it states examination must be necessary. Given that data is likely to be sensitive personal data, this should be 'strictly necessary' in accordance with section 35(5)(a) of the DPA 2018.

113. There is reference on page 6 to the 'legal requirement for consent to take possession of digital devices'. It is not clear what this relates to. Please specify.

114. Reference is made (page 6) to 'informed consent'. This is similar or the same as data protection terminology and is confusing when the consent relied upon as we understand it has nothing to do with the Data Protection Act 2018.

115. On page 6 it refers to 'Concerns raised through consultation and broader evidence bases have focused on enhanced information to support informed consent in particular:

- Access, review, processing and management of data within digital devices held by Police.
- The amount of time Digital Devices are held by Police/COPFS
- The legal basis for the seizure and examination of the digital devices
- Dependency on digital devices in the modern era
- Understanding, accessibility and foreseeability of Police processes, powers and terminology.'

116. It is notable that concerns have related to police 'terminology'. This underlines the point we keep making about the misleading use of 'consent' and reference to 'informed consent' and 'withdrawal of consent.'

117. Later in the document it also states that 'Feedback from Youth Work organisations (through consultation) has highlighted that young people struggle to understand some of the language used by Police Scotland and the impact that such a process may have on them and their rights.'

118. We note that the concerns raised by consulted groups have a particular focus on the examination stage i.e. processing of sensitive personal data, at which point consent is not a lawful basis for processing. The documents on consent does nothing to address these concerns. We note our statements above regarding extraction, examination and disclosure/sharing. This is the information that individuals need.

119. Police Scotland discuss victims of sexual crime. However, they have failed to demonstrate that they have considered that at the time an individual report a serious sexual offence they are likely to be in a state of distress and this compromises the ability to give informed consent.

120. In considering the impact on the use of mobile phone extraction on a number of different sections of the Human Rights Act 1998, Police Scotland have not demonstrated consideration of the impact of extracting vast quantities of data that include data related to third parties. This could mean that victims/witnesses are put under pressure not to indicate there is evidence on phones because the police will extract all data including third parties and there is no clear limit to what is examined.

Digital Device Consent Capture Flow

121. We have been explicit on our concerns about the use of consent above.

122. We do not understand the sentence: "The Data Protection Act 2018 permits police to keep and use information extracted from a device, even if you withdraw your consent for police to retain the device itself." We request more information on what Police Scotland mean, what parts of the DPA 2018 they are referring to.

123. The flow chart refers to consent as 'lawful authority'. Further information is requested on the relevant legislation that makes this lawful authority.

Digital Device Consent Withdrawal Flow Process

124. As above regarding the statement in the left-hand box referring to DPA 2018.

Digital Device Examination Request Form Flow Process

125. We welcome the clarity in the top left box that the device can be taken even if consent is refused and that the device can be retained despite withdrawal. This is the reality of the weakness of consent.

126. We note our comments above on the citation of the DPA 2018.

127. We note that at the examination stage there is nothing that signifies examination should be limited to that which is strictly necessary.

Digital Device Examination - Principles

128. We note that on page 1/2 it states that the legitimate purposes of digital device examinations are to preserve life; determine whether or not the contents of the device are of relevant evidential value; to capture evidential material.

129. We are concerned with the way that this is phrased in that it appears that is could justify a fishing expedition for content of evidential value.

130. We have made detailed submissions in relation to the DPA 2018 and Human Rights Act 1998 in previous submissions and do not repeat those here.

131. No reference is made to audit of cybercrime hubs, only kiosks. (page 7)

Digital Device Journey Request Flow Process

132. The flow diagram does not indicate why 'reasonable grounds' might exist to believe that a device of a victim or witness of crime holds evidence relevant to the investigation. Further elaboration is needed by Police Scotland how this is fact specific to the investigation i.e. would the suspect already have been interviewed; how reasonable grounds are reached.

133. At the 'Does device contain evidence' question in the flow process, this needs further elaboration and documentation. If this is to lead to the examination of the device then it needs to be very clear on what basis it is believed that the device contains evidence and what evidence exactly will be examined.

134. It is noted that the flow process states: extracted contents reviewed by Investigating Officer; relevant evidence identified? It is not clear what limits exist at the examination stage and where the protections of only looking at what is 'strictly necessary' is embedded in the process.

Data Protection Impact Assessment – Cyber Kiosks

135. Our comments made in our previous submission on the Data Protection Impact Assessment remain.

136. Q3 states that "The search for evidential material can be filtered, directing the triage to specific areas such as Text messages, Call Data, Chat (Whats app / Snap chat), Multimedia (Audio, Video, Photographs) Internet history, Email etc."

137. Q5 states that "Focused Triage, allowing investigators to target specific, relevant areas of the device, for example, text messages, photographs etc., thus minimising intrusion into personal data."

138. It is unclear whether Police Scotland are indicating that selective extraction is possible or whether they are referring to search parameters that 'can' be applied but might not always be applied.

139. Q3 goes on to state that "This also includes the ability to limit the search using date range of keyword search criteria."

140. We note that in Q3 Police Scotland use terminology such as 'submitted' and 'obtained voluntarily' and 'voluntarily submitted' rather than using 'consent.' If Police Scotland are happy to use this terminology in the DPIA it is unclear why they can't use the same for the public facing documents.

141. We note that Q11 states that "A digital device can be regarded as being the electronic equivalent of a briefcase or filing cabinet, where the device is often protected by some sort of barrier or lock which requires a PIN or password to access its 'contents'. We have previously criticised this kind of comparison in our previous submission[6].

142. As noted above we do not agree with and we and others have repeatedly raised questions and concerns regarding Police Scotland's legal basis for seizure and examination.

143. Q11 section 6 Data Processing is confusing. It states that 'subsequent processing of recovered personal data is permitted by the DPA 2018'. We have explained above the DPA 2018 cannot be relied upon to provide lawful basis for processing personal data, but if Police Scotland are going to process personal data then this must be done in a way that is in accordance with the DPA 2018. Therefore, '6.1' should state that 'Any subsequent processing of recovered personal data must be in accordance with the DPA 2018.'

[6] https://privacyinternational.org/sites/default/files/2019-09/Review%20of%20Police%20Scotland%20Inquiry%2011%20September%202019.pdf

144. We are not aware that the 'information on the Kiosk and general digital device forensics' has been disclosed to the External Reference Group. (page 38). We request a copy.

Audit

145. Further thought needs to be given to how seizure and extraction of phones belonging to victims and witnesses is subject to independent audit.

146. This includes:
    - How many phones now go to the cybercrime hub
    - What is the anticipated reduction as a result of the cybercrime kiosks
    - How will this be audited

Selective Extraction

147. Privacy International has written about the use of selective extraction in mobile phone extraction[7].

148. Police Scotland have contracts with Cellebrite. Cellebrite state that they now support selective extraction, meaning that police investigators need only collect data from a device that is strictly relevant to the case in question[8]. However, we believe that the reality is more complicated as we have set out in our recent review of selective extraction[9].

149. Police Scotland indicate that they can limit what is 'viewed' or 'examined' using parameters (but not all the time). However the recently disclosed documents indicate that they would conduct a full extraction so all data on the phone would be collected and retained by Police Scotland.

150. We ask the following questions specifically to Police Scotland:

    - Does the extraction at the cybercrime hubs work by extracting all data and then limiting what a police officer can view via search parameters?
    - Or, can you limit the types of data that are extracted from the phone?
    - Or, can you limit the type and data range of data that is extracted from a phone?
    - If you extract all data / all data of a certain type and then limit at the examination stage, is all the data collected and retained, even if it is not examined?

[7] https://privacyinternational.org/news-analysis/3281/can-police-limit-what-they-extract-your-phone
[8] https://privacyinternational.org/news-analysis/3281/can-police-limit-what-they-extract-your-phone
[9] https://privacyinternational.org/news-analysis/3281/can-police-limit-what-they-extract-your-phone

- What processes and procedures do you have in place to ensure that search parameters are applied?
- What procedures do Police Scotland carry out in order to determine / assess what is strictly necessary.
- Is the system set up to ensure that it is possible for independent audit to take place to review whether examination has been misused, abused or more data that is strictly necessary has been processed.

Internet of things

151. Police Scotland state in the disclosed documents that consent i.e. voluntary submission can be relied upon to seize connected devices. Exploiting connected devices or internet of things (IOT) by law enforcement raises new challenges and risks that have not been sufficiently explored by Police Scotland.

152. We have little understanding of the capabilities of many IOT devices and often do not realise for example how insecure they are. Barbie's connected smart doll released in 2015 came equipped with a microphone, voice recognition software and AI that allowed a call-and-response function between the child user and the doll. The device lacked security[10].

153. In a separate example, a smart light bulb, just through collecting and analysing when it is turned off and on, can learn household behaviours. In 2017 it was reported that whilst vacuuming your home, Roomba 980's sensors could report on the size of a home and amount of furniture[11].

154. Devices log, process and transfer vast amounts of data about some of the most intimate parts of our everyday lives, often without the owner of that device realising. The owner of a device may not know what data the device collects, shares and stores. Whilst some may be visible to the user via a screen interface, a large amount if invisible.

155. Given that we are often ignorant of the capabilities of the devices that we own and surround us, we do not believe that individuals can be 'informed' and thus consent cannot be relied upon to seize these devices.

156. Police Scotland have failed to demonstrate that they have considered issues such as information asymmetry, power imbalance, quality and reliability of evidence and device insecurity in terms of whether consent can be relied upon, due to the level at which the individual must be 'informed' and have 'understanding'.

[10] https://privacyinternational.org/long-read/3026/my-fridge-my-witness

[11] https://privacyinternational.org/long-read/3026/my-fridge-my-witness

157. Users do not know the full range of data that connected devices generate, what is collected by servers and what persists on the device itself. This is through no fault of the user, rather a systemic problem within such devices.