Police, Crime, Sentencing and Courts Act 2022

Extraction of Information from Electronic Devices: Draft Code of Practice

Home Office

Consultation

Response

July 2022

For further information contact

Tyrone Steele, Criminal Justice Lawyer
Email: tsteele@justice.org.uk

JUSTICE, 59 Carter Lane, London EC4V 5AQ
email: admin@justice.org.uk website: www.justice.org.uk

Introduction

1. JUSTICE is an all-party law reform and human rights organisation working to strengthen the justice system. It is the UK section of the International Commission of Jurists. Our vision is of fair, accessible and efficient legal processes in which the individual's rights are protected and which reflect the country's international reputation for upholding and promoting the rule of law.

2. This response addresses JUSTICE's concerns with the Home Office's draft Code of Practice on the extraction of information from electronic devices (May 2022) (the "**Draft Code**"), issued pursuant to the Police, Crime, Sentencing and Courts Act 2022 (the "**Act**"),[1] and its corresponding consultation (the "**Consultation**").[2] The Act includes powers for authorised persons to extract information from electronic devices in certain circumstances.[3] Section 37 allows authorised persons to extract information for the purpose of preventing, detecting, investigating, or prosecuting crime; locating a missing person; or protecting a child or at-risk adult from neglect or physical, mental or emotional harm.[4] This power is only exercisable where the user of the device has voluntarily provided the device to the authorised person and that user has agreed to the extraction of information from the device.[5]

Effect of the Code

3. The Draft Code states that an authorised person, when deciding whether to exercise the section 37 power or the extent to which to exercise it, must have regard to the Code of Practice. Paragraphs 12 to 14 set out the consequences for the failure of an authorised person to abide by the Draft Code. While the Draft Code notes that failure to abide by its requirements does not make the authorised person liable in civil or criminal proceedings, it explains that such failure could be admissible as evidence in criminal or civil proceedings,

---

[1] Home Office, "Extraction of information from electronic devices: Draft Code of Practice" (May 2022).

[2] Home Office, "Open consultation - Extraction of information from electronic devices: code of practice" (Updated 11 July 2022)

[3] Per s.44(2) of the Act, which provides that for the purposes of section 37, an authorised person includes police officers and police constables, British Transport Police, Ministry of Defence Police, members of the military, and immigration officers.

[4] Police, Crime, Sentencing and Courts Act 2022 s37(2).

[5] *Ibid* at s37(1).

and may be taken into account by the court in deciding any question in the proceedings.[6] However, this all simply repeats what is already set out in the Act.[7] Beyond this, the Code merely states failure to comply with the Code could result reports to the Information Commissioner or that it could result in unspecified professional disciplinary consequences.

4. We consider the lack of more detailed explanations which set out the implications for authorised persons who unlawfully engage the Act's powers to be a serious oversight. Failure to follow the Act and the Draft Code has the potential for serious consequences for victims of sexual offences, the organisation the authorised person is employed within, and the authorised person themselves. [8]

Victims of Sexual Offences

5. The Draft Code does not properly explain how serious an effect a failure to follow its requirements has on victims. Paragraph 128 emphasises that victims of rape and other sexual offences may be particularly concerned about sharing sensitive information.[9] Further, paragraph 116 acknowledges that a primary reason why victims of these offences may withdraw their complaints is the possibility of having to hand over personal and sensitive information[10] Aside from this, the importance of authorised persons following the Draft Code to protect the dignity and humanity of sexual offence victims is given insufficient attention. Such victims have described the process of electronic extraction as causing them to feel as if they are under suspicion rather than the suspect themself.[11]

6. This underlines the need for a careful and considered approach to electronic extraction, which the Draft Code should provide. Electronic extraction that goes beyond an intrusion into a user's private life that is necessary and proportionate, or fails to follow proper procedure and process, is dehumanising, and in particular for victims of sexual offences. As such, the Draft Code should make clear upfront in the section which explains consequences for failure to abide by its requirements.

---

[6] *Supra* note 1 Home Office, at para. 12-13.

[7] Police, Crime, Sentencing and Courts Act 2022 s37(11), s42(9)-(10).

[8] *Supra* note 1 Home Office at para. 14.

[9] *Ibid.* at para. 128.

[10] *Ibid* at para. 116.

[11] Big Brother Watch, Amnesty International, Centre for Women's Justice, Defend Digital Me, End Violence Against Women, Fair Trials, JUSTICE, Rape Crisis England & Wales, the Survivors' Trust, Liberty, Privacy International, 'Report Stage Briefing on digital extraction powers in the Police, Crimes, Sentencing and Courts Bill for the House of Lords' (December 2021), p.9.

Judicial Review

7. Paragraphs 12-14 do not inform authorised persons that breaching the Act, as distinct from a breach of the Draft Code, could lead to judicial review of the authorised person's actions. If an authorised person uses the power conferred by section 37 to extract information from electronic devices in a manner that exceeds or does not comply with the Act, (e.g. for a purpose *not* specified in section 37(2)),[12] then such action would be *ultra vires* ("beyond the powers") and the court could strike it down.[13] At no place is this mentioned with the Draft Code.

Data Protection Law

8. Paragraphs 21-30 explain that an authorised person should act within the scope of data protection laws.[14] However, the Draft Code fails to set out the consequences of a potential breach of data protection law could have. The extraction of electronic data from a device would amount to processing in terms of the Data Protection Act 2018 (the "**DPA**").[15] Such processing needs to meet one of several conditions including whether it was necessary for the exercise of functions conferred on a person by statute.[16]

9. Further, nearly all electronic extraction will involve sensitive processing. This is defined under section 85(8) of the DPA, as processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; data concerning health; data concerning an individual's sex life or sexual orientation.[17] Sensitive processing is subject to a set of even more stringent conditions.[18] As such, failures to comply with both the Act and the Code may also be breaches under the DPA. Under the DPA, there are a range of enforcement options that the Information Commissioner can use against organisations,[19] up to and including fines of 20 million Euros.[20] Moreover,

---

[12] Police, Crime, Sentencing and Courts Act 2022 s37(2).

[13] M. Elliott and R. Thomas, *Public Law* (2nd ed., OUP, 2014) para. 5.1.

[14] *Supra* note 1 Home Office at para. 13.

[15] Data Protection Act 2018 s3(4).

[16] *Ibid*, sch. 10.

[17] *Ibid*, s85(8).

[18] *Ibid*, s86(2)(b), sch. 10.

[19] *Ibid*, Part 6.

[20] *Ibid*, s157(5)(a).

victims of a breach of the DPA can also sue for damages.[21] These consequences should be clearly set out and explained in the Draft Code.

Admissibility in as Evidence in Civil or Criminal Proceedings

10. While the Draft Code does state, at paragraph 13, that failure to follow the code is admissible in evidence in criminal or civil proceedings, and may be taken into account by the courts, it gives no examples of the types of proceedings in which a breach will be relevant, or how it would be taken into account. The Draft Code should give such examples.

Professional Misconduct

11. Paragraph 14 notes that a failure to follow the Draft Code could be considered in professional disciplinary hearings. However, it fails to specify how such failure would be relevant to those hearings. For instance, the Police Code of Ethics sets out standards of professional behaviour expected from officers. The second of these standards is that officers will exercise their powers and authority lawfully.[22] Failing to exercise the power under section 37 under the Act is unlawful. As such, the Draft Code should set this out as an example of how failing to use the powers in the Act lawfully could be relevant in professional disciplinary proceedings.

12. The same standard requires that the police treat members of the public with respect.[23] Further, section 9.2 of the Code of Ethics obliges officers to ask themselves whether an action might result in members of the public losing trust and confidence in the policing profession.[24] It is likely that breaching most of the Draft Code's provisions would result in breaches of the Code on either of these bases. For instance, failure to inform a user how any collateral information obtained will be managed and when the device is likely to be returned could be a breach of both.[25] Such a failure would seem to lack respect for the centrality that digital devices have to users lives and the volume of private information likely to be stored within them, alongside damaging public trust, particularly amongst

[21] Data Protection Act 2018 s169(1).

[22] College of Policing, 'Code of Ethics: A Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales' (2014) 4.

[23] *Ibid.*

[24] *Ibid.* Para. 9.2.

[25] *Supra* note 1 Home Office at para. 88.

victims of sexual violence. The Draft Code should more fully make clear to authorised persons how breaches of the Act and the Draft Code would relate to professional disciplinary hearings, particularly with reference to codes of ethics/conduct.

The need for strict necessity

13. The Draft Code acknowledges that the section 37 and section 41 powers must be exercised in accordance with the European Convention on Human Rights (the "**ECHR**"), Data Protection Act 2018 (the "**DPA**"), and the UK General Data Protection Regulation (the "**UK GDPR**").[26] Nevertheless, the Draft Code could go further in explaining to authorised persons how they are to use these powers in a way that is compatible with the ECHR. Section 37(5)(c) and Section 41(4)(b) requires that the authorised person be satisfied that exercising the power in Section 37 or 41 is necessary and proportionate to achieve the purpose for which the authorised person in exercising that power.[27] The Draft Code makes no mention of the fact that the requisite standard of necessity required in this context is that of "*strict necessity*".

14. The Draft Code does give some assistance in operationalising this test. It states that for the exercise of these powers to be proportionate, the information sought must be needed to achieve the relevant purpose for which the power is exercised and that the purpose cannot be achieved by other less intrusive means. Further, the authorised person is instructed to record their rationale as to why the information extraction is necessary and proportionate.[28]

15. The standard of necessity applicable in the context of the powers under sections 37 and 41 is that of "*strict necessity*". Baroness Williams herself acknowledged that strict necessity is the correct standard during the Act's Committee Stage, despite declining to amend the Bill amended to reflect this:

> *"In every case where authorised persons are extracting sensitive personal information … they must continue to meet the strict necessity threshold in the Data Protection Act. It is therefore not necessary to duplicate that existing legal requirement in the Bill; it is there."*[29]

[26] *Supra* note 1 Home Office at para. 16.

[27] Police, Crime, Sentencing and Courts Act 2022 s37(5)(c), s41(4)(b).

[28] *Supra* note 1 Home Office at para. 48.

[29] HL Deb (27 October 2021) Vol. 815, Col. 883. Available: here.

16. Further, due to the lack of clarity between the difference in scrutiny between necessity and strict necessity it is essential that it is clear to authorised persons are aware that it is the latter test that is operationalised. There is no risk involved in what Baroness Williams' calls "*duplication*"; it will only make the applicable standard clearer.[30] As such, the Draft Code should explain that authorised persons should only exercise the powers under sections 37 and 41 where digital extraction is strictly necessary.

Risk of obtaining other information

The "Reasonable Practicability" Test and the ECHR

17. Despite the Draft Code's assurances that the powers exercisable under sections 37 and 41 must be used in compliance with the ECHR, its approach to proportionality risks acting contrary to the requirements of Article 8 ECHR. Where there is a risk of obtaining information other than that which is necessary for the purposes the power is being used, section 37(7) requires the authorised person to be satisfied that the use of the power is proportionate.[31] In ensuring that the use of the power is proportionate, the authorised person must be satisfied there are no other means of obtaining the information that avoid the risk. If other means exist, it must not be reasonably practicable to use them.[32]

18. This is an exceedingly low bar. For instance, a police officer would be able to download the entirety of the data on a user's device, regardless of the fact that technology exists which would allow for a more targeted search or extraction. Article 8 ECHR permits interfering with the right to privacy only where it is "*necessary in a democratic society*". We are unaware of any interpretation of this standard that permits an intrusion into the right to privacy where other means that avoid an interference exist but it is not reasonably practicable to use them. [33] The Draft Code should set an appropriately high standard to

[30] Big Brother Watch, Amnesty International, Centre for Women's Justice, Defend Digital Me, End Violence Against Women, Fair Trials, JUSTICE, Rape Crisis England & Wales, the Survivors' Trust, Liberty, Privacy International, 'Report Stage Briefing on digital extraction powers in the Police, Crimes, Sentencing and Courts Bill for the House of Lords' (December 2021) 13-14.

[31] Police, Crime, Sentencing and Courts Act 2022 s37(6).

[32] Police, Crime, Sentencing and Courts Act 2022 s37(7).

[33] Big Brother Watch, Amnesty International, Centre for Women's Justice, Defend Digital Me, End Violence Against Women, Fair Trials, JUSTICE, Rape Crisis England & Wales, the Survivors' Trust, Liberty, Privacy International, 'Report Stage Briefing on digital extraction powers in the Police, Crimes, Sentencing and Courts Bill for the House of Lords' (December 2021), p.15.

avoid acting contrary to Article 8 ECHR, encouraging authorised persons to make use of technologies available given the importance of safeguarding users' privacy.

Confusion Between Proportionality and Necessity

19. Notably, the test adopted seems to misunderstand the role of proportionality as opposed to necessity. As explained by Privacy International, necessity refers to whether extraction is *actually* necessary rather than being *"a mere advantage"*. Proportionality, on the other hand, refers to the need to ask whether the infringement on the user's right to privacy is justified by the weight of the purpose that the extraction is seeking to pursue.[34] For instance, extraction of a user's electronic device would be more likely to be justified in seeking to investigate a murder than a theft. It is once more notable that section 37(7) that only sets out the two alternative conditions that must be fulfilled in order for the exercise of the power in section 37 to be proportionate: (a) there are no other means of obtaining the information sought by the authorised person which avoid that risk, or (b) there are such other means, but it is not reasonably practicable to use them. [35]

20. Neither of these conditions invoke a test of proportionality. Both outline situations where it would be *necessary* to obtain the other information to achieve the law enforcement goal. Proportionality involves considering whether that goal can be justified when weighed against the instruction into the relevant user's privacy.

21. The Draft Code provides an opportunity to clarify how authorised persons can use the section 37 powers in a proportionate manner. While the Act sets out two conditions which need to be fulfilled for the authorised person to be satisfied the use of the power is proportionate, it does not state that these are the *only* conditions that need to be fulfilled. The Draft Code does mention at the outset that there is a need for an authorised person to carefully consider whether an extraction pursuant to the powers in section 37 and 41 amounts to an interference with the user's right to privacy under Article 8 ECHR, and whether that interference is justifiable.[36] However, it is never made clear how this broad principle fits within the regime under section 37.

22. This could be incorporated into the Draft Code of Practice by stating that, in addition to meeting one of the two conditions s37(7) sets out, the authorised person must be independently satisfied the use of the power is justified and so proportionate. Therefore,

[34] 'Legality, Necessity, and Proportionality' Privacy International.

[35] Police, Crime, Sentencing and Courts Act 2022 s37(7).

[36] *Supra* note 1 Home Office at para. 18.

the Draft Code should state for the use of the section 37 power to be proportionate it must justifiable when weighing the law enforcement goal involved in using the power against the user's right to privacy. It should be made clear that this test must be met over and above fulfilling one of the tests under s37(7).

Lack of Guidance

23. The Draft Code rightly refers to the case of *Bater-James & Anor. v R* as a source of guidance on when other means than electronic extraction should be used rather than exercising the section 37 power, when applying the test under s37(7).[37] It is correct that the Court of Appeal suggested that taking screenshots or another method of record may be appropriate other than using electronic extraction.[38] Further, paragraph 50 of the Draft Code also suggests simply examining the device if authorised persons need to examine only a limited number of messages.[39]

24. However, beyond these suggestions, the Draft Code gives no further suggestions on when it is not reasonably practicable to avoid using electronic extraction. This is particularly concerning given the lack of precedent for a test based on reasonable practicability. As such, if a test of reasonable practicability is to be used to determine whether an authorised person should proceed with electronic extraction where there is a risk of obtaining unnecessary information, the Draft Code should include a number of detailed examples, alongside accompanying guidance, to ensure best practice.

Assessing whether there is a risk of obtaining confidential information

25. The Draft Code, at paragraphs 62-65, is too vague in its advice to authorised persons as to how they should assess the risk of obtaining confidential information. Section 43 states that confidential information is confidential journalistic material within the meaning of the Investigatory Powers Act 2016 or protected material.[40] Under the Act, protected material includes items subject to legal privilege, person records held by a person through any

[37] *Supra* note 1 Home Office at para. 51.

[38] *Bater-James & Anor. v R.*, [2020] EWCA Crim 790 Para. 80.

[39] *Supra* note 1 Home Office at para. 50.

[40] Police, Crime, Sentencing and Courts Act 2022 s43(1).

occupation or office that is held in confidence, and material held in the same way through an express or implied undertaking to hold it in confidence.[41]

26. The Draft Code simply advises that the authorised person should use their professional judgment in assessing the risk of obtaining confidential information and whether it is appropriate to ask the user. It also acknowledges that when the user is a lawyer or journalist that it can be reasonably assumed that their device contains a high volume of confidential material. By way of guidance, the Draft Code simply advises that it may be appropriate to ask them whether such material is on their device.[42]

27. This underplays the risk involved in disclosing confidential information. Confidential journalistic information under the Investigatory Powers Act 2016 and protected material covers a range of information that could have severe consequences both for the user and who that information relates to if the information leaves the user's control. We consider that the Draft Code should mandate that authorised persons ask a user whether their device contains any confidential information rather than only requiring an authorised person to consider whether it is appropriate to ask the user.

Failure to limit authorised person's possession of the device

28. The Draft Code fails to sufficiently limit how long an authorised person can keep the device that has been subject to electronic extraction within their possession. Paragraph 133 states that in all cases authorised persons should seek to return the device to the user as soon as possible. Further, in the case of a rape victim, the Draft Code provides that this should ideally be within 24 hours.[43] Beyond this, the Draft Code places no limits, or suggestions of best practice, on how long an authorised person may retain the device. Given recurring problems with the police taking excessive amounts of time to return victim's phones, these safeguards are insufficient. A 2019 Freedom of Information request by Big Brother Watch found that average wait time amongst police forces to examine digital devices varied from three weeks to four months.[44]

[41] Police, Crime, Sentencing and Courts Act 2022 s43(2); Police and Criminal Evidence Act 1984 s11(1)(a), s14(2); Police, Crime, Sentencing and Courts Act 2022 s37(10).

[42] *Supra* note 1 Home Office at paras. 63-64.

[43] *Ibid.* para. 133.

[44] Big Brother Watch 'Digital Strip Searches: the police's data investigations of victims' (2019) 18.

29. Victims and other users should not face the prospect of being left without access to their electronic device for potentially months on end and without the certainty of when that device will be returned to them. Users rely on phones and other electronic devices for living both their personal and work lives. Lack of access constitutes a major disruption to being able to live their lives. Many victims, especially in the immediate aftermath of the alleged offence, will need the support of friends and family. Access to a phone or other electronic device may be a lifeline to accessing that support. On top of this, electronic devices will contain a wealth of deeply personal and private data concerning the user. Being left unable to have access to that information for a long, undefined period of time undermines their right to privacy and is likely to be a source of serious distress.

30. As such, the Draft Code should state that the electronic device should ordinarily be in the authorised person's possession for no more than 24 hours, but in any case, no longer than 30 days. If that time lapses without the electronic extraction taking place, a new agreement should be sought. This should all be reflected within the written notice.

Presence of user during search

31. The Draft Code fails to include straightforward measures to ensure a user's right to privacy when undertaking the search. During the Act's report stage, JUSTICE sought to have the Bill amended so that searches of the user's electronic device would take place with the user in-person unless either the user or the authorised person considered this impracticable or inappropriate. This amendment aimed to provide reassurance to users and foster trust in the process of extraction. We noted that when an individual reports a burglary, they would be present during the police's search of their home.[45]

32. The presence of a user during a search would both help ensure accountability for authorised persons when the carry out searches of electronic devices. This is because their oversight provides a witness independent of the authorised person of the conduct of the search. Further, the user's presence will assist in demonstrating that such search has met the tests of strict necessity and proportionality. Often, the user will be the best judge of where relevant information will be held on the device and where unnecessary, and vitally private, information is contained. The Draft Code should state that data extraction should

[45] Big Brother Watch, Amnesty International, Centre for Women's Justice, Defend Digital Me, End Violence Against Women, Fair Trials, JUSTICE, Rape Crisis England & Wales, the Survivors' Trust, Liberty, Privacy International, 'Report Stage Briefing on digital extraction powers in the Police, Crimes, Sentencing and Courts Bill for the House of Lords' (December 2021), p.20.

take place with the user in-person unless either the user or the authorised person considers this to be impracticable or inappropriate.

Voluntary provision, agreement, and undue pressure

33. We are concerned that the Draft Code's provision, at paragraph 83, that where a victim is not capable of providing agreement in writing to electronic extraction, the authorised person may secure that agreement orally, leaves open the wide potential for abuse. The Draft Code provides that if agreement from the user to voluntarily provide their device cannot be provided in writing due to the user's physical impairment or lack of literacy skills, the agreement may be given orally so long as that agreement is then recorded in writing.[46] Further, the Draft Code provides the user cannot have been unduly pressured or coerced by anyone to provide the advice and that the individual must have freely made an informed and conscious choice to provide the device. The Draft Code gives the example of a person being made to feel that the investigation will be discontinued, or other reasonable lines of enquiry will not be followed up if they do not provide their device.[47]

34. Once more, it must be emphasised that the user of the device has voluntarily provided their device is a requirement under the Act.[48] As such, JUSTICE is concerned with the inadequate safeguards the Draft Code sets out to ensure that users with physical impairments or lack literacy skills do truly voluntarily provide their device for electronic extraction. For instance, Crown Prosecution Service ("**CPS**") provides that police officers have a responsibility, when there is a difficulty communicating with a witness, to hold an early special measures discussion with the CPS to agree the form of the statement to be taken and which special measures are appropriate, including whether there is a need for an intermediary.[49] Intermediaries use their skills to ensure that vulnerable persons are able to answer what is being asked of them and that their answers are understood in reply. They can write out a report explaining the strategies that would make communication easier and to assist the vulnerable person in answering in as much detail as possible.[50]

35. We are concerned about the lack of reference to special measures and, in particular, intermediaries, in supporting vulnerable persons, within the Draft Code. Despite the highly

[46] *Supra* note 1 Home Office at para. 38.

[47] *Ibid.* paras. 84-85.

[48] See above para 2.

[49] 'Special Measures' Crown Prosecution Service.

[50] 'Intermediary Role' Intermediaries for Justice.

invasive nature of electronic extraction, the Draft Code offers less safeguards for vulnerable persons when agreeing to provide their device as against when they partake in a police interview. In addition, the rest of the guidance on ensuring the vulnerable person has voluntarily provided their device is too vague. Rather than simply giving examples of situations where the user will not have provided their device freely and voluntarily, the Draft Code should fully make clear the steps needed to ensure the user has made an "*informed choice*".

36. As such, the Draft Code, at a minimum, should spell out the steps needed to ensure that vulnerable individuals have made and informed, and so voluntarily, choice when they provided their device. It should also include guidelines for applying special measures or making use of intermediaries when a user is not capable of providing in writing agreement to the electronic extraction.

Written Notice

37. Paragraph 87 sets out the information that the authorised person must provide to the user within a written notice when they exercise the power under section 37. This specifies that the written notice must contain: the information sought; why the information is sought (and, where relevant, how it supports a reasonable line of enquiry); how the information will be dealt with once it has been extracted (including who will see it); that the person may refuse to provide the device or agree to the extraction of information from it; and that the investigation or enquiry for the purposes of which the information is sought will not be brought to an end merely because of a refusal to provide the device or agree to the extraction of information from.[51]

38. However, paragraph 88 provides that the user need only be orally informed of how any collateral information obtained will be managed; of when the device is likely to be returned; and that they can make a complaint to the controller if they feel the request for information is excessive or that they have been coerced into providing the device and giving agreement.[52] The information in paragraph 88 is of vital importance to the user. The requirement that the this information is contained in a written notice is central to ensuring accountability for the authorised person and in carrying out the extraction and so ensuring that users are properly informed when they make the decision to provide their device.

[51] *Ibid.* para. 87.

[52] *Ibid.* para. 88.

39. It is for this reason that JUSTICE sought to have the Act amended to have this information included the written notice as part of the statutory scheme. Moreover, in JUSTICE's proposed amendments, we sought to have an explanation what less intrusive methods to obtain the information were considered before the request for extraction was made and why no less intrusive means are possible.[53] As such, we consider that the Draft Code should state that written notices should contain the information set out in paragraph 88 as well as an explanation of what less intrusive methods to obtain the information were considered and why no less intrusive means were possible.

Need for a review of a request for electronic extraction independent of the initial decisionmaker

40. The Draft Code provides an insufficient mechanism for review of a request for electronic extraction from a user's device. Users are able to make a complaint under the DPA to the controller if they feel the request for information made of them is excessive or if they feel they have been coerced into giving the device and giving agreement.[54] In these circumstances, the controller must erase the personal data obtained through the processing without undue delay.[55]

41. However, the flaw in this complaints mechanism becomes apparent when the definition of a controller is considered. Section 32(1) states the definition of controller includes the competent authority which determines the means and purposes of the processing of personal data.[56] In context of exercising the Act's section 37 power, this will be someone within the same organisation (most likely a police force) as the authorised person. As such, the mechanism to review a request for electronic extraction of a user's device does not have a review mechanism that is independent of the authorised person as initial decisionmaker.

42. There is a need to stress the importance of having access to an impartial and independent mechanism to review the request for electronic extraction. The necessity of having

[53] Big Brother Watch, Amnesty International, Centre for Women's Justice, Defend Digital Me, End Violence Against Women, Fair Trials, JUSTICE, Rape Crisis England & Wales, the Survivors' Trust, Liberty, Privacy International, 'Report Stage Briefing on digital extraction powers in the Police, Crimes, Sentencing and Courts Bill for the House of Lords' (December 2021), p.11.

[54] *Supr at* note 1 Home Office at para. 88.

[55] Data Protection Act 2018 s47(1)(a).

[56] *Ibid*. s32(1)(a).

independent and impartial decision-makers within courts and tribunals is deep-seated within the UK constitution, being reflected in common law through the maxim *"no one may be a judge in [their] own cause"*.[57]

43. It is not sufficient for an appeal mechanism only to act in an independent and impartial manner. It must also be seen to do so. The mechanism for appealing a request for electronic extraction of a user's device must therefore operate separately from the initial decision-maker. The Draft Code should set out such a process for reviewing whether the request for information made of the user was excessive or whether the user has been coerced into giving the device and giving agreement.

JUSTICE

19 July 2022

[57] *R v Bow Street Metropolitan Stipendiary Magistrate Ex p. Pinochet Ugarte (No. 2)* [2001] 1 A.C. 119 at 141.