# Complainant Phone Data Extraction by Police in England and Wales: Outstanding Issues and Practical Guidance

July 2022

***This research report is produced for informational purposes only. It does not constitute any form of legal advice and it should not be relied on, or treated as a substitute for, legal advice tailored to specific circumstances.***

# Contributors

### Faculty Advisor

Dr Jonathan Rogers
*University Assistant Professor in Criminal Justice, University of Cambridge*
*Co-Deputy Director of the Cambridge Centre for Criminal Justice*
*Co-Director of the Criminal Law Reform Now Network*
*Fellow of Fitzwilliam College*

### Cambridge Pro Bono Project – Executive Directors

Alexandra Allen-Franks
*PhD Candidate, Law, University of Cambridge*

### Project Managers

Tim Cochrane
*PhD Candidate, Law, University of Cambridge*

Nicholas Goldrosen
*PhD Candidate, Criminology, University of Cambridge*

### Project Researchers

Delene Adams
*MPhil Criminology Candidate, University of Cambridge*

Harpreet Gupta
*LLM Candidate, University of Cambridge*

Georgia Speechly
*LLM Candidate, University of Cambridge*

Isabelle St-Hilaire
*LLM Candidate, University of Cambridge*

Mayeda Tayyab
*MPhil Criminology Candidate, University of Cambridge*

# Acronyms

| | |
|---|---|
| APP | Authorised Professional Practice |
| CDPA | Copyright, Designs, and Patents Act 1988 |
| CPIA | Criminal Procedure and Investigations Act 1996 |
| DPA 2018 | Data Protection Act 2018 |
| ECHR | European Convention on Human Rights |
| EDPB | European Data Protection Board |
| EU | European Union |
| GDPR | EU General Data Protection Regulation |
| HRA | Human Rights Act 1998 |
| LED | EU Law Enforcement Directive |
| NPCC | National Police Chiefs' Council |
| PACE | Police and Criminal Evidence Act 1984 |
| PCSC Act | Police, Crime, Sentencing, and Courts Act 2022 |
| UK GDPR | UK General Data Protection Regulation |

# Table of Contents

**I. INTRODUCTION** ..... **6**

**II. PRE-EXISTING LEGAL FRAMEWORK REGULATING POLICE SEARCHES OF COMPLAINANT MOBILE PHONES** ..... **7**

**A. OVERVIEW** ..... **7**
**B. CONSENT SEARCHES** ..... **9**
PART 3 OF THE DPA 2018 ..... 9
COMMON LAW ..... 11
UK GENERAL DATA PROTECTION REGULATION ..... 12
INVESTIGATORY POWERS ACT 2016 ..... 13
**C. NECESSITY/PROPORTIONALITY ANALYSIS** ..... **14**
**D. HUMAN RIGHTS CONSIDERATIONS** ..... **17**
EUROPEAN CONVENTION ON HUMAN RIGHTS ..... 17
RELEVANT FOREIGN JURISPRUDENCE ..... 18

**III. IMPACT OF THE POLICE, CRIME, SENTENCING AND COURTS ACT 2022** ..... **20**

**A. BACKGROUND** ..... **20**
**B. OVERVIEW** ..... **21**
**C. CONSENT SEARCHES** ..... **22**
**D. NECESSITY/PROPORTIONALITY ANALYSIS** ..... **24**

**II. OUTSTANDING PROBLEMS** ..... **26**

**A. CONSENT SEARCHES** ..... **26**
TO WHAT EXTENT CAN COMPLAINANTS MEANINGFULLY CONSENT? ..... 26
IS PART 3 OF THE DPA 2018 CONSISTENT WITH THE LED? ..... 31
**B. NECESSITY/PROPORTIONALITY ANALYSIS** ..... **36**
WHAT GOES ON THE SCALES IN THE PROPORTIONALITY BALANCING TEST? ..... 36
WHAT DOES "REASONABLY PRACTICABLE" MEAN? ..... 38
WHAT DOES PROPORTIONALITY MEAN IN THE CONTEXT OF SEEKING EXCULPATORY INFORMATION? ..... 39

**IV. RECOMMENDATIONS AND HYPOTHETICAL SCENARIOS** ..... **40**

**A. POLICE GUIDANCE** ..... **41**
**B. HYPOTHETICAL SCENARIOS** ..... **42**
COMPLAINANT REPORTS SEXUAL ASSAULT BY A STRANGER ..... 42
COMPLAINANT REPORTS HISTORIC ALLEGATIONS ..... 43

COMPLAINANT CONSENTS TO POLICE PROCESSING THEIR DATA, BUT REFUSES TO HAND OVER HER DEVICE, AS IT WILL BE FOR SUCH A LONG PERIOD ..... 43
COMPLAINANT CONSENTS TO HANDING OVER THEIR DEVICE AND FOR DATA TO BE EXTRACTED, BUT THEY ARE EMOTIONAL AND DISTRESSED AFTER A TRAUMATIC INCIDENT OR AFTER RECOUNTING PAINFUL MEMORIES ..... 44
COMPLAINANT CONSENTS TO THEIR DEVICE BEING HANDED OVER, AND INFORMATION BEING EXTRACTED FROM IT. HOWEVER, AFTER A FEW DAYS, THEY RETURN AND WITHDRAW THEIR CONSENT, AND DEMAND THE RETURN OF THEIR DEVICE. ..... 44

**V. CONCLUSION ..... 45**

## I. INTRODUCTION

This report addresses how and when police (and other law enforcement) in England and Wales should access personal data from electronic devices of complainants, particularly when investigating sexual offences.

It is now undisputed that electronic data offers huge scope for criminal investigations. As courts have recognised globally, electronic devices have revolutionised the amount of information easily accessible to investigators in a criminal matter. 'A single mobile device now frequently contains an array of information that 40 years ago would have been found in multiple different locations,' noted the Court of Appeal of England and Wales recently.[1] Most people now carry one, functionally keeping their letters, diary, notepad, and photo albums in their pockets; as the US Supreme Court pithily noted, '[smartphones] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.'[2] NGOs, lawyers, and politicians have, however, recently brought attention to one particularly concerning way police leverage this data treasure-trove: by downloading and examining the contents of devices from complainants, particularly when investigating serious sexual offences. This phenomenon has been the subject of recent publications by the UK government and others.[3]

This report aims to build on these publications, by focusing on two unsettled issues. First, from the perspective of investigators, this data provides a relatively straightforward way of assessing potential weaknesses or inconsistencies in the complainant's account. Yet, on the other hand, the routine or regular inspection of complainant's devices is reportedly unnerving and distressing for many complainants—disproportionately women—treating them in many respects more as suspects than complainants, casting suspicion on their accounts. Secondly, this data inspection has been perceived by complainants to be overbroad and intrusive, giving police access not only to potentially relevant information but also to the entirety of a complainant's private life. Moreover, since these devices are commonly taken and processed on the basis of a complainant's consent, many reported being told, explicitly or implicitly, that their case would not be investigated if they did not hand over their phone.[4]

---

[1] *Bater-James v R* [2020] EWCA Crim 790 [73].

[2] *Riley v California* 573 US 373, 382 (2014).

[3] See for example Big Brother Watch, 'Digital Strip Searches: The Police's Data Investigation of Victims' (July 2019); Information Commissioner's Office [**ICO**], *Information Commissioner's Opinion: Who's Under Investigation? The processing of victims' personal data in rape and serious sexual offence investigations* (31 May 2022) [**ICO, *Who's Under Investigation?***]; and UK Government, *The end-to-end rape review report on findings and actions* CP 437 (June 2021) 35, 37–38, and 40–42.

[4] See Big Brother Watch (n 3) 47–50.

These two issues—the perceived overbroad digital searches and the pressure complainants feel to consent to them—frame this report. We first consider the issue of consent: to what extent can complainants genuinely freely allow police to search their devices in these cases, and to what extent does consent provide a sufficient basis, or even relevant criterion, under data protection laws for such data processing? We then turn to the necessity and proportionality of these searches: when should police undertake inquiries of complainants' devices, and when should they not? When they do, what bounds should be placed on that inquiry? In examining each of these issues—consent and necessity/proportionality—we consider both the pre-existing legal framework in England and Wales and the new regulatory regime now contemplated by the Police, Crime, Sentencing, and Courts Act 2022 (**PCSC Act**). Our analysis of the PCSC Act is necessarily speculative, as this legislation was enacted shortly before the research underlying this report was complete.

This report has four substantive parts. Part I addresses the legal position in relation to consent and necessity/proportionality immediately prior to the enactment of the PCSC Act. Part II then briefly considers how the PCSC Act is likely to impact these two issues. The remaining parts of our report are forward-looking. Part III outlines outstanding problems raised by our consideration of both the issues of consent and necessity/proportionality, flagging ambiguities in the law of which police should be aware and areas for further research. Part IV then attempts to provide practical advice for policy-making in light of these uncertainties. We suggest policy elements, illustrated by hypothetical scenarios, to guide police discretion in line with the law.

## II. PRE-EXISTING LEGAL FRAMEWORK REGULATING POLICE SEARCHES OF COMPLAINANT MOBILE PHONES

This section of the report addresses the pre-existing legal framework, prior to the enactment of the PCSC Act, regulating police searches of complainant mobile phones. As set out, it focuses on two key issues police must navigate when considering and carrying out such searches: the role of complainant consent and the necessity/proportionality test. These two issues engage various areas of the law: common law; statutory powers regulating police investigations; data protection; and human rights. This section therefore begins with a high-level overview of these relevant legal areas. It then outlines specific law relevant to each issue. It then concludes by considering overarching human rights considerations.

### A. Overview

The powers of the police in England and Wales evolved historically from the common law. While most police powers are now codified by statute, the common law continues to provide

police with a non-coercive power to obtain and store information for law enforcement purposes.[5] The primary statute now regulating police powers is the Police and Criminal Evidence Act 1984 (**PACE**). A host of other statutes provide additional powers and duties on police. These include the Criminal Procedure and Investigations Act 1996 (**CPIA**), which relevantly recognises the duty on police to obtain and retain relevant evidence and pursue reasonable lines of enquiry during criminal investigations.[6] Police powers are also supplemented by guidance: these include formal guidance issued pursuant to PACE, CPIA and other statutes,[7] as well as free-standing further guidance by the Attorney-General and others.[8]

Police are also subject to UK data protection law. In addition to other data protection laws outlined below, key for present purposes is Part 3 of the Data Protection Act 2018 (**DPA 2018**), incorporating into UK law the European Union (**EU**) Law Enforcement Directive (**LED**).[9] The LED regulates "competent authorities" (such as the police), in place of other data protection laws, where these authorities process data "for law enforcement purposes". In 2021 the College of Policing published additional guidance within its Authorised Professional Practice (**APP**) regarding extraction of material from digital devices, discussing the application of Part 3 of the DPA 2018.[10]

Finally, police—like all public authorities—should also normally comply with human rights pursuant to s 6 of the Human Rights Act 1998 (**HRA**). The HRA incorporates the European Convention on Human Rights (**ECHR**) into domestic UK law, including the law of England and Wales. As a core public authority, the HRA requires that police act in accordance with the

[5] *R (Catt) v Association of Chief Police Officers* [2015] UKSC 9 [7] (Lord Sumption). See *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058 [38].

[6] See Criminal Procedure and Investigations Act 1996 [**CPIA**], s 23(1)(a); and *R v E* [2018] EWCA Crim 2426 [17].

[7] See for example Home Office, 'PACE Code B, Revised Code of Practice for Searches of Premises by Police Officers and the Seizure of Property Found by Police Officers on Persons or Premises' (2013); and Ministry of Justice, 'Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice: Revised in accordance with section 25(4) of the Criminal Procedure and Investigations Act 1996' (March 2015) [**CPIA Code**].

[8] See for example Attorney-General's Office, 'Attorney-General's Guidelines on Disclosure: For investigators, prosecutors and defence practitioners' (2020) [**AG Disclosure Guidelines**].

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119 [**LED**].

[10] College of Policing, Authorised Professional Practice [**APP**], 'Extraction of Material from Digital Devices' (2021) [**APP*, Extraction of Material***]. See also *R (J) v West Mercia Police* [2022] EWHC 26 (Admin) [86] ("The APP Guidance is guidance, not legislation, but there would need to be a good reason not to follow it").

ECHR at all times, except where required to do otherwise by primary legislation, including when investigating and prosecuting offences.[11] The primary rights most likely to be engaged in such circumstances are the right to a fair trial protected by Article 6 ECHR and the right to respect for private and family life protected by Article 8 ECHR.

The above is a high-level overview of various legal powers relevant to this area. How these various legal mechanisms impact the areas analysed in this report—police's ability to request consent searches and the application of the necessity/proportionality test—are what this report turns to next.

## B. Consent Searches

*Part 3 of the DPA 2018*

Part 3 of the DPA 2018 is the key mechanism regulating consent searches here. As noted, Part 3 transposes the LED into UK law and regulates data processing by competent authorities for law enforcement purposes. It sets out a number of principles of data processing. The first principle—most relevant to the issue of consent—requires that processing be "lawful and fair".[12] Pursuant to s 35(2), processing must be "based on law" and meet either of the two criteria: consent ("the data subject has given consent to the processing for that purpose") or necessity ("the processing is necessary for the performance of a task carried out for that purpose by a competent authority").

'Consent' is not defined in Part 3 of the DPA 2018, but is defined for purposes of Part 4 (regulating data processing for intelligence purposes) as "a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data".[13] Although this definition does not directly apply to Part 3 processing, it largely reflects the definition of consent in the UK General Data Protection Regulation (**UK GDPR**) (discussed below) and incorporates similar aspects: consent should be voluntary, specific, informed, unambiguous and indicated by the individual's clear affirmative action. There is no indication that any other definition of consent is contemplated by Part 3 of the DPA 2018; in fact, the UK

[11] See Human Rights Act 1998, s 6(2).
[12] Data Protection Act 2018 [**DPA 2018**], s 35(1).
[13] ibid s 84.

government has recently announced plans to amend Part 3 to introduce a consent definition aligning with the rest of UK data protection law.[14]

Additional requirements apply to 'sensitive processing',[15] which is defined in s 35(8) as follows:

> (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.

Where sensitive processing is carried out on the basis of the data subject's consent, consent alone is insufficient. In addition to such consent, Part 3 of the DPA requires that, "at the time when the processing is carried out, the controller has an appropriate policy document in place".[16] This document must, pursuant to s 42(4):

> (a) explain[] the controller's procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and
> (b) explain[] the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

Where sensitive processing is not based on the data subject's consent, the processing must: (i) not only be necessary but *strictly* necessary; (ii) meet at least one of the conditions set out in sch 8 (Conditions for sensitive processing under Part 3); and (iii) the controller must, again, have an appropriate policy document in place at the time the processing is carried out. Schedule 8 lists various conditions, including: where processing is necessary "for the exercise of a function conferred on a person by an enactment or rule of law" and "for reasons of

[14] Data Protection and Digital Information HC Bill (2022–23) [143] [**DPDI Bill**], cl 4. See Explanatory Notes to the DPDI Bill, paras 19 and 112–117. See also Department for Digital, Culture, Media and Sport,
Impact Assessment: Data Protection and Digital Information Bill' (6 July 2022) [265] (acknowledging the "risk that [consent] may be interpreted incorrectly in the absence of a clear definition").

[15] DPA 2018, ss 35(3)–35(5).

[16] ibid s 35(4).

substantial public interest";[17] "for the administration of justice";[18] "to protect the vital interests of the data subject or of another individual".[19] In addition to various other (largely administrative) conditions,[20] sch 8 also allows processing that "relates to personal data which is manifestly made public by the data subject".[21]

Section 44 sets out information that must be provided to data subjects (for all types of data processing). It is acceptable to simply make certain of this information public, but more specific information—such as the purposes of processing the personal data[22]—would likely need to be provided directly to the data subjects themselves. Information to be provided to all data subjects includes: the identity and contact details of the controller, the contact details of the data protection official,[23] the purposes for which data will be processed, and the existence of data subjects to request access to personal data, rectification of personal data, and erasure of personal data or restriction of its processing.[24] A second category of information to be provided includes information about the legal basis for processing, the period for which data will be stored, categories of recipients of the personal data, and any other information required for data subjects to exercise their rights. However, this second category need not be provided to data subjects (in whole or in part) if such provision would: obstruct an investigation; prejudice prevention, detection, investigation or prosecution of criminal offences; or interfere with protecting public or national security or the rights and freedoms of others.[25] If this second category of information is not provided, information about this restriction must be provided to the data subject without delay.[26]

*Common law*

At least to the extent such processing is reliant on taking possession of the complainant's mobile device, common law consent (i.e. voluntary informed agreement) provides the historical requirement for the taking of such physical possession and may continue to play a

[17] ibid sch 18, para 1.
[18] ibid sch 18, para 2.
[19] ibid sch 18, para 3.
[20] See ibid sch 18, paras 4 and 6–9.
[21] ibid sch 8, para 5.
[22] ibid s 44(1)(c).
[23] See also ibid ss 69-71.
[24] ibid ss 45-47.
[25] ibid s 44(4).
[26] ibid s 44(5).

role.[27] Common law consent has several requirements.[28] First, a basis in law must be established to process data. This may be the requirement to pursue all reasonable lines of enquiry.[29] Next, either informed consent must be given, or extraction must be necessary for a law enforcement process.

*UK General Data Protection Regulation*

The UK GDPR[30]—replacing the EU General Data Protection Regulation (**GDPR**) and supplemented by Part 2 of the DPA 2018—applies by default to other instances of data processing, with some exceptions (notably, processing by intelligence services, which is instead regulated by Part 4 of the DPA 2018).

Consent may also be the legal basis enabling police to intercept (in real-time) communications from telecommunication operators in certain circumstances, set out in the IPA. While this may have some utility for police during criminal investigations into serious sexual assault as outlined below, this report focuses on Part 3 of the DPA 2018, as it assumes that police searches of complainant devices will be for law enforcement purposes—in which case Part 3 will govern. Details of alternative procedures under the UK GDPR and IPA are nonetheless also set out in this report for context.

Consent of a data subject is defined in Article 4(11) of the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Article 6(1) establishes various lawful grounds for processing data, including consent from the data subject "to the processing of his or her personal data for one or more specific purposes".[31]

Article 7 sets out the conditions for consent as follows:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which

[27] See ICO, 'Mobile phone data extraction by police forces in England and Wales' (June 2020) 33.

[28] *R (H) v Commissioners of Inland Revenue* [2002] EWHC 2164 (Admin) [55]. See generally *Morris v Murray* [1991] 2 QB 6 (CA).

[29] See for example *R v Altun* [2021] EWCA Crim 1844 [29]–[31].

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) [**UK GDPR**].

[31] UK GDPR, art 6(1)(a).

is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Recital 42 requires that pre-formulated consent must be intelligible and easily accessible, and a data subject must have a genuine choice, and be able to refuse or withdraw consent without detriment. Recital 43 provides further that if there is a clear imbalance between the data subject and controller, particularly where the controller is a public authority, consent should not provide a valid ground.

Article 9(1) prohibits processing of personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Special Category Data). Section 9(2)(a) provides that this prohibition does not apply if "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes".

Recital 51 notes that photographs of people should not systematically be considered processing of special categories of personal data; they are considered biometric data "only when processed through a specific technical means allowing the unique identification or authentication of a natural person". This may be helpful in interpreting Part 3 of the DPA 2018 and its sensitive processing requirements.

*Investigatory Powers Act 2016*

The IPA sets out the requirements for intercepting live or stored communications from telecommunications or postal operators.[32] Interception of such communications outside the

[32] See Investigatory Powers Act 2016 [**IPA**], s 4.

IPA's requirements is a criminal offence.[33] A warrant is ordinarily required to conduct such interceptions, subject to certain exceptions.[34] Notably, s 44 of the IPA provides that consent will be sufficient for interception either if both the sender and recipient have consented to interception, or one party has consented and a concurrent directed surveillance authority is in place.[35] This means that consent of only one party to a communication is insufficient to lawfully ground an interception, thus providing some protection to the other party (or parties) to that communication.

Section 56 of the IPA provides, *inter alia*, that no evidence may be adduced in legal proceedings if it discloses any content of an intercepted communication or any secondary data relating to an intercepted communication where one could infer that the evidence was obtained by interception. In essence, this means that police may exercise powers under the IPA in order to advance an investigation, but the immediate fruits of this exercise—i.e. the intercepted communications and the data associated with them—may not be adduced as evidence in legal proceedings. This is intended to protect the confidentiality of investigatory techniques.[36] However, this prohibition does not apply when communications are intercepted through consent: s 44 interceptions are listed in sch 3 of the IPA as exceptions to the general admissibility rule in s 56. As such, if communications are intercepted in real-time with consent of one or both parties, and otherwise in accordance with s 44, they may be used as evidence.

**C. Necessity/Proportionality Analysis**

Beyond consent, the extraction of data from a complainant's device must be necessary and reasonable in the context of the police's investigation. This criterion of reasonableness dictates a minimum standard of diligence that investigators must meet and also limits investigators from engaging in needless data extraction. As regards the minimum standard, investigators are bound by the CPIA to pursue all "reasonable lines of inquiry."[37] They must pursue both evidence that tends towards the suspect's guilt as well as that which might be exculpatory.[38] Hence, if information on a complainant's device might pertain to a reasonable line of inquiry, investigators must seek that information.

[33] ibid.

[34] ibid s 6.

[35] See Regulation of Investigatory Powers Act 2000, pt 2.

[36] See Ian Walden, *Computer Crimes and Digital Investigations* (2nd edn, OUP 2016) [6.70]. For further analysis, see [6.71]–[6.81].

[37] CPIA s 23.

[38] CPIA Code (n 7) [3.5].

At the same time, the necessity of seeking such information is also cabined by reasonableness. While every case is fact- and context-dependent, examining a digital device is not necessary when there are no reasonable grounds to believe that the digital device may reveal material relevant to the inquiry or the likely issues at trial.[39] As the Court of Appeal of England and Wales has emphasised, investigators should not adopt a default stance that complainants' devices ought to be seized or inspected in every case absent a particularised need to do so.[40] A reasonable line of inquiry, moreover, is more than a simple hunch or "mere conjecture or speculation".[41] Police and prosecutors are not obliged to sift through all possible evidence to find potential exculpatory material; such inquiries are limited to what is reasonable.[42]

There will be some cases in which electronic evidence extraction is, from the outset, likely to be unreasonable. For example, investigations into alleged serious sexual offences involving an assailant previously unknown to the victim, or into historical allegations, may well typically be unlikely to require searching and extracting a complainant's electronic communications.[43] This criterion of reasonableness will also dictate how extensively investigators might look for electronic communications evidence, i.e. even where a search of data from a complainant device may be reasonable to some extent, the extent of that search must itself be reasonable. CPS guidance, for example, provides that, in cases where parties are known to each other but only briefly, a review of just their communications with each other might be warranted; conversely, in a case where either the complainant or suspect indicates that their communications (including with third parties) contain relevant evidence, a more thorough extraction and search might be needed.[44] Similarly, in investigations of alleged protracted coercive or abusive behaviour, an extensive review of communications between suspect and complainant would be reasonable, not least because the timeframe and volume of relevant communications will be greater.[45] In each scenario, as the above makes clear, reasonableness is a fact-specific criterion.

---

[39] *Bater-James* (n 1) [68].

[40] *R v E* (n 6) [24]; and *Bater-James* (n 1) [77].

[41] *Bater-James* (n 1) [77].

[42] ibid [71].

[43] Crown Prosecution Service [**CPS**], 'Disclosure – A guide to "reasonable lines of enquiry" and communications evidence', *Legal Guidance* (5 July 2018) [13], https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence **[CPS, *Disclosure*]**.

[44] Ibid [14]–[16].

[45] Attorney General's Office, AG Disclosure Guidelines (n 8) Annex A, [13].

Finally, law and guidance prior to the enactment of the PCSC Act recognised that, not only must data extraction from complainants' devices be reasonable, it must also be proportionate in its scope and disruption. Investigators should seize and examine data only insofar as reasonableness dictates, given the facts as understood at that point in the investigation.[46] To do so, they might employ techniques such as: taking photographs of communications as they appear on a complainant's device (as opposed to extracting data from that device using software); obtaining evidence from the suspect's device; or searching only specified categories or types of data.[47] This may be accomplished by limiting a search to a review of particular applications (e.g. Facebook Messenger), certain timeframes and/or through the use of keywords. Speaking generally, when it comes to such investigations—including any disclosure to defendants—"the law is prescriptive of the result, not the method."[48] Investigators are not required to employ a specific strategy, but rather must comply with the overarching imperative to pursue all reasonable lines of inquiry in a proportionate manner.

Such data extraction theoretically engages copyright law. For example, where police take a photo of a communication as it appears on a device, the author of that communication will (usually) be the holder of any copyright.[49] Taking a photograph of a copyright work would normally be an infringing act under the Copyright, Designs, and Patents Act 1988 (**CDPA**),[50] unless the copyright holder licences the act.[51] Such licensing could occur informally, essentially requiring consent—albeit it therefore gives rise to the same issues regarding consent as are addressed elsewhere in this report. In any event, s 50 of the CDPA provides that copyright is not infringed where an otherwise infringing act is authorised by Parliament. To the extent data extraction occurs pursuant to PACE or now—as addressed below—the PCSC Act, s 50 will likely be satisfied.[52]

[46] See generally CPS, 'Disclosure Manual: Chapter 30 - Digital Material', *Legal Guidance* (updated 14 July 2022), https://www.cps.gov.uk/legal-guidance/disclosure-manual-chapter-30-digital-material **[CPS Disclosure Manual**].

[47] ibid; and *Bater-James* (n 3) [78]–[79].

[48] *R v Richards* [2015] EWCA Crim 1941 [48].

[49] Copyright, Designs and Patents Act 1988, s 9.

[50] See ibid ch 2.

[51] ibid ss 16, 17(2).

[52] See also ibid s 45 (stating that copyright is not infringed by anything done for the purposes of judicial proceedings, which would presumably cover some police data extraction).

## D. Human Rights Considerations

*European Convention on Human Rights*

As noted, Article 6 of the ECHR protects the right to a fair trial. Through various specific rights, it seeks to ensure an adversarial process, where both parties have equal access to evidence, witnesses, and information. As a result, generally, information and evidence relied on by the state, or which may assist the defence's case, should be disclosed to the accused.[53] This may include information extracted from a complainant, witness, suspect or accused's mobile device.[54] However, this right must be balanced against the right to private life, which may, depending on the circumstances, be used to limit Article 6.[55]

Article 8 of ECHR, which sets out the right to respect for private and family life, provides:

> 1. Everyone has the right to respect for their private and family life, their home and their correspondence; and
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

For an interference with Article 8(1) to be justified under Article 8(2), it must occur in accordance with sufficiently clear domestic law, pursue a legitimate aim, and be *necessary* in a democratic society for certain purposes (including prevention of disorders and crime, or public safety). The latter requirement is worth reiterating: even where, e.g., consent is provided, processing of personal data may only be carried out if it is *necessary* for a specific purpose. With this in mind, consent as a ground for lawful processing in Part 3 of the DPA 2018 is not necessarily independent of the requirement of strict necessity, since necessity is required by Article 8(2) of the ECHR/HRA and, by extension, s 6(1) of the HRA.

Any interference (including, in this context, the extraction of data from a complainant's device) must also be proportionate to the purpose served. For an interference with Article 8 rights to be considered justified before a UK court it must meet the test in *Bank Mellat v. Her Majesty's Treasury*:[56]

---

[53] See *Kennedy v United Kingdom* App no 26839/05 (European Court of Human Rights [**ECtHR**], 18 May 2010) [184].
[54] See for example *R v E* (n 6) [28]–[42].
[55] See for example *In Re A (A Child)* [2012] UKSC 60 [25].
[56] [2013] UKSC 39 [78].

> [I]t is necessary to determine (1) whether the objective of the measure is sufficiently important to justify the limitation of a protected right, (2) whether the measure is rationally connected to the objective, (3) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and (4) whether, balancing the severity of the measure's effects on the rights of the persons to whom to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter.

Under the ECHR (and equivalent foreign rights regimes, as discussed below), where personal data is obtained by state authorities without the knowledge of the data subject, the right to private life requires that certain minimum safeguards be in place to avoid abuses, including misuse of power and unnecessary intrusions. The types of safeguards will differ depending on the circumstances, but relevant considerations include: the nature, scope, and duration of the possible (interfering) measures; the grounds required for ordering them; the authorities competent to permit, carry out and supervise them; and the kind of remedy provided by the national law.[57]

Although the European Court of Human Rights (**ECtHR**) caselaw generally deals with secret intelligence, its reasoning should apply equally to other means of accessing private information about a person, without the knowledge or consent of that person, for the sake of crime prevention, investigation, and prosecution. In particular, third parties whose communications and information are extracted from the device of a person who has consented to that extraction are arguably in the same position as individuals whose communications were secretly intercepted by the state. As such, third parties have a right under Article 8 ECHR to safeguards that minimise any intrusion into their privacy rights.

*Relevant foreign jurisprudence*

Foreign jurisprudence is commonly applied by the ECtHR and UK courts to interpret the scope of ECHR rights. This section briefly considers the law of two comparable jurisdictions, South Africa and Canada. As set out below, the equivalent rights regimes in those jurisdictions recognise similar rights and appear to impose similar restrictions on police search and seizure of data in analogous scenarios.

The South African Constitutional Court has confirmed the necessity of minimum safeguards to protect privacy rights in the context of real-time interception of communications and (more

[57] *Klass v Germany* A/28 (ECtHR, 6 September 1978) [50].

broadly) the search and seizure of personal information and documentation.[58] In particular, the authorisation and oversight of an independent third party is critical under South African law in ensuring that an appropriate balance is struck between the obligation to investigate and prevent crime and the protection of individual privacy rights.[59] This is not dissimilar from the position taken in *Gaskin v United Kingdom*, where the ECtHR held that, if access to records relating to an individual's private life ('Person A') were refused by another person ('Person B') who contributed to those records, the principle of proportionality required that an alternative option must be available, whereby an independent authority would finally decide whether access should be granted.[60] As such, the mere fact that information regarding Person A is included in the record, and that Person A consents to its disclosure is insufficient; either Person B must consent, or an independent authority must review the matter and make a final determination. While that scenario concerns accessing one's own information (to which another has also contributed), its potential relevance to searches of complainant devices is clear: communications on a complainant devices may contain personal data not only of the complainant—and alleged assaulter—but a host of other third parties. This South African (and ECtHR) guidance emphasises that such third parties should be taken into account in considering the reasonableness of any particular search.

In the Canadian context, s 8 of the *Canadian Charter of Rights and Freedoms* provides that "[e]veryone has the right to be secure against unreasonable search or seizure." As such, it protects individuals from certain invasions of privacy at the hands of government. In relation to suspects, the Supreme Court of Canada has explained that the "common law power to search incident to lawful arrest" allows police to search cell phones found on a suspect who has just been arrested; however, safeguards are imposed when the contents of cell phones are searched in order to balance "the important law enforcement objectives" against "the very significant privacy interests at stake in cell phone searches".[61] Outside that arrest context, prior judicial authorisation is required to intercept and capture "private communications".[62] Justices of the Supreme Court of Canada have repeatedly acknowledged the deep invasions of privacy that can result from searches of mobile phones, in both majority opinions and

[58] *Minister for Safety and Security v Van der Merwe & Ors* [2011] ZACC 19; and *AmaBhungane Centre for Investigative Journalism Anor v Minister of Justice & Ors* [2021] ZACC 3.

[59] *AmaBhungane* (n 58) [32] and [82].

[60] *Gaskin v United Kingdom* App no 10454/83 (ECtHR, 7 July 1989) [49].

[61] *R v Fearon* 2014 SCC 77 [74]. The conditions are the following: (1) "the arrest must be lawful"; (2) "the search must be truly incidental to the arrest"; (3) "the nature and extent of the search must be tailored to its purpose", meaning "only recently sent or drafted emails, texts, photos and the call log will, generally, be available, although other searches may, in some circumstances be justified"; and (4) "the police must take detailed notes of what they have examined on the device and how they examined it".

[62] Canadian Criminal Code, ss 183, 184.2; and *R v Mills* 2019 SCC 22.

dissents/concurrences.[63] Similar authorisation procedures, involving independent oversight, typically apply in England and Wales when police seek to use coercive powers to obtain private data. For example, PACE requires that search warrants or production orders be obtained to gather such data.[64] Even more onerous obligations typically apply to intercept personal data in real-time from telecommunication or similar agencies.[65] The same restrictions do not, however, apply to searches of stored data undertaken by consent, as noted above, despite the impact of such searches on Art 8 ECHR and similar rights potentially being identical. As explored below—and as underscored by this comparative analysis—the impact of searches of complainant devices on rights generally mandates a strict approach to necessity and proportionality analyses generally and may raise particular issues for the continued viability of consent searches in particular.

## III. IMPACT OF THE POLICE, CRIME, SENTENCING AND COURTS ACT 2022

This section turns to the PCSC Act. It first provides background on the aspects of this legislation that relate to police data extraction of complainant (and other) devices. It then considers how the PCSC Act will further regulate the two issues focussed on in this report: consent searches and the necessity/proportionality analysis.

### A. Background

Notwithstanding the legal and procedural guardrails outlined in the previous section, NGO and media reports have highlighted recurrent issues around extracting data from complainants' devices.[66] Numerous complainants, overwhelmingly women, reported that police made handing-over their devices a condition of investigating their reports.[67] At least until recently, the vast majority of police forces in England and Wales apparently regularly engaged in such data extraction, citing pressure from the CPS to do so in every case.[68] In many investigations, complainants were given a notice and consent form drafted by the National Police Chiefs' Council (**NPCC**) which explained that not providing their devices would likely result in a

[63] See for example *Fearon* (n 61) [58] ("[T]he search of a cell phone has the potential to be a much more significant invasion of privacy than the typical search incident to arrest."). See also [127] (LeBel, Abella, and Karakstansis JJ dissenting on other grounds) (endorsing similar analysis); and *R v Vu* 2013 SCC 60 [40]–[45] (distinguishing cellphones from other "receptacles"). See generally *Mills* (n 62) [93] (Martin J concurring) (quoting *R v Jones* 2017 SCC 60 [45]; and citing *TELUS* 2013 SCC 16 [32]).

[64] Police and Criminal Evidence Act 1984, ss 8–15 and sch 1.

[65] See IPA, s 6.

[66] See n 3 above.

[67] Big Brother Watch (n 3) 47–50.

[68] Ibid 8.

discontinued investigation; the use of this form was dropped in the face of litigation in 2020.[69] In the wake of these issues, the legal and procedural framework for how and when police could extract data from complainants' devices became quite muddled.

The PCSC Act was intended, amongst other things, to provide legal clarity for this process of extraction. At a House of Commons' Committee hearing on the draft legislation, NPCC Chair Martin Hewitt testified that "we need the legal framework to allow us to do [extraction] properly and we then also need the resourcing and the capabilities to do it within the right time limits."[70] On its face, the PCSC Act aims to bring more clarity; as Baroness Williams of Trafford, the PCSC Act's House of Lords sponsor, stated: "[o]ur focus is on protecting privacy and supporting victims of crime and others who voluntarily provide information to the police."[71] While it is beyond the scope of this report to comprehensively summarise the background to this legislation—or to take an overall normative view on its reforms—the Parliamentary record clearly shows that the PCSC Act's provisions are meant to address the lack of specific (or consistent) legal guidance for the extraction of data from complainants' digital devices, especially given the public outcry on the topic.

**B. Overview**

The PCSC Act both creates new powers for data extraction by authorised persons in itself and regulates those powers by providing for a code of practice.[72] This publication—currently in draft form as of July 2022—will set out the exact provisions for how powers in the former must be exercised, while the process for the code of practice's composition and review is outlined in s 42.[73] While the merits of leaving the exact parameters for extraction to be determined via the code were questioned in the House of Lords,[74] this process is arguably analogous to the issuance of guidance under PACE and CPIA.[75] The code of practice does not create any new civil or criminal penalties for its violation; nonetheless, it is relevant for courts to consider,

**69** Alexandra Topping, 'Police and CPS scrap digital data extraction forms for rape cases', *The Guardian* (16 July 2020) https://www.theguardian.com/society/2020/jul/16/police-and-cps-scrap-digital-data-extraction-forms-for-cases.

[70] Police, Crime, Sentencing and Courts Bill Deb 18 May 2021, col 16.

[71] HL Deb 14 September 2021, vol 814, col 1280.

[72] See PCSC Act, sch 3. These authorised persons include police constables across all territorial jurisdictions, British Transport Police constables, and investigators from a host of agencies including the National Crime Agency, HM Revenue and Customs, Border Force, and Gangmasters and Labour Abuse Authority. For the purposes of this report, we focus on the use of these powers by police investigators.

[73] See PCSC Act, s 42. The consultation regarding the code concluded on 19 July 2022, and the code is now due to be laid before Parliament.

[74] HL Deb 14 September 2021, vol 814, col 1317.

[75] See text accompanying n 7 above.

particularly in deciding whether to exclude certain evidence and/or whether the police have breached the HRA/ECHR. Violation of the code can also lead to administrative discipline.[76] The provisions of the PCSC Act and the code must be exercised in accordance with other legal provisions outlined above—e.g. the DPA 2018 and ECHR—they do not supersede them.[77] In the sections that follow, we outline the major impacts of the PCSC Act on consent and necessity/proportionality in the context of complainants' devices.

### C. Consent Searches

The PCSC Act creates a new power in s 37 by which authorised persons might extract data from devices which are voluntarily given to them for several purposes, including the investigation of crime, prevention of harm to children and vulnerable adults, and finding missing persons.[78] This aspect of the PCSC Act appears to purposely avoid the term 'consent', referring instead to obtaining the device user's 'agreement' in order to distinguish this concept from 'consent' as it is used under UK data protection law.[79] It also aims to avoid potential issues or confusion relating to the inability of the device user to consent to the processing of personal data belonging to other individuals with whom they have contact and stored on the device, as discussed further below.

Importantly, s 37 emphasises that agreement to turn over possession of an electronic device and agreement to processing of personal data from the device are separate. It provides that "[a]n authorised person may extract information on an electronic device from that device" if the device has been voluntarily handed over, *and* the user has agreed to extraction of information from the device. This extraction power may only be exercised for prevention, detection, investigation or prosecution of a crime; location of a missing person; or protecting at-risk persons from neglect or harm.[80]

---

[76] Home Office, 'Extraction of information from electronic devices: Draft Code of Practice' (11 July 2022) [**Draft Code**] [12]–[14].

[77] ibid [16].

[78] PCSC Act, s 37. The legislation also creates a power for the extraction of data from the devices of the deceased: see s 41. While the standards and code of practice for exercising both powers are similar, we address only the s 37 power in this report.

[79] See Big Brother Watch, Amnesty International UK, Centre for Women's Justice, defenddigitalme, End Violence Against Women, Fair Trials, JUSTICE, Liberty, Privacy International, Rape Crisis England & Wales, The Survivors' Trust [**Coalition**], 'Report Stage Briefing on digital extraction powers in the Police, Crime, Sentencing and Courts Bill for the House of Lords' (December 2021) 11 ("The language used in this clause deliberately avoids the use of the word 'consent' to evade the legal rights afforded by the consent process as provided by the Data Protection Act 2018, including the ability to give specified and limited consent to data use and the ability to withdraw consent at any time. The term 'agreed' is [instead] now defined").

[80] PCSC Act, s 37(2).

Section 39 sets out the requirements for voluntary agreement, both to handing over possession of the device and for extraction of information from the device. In substance, the requirements are like common law consent outlined below: voluntary agreement must be informed and obtained without undue influence. However, s 39(3) sets out formal requirements for such voluntary agreement: the person must be given written notice specifying what information is sought, the reason it is sought, how the information extracted will be dealt with, that they may refuse or withdraw their agreement to hand over the device or have information extracted from it and that, if they do, the relevant investigation or enquiry will not cease for that reason. The current draft code of practice is particularly insistent on this final point; in the event the complainants' device is indeed the only reasonable line of inquiry, this fact must be clearly explained.[81]

The individual must then confirm their agreement in writing both to handing over the device and to extraction of information from it, and be given a copy of that written agreement.[82] If written agreement is not possible due to a physical impairment or lack of literacy, oral agreement may be given, but must be recorded in writing, and a copy of that record provided to the person.[83] Consent can also be withdrawn under this framework, and this withdrawal will generally cause investigators to cease data processing, though they might have to retain or disclose data in line with disclosure obligations.[84]

Finally, the draft code of practice addresses the vulnerability of complainants who might be asked to give their devices to police. The code of practice gives specific direction to consider the impacts of trauma on victims of crime and how this might affect their ability to consent to data extraction.[85] It also instructs that such victims might be supported by an independent advisor, social worker, friend, or family member, particularly in deciding whether to allow for data extraction.[86] While these provisions do not create new legal tests or standards for consent as a basis to extract and process data, they reinforce the specific impact of trauma on victims' ability to consent following a serious sexual offence. We highlight, in Part IV of this report, further issues with consent in this context.

[81] Draft Code (n 76) [86].
[82] PCSC Act, ss 37(6)–(7).
[83] ibid s 37(5).
[84] Draft Code (n 76) [95]–[97].
[85] ibid [111].
[86] ibid [112], [120]–[127]

**D. Necessity/Proportionality Analysis**

Any increased clarity that the PCSC Act can provide around the necessity and proportionality standard for data extraction is limited by the fact-specific nature of such a determination. Furthermore, the PCSC Act, when used for the investigation of crime, does not supplant the CPIA duty for investigators to pursue all reasonable lines of inquiry.[87] Nonetheless, the PCSC Act and draft code of practice make four main contributions to law surrounding necessity and proportionality. First, they reiterate and clarify the holding in *Bater-James* around what reasonableness and necessity constitute. Second, the legislation and its draft code of practice make clear that data extraction is a means of last resort, only to be pursued if other options are unavailable. Third, the draft code specifically considers how proportionality applies to third-party and (other) confidential data which might be held on complainants' devices. Finally, the draft code outlines basic operational considerations for how investigators should use these powers. We discuss these contributions in turn.

The basic standard for necessity under the PCSC Act is equivalent to that laid out in *Bater-James* and associated guidance. If an officer wishes to use the s 37 PCSC Act power for the investigation of crime, they must "reasonably believ[e] that information stored on the electronic device is relevant to a reasonable line of enquiry" and be "satisfied that exercise of the power is necessary and proportionate."[88] The draft code of practice reiterates the holding in *Bater-James* that there should not be a general presumption in favour of extraction in all cases or certain types of cases categorically.[89] Additionally, officers seeking extraction should document their proportionality assessment and how they have balanced the necessity of the information sought against the invasion of privacy.[90] Finally, as in *Bater-James*, even once an investigator is satisfied that extraction is necessary and proportionate, they must have regard for ways to minimise intrusion, such as by using "selective extraction and use of targeted key words, date ranges or other specifics."[91]

The PCSC Act and draft code of practice emphasise that data extraction from complainants' devices must only be used once other alternatives have been considered and rejected. If any information other than that sought might be discovered in the process of extraction, investigators must consider alternate means of getting that information.[92] These means might

[87] ibid [44].
[88] PCSC Act, s 37(5).
[89] Draft Code (n 76) [45].
[90] ibid [48].
[91] ibid [53]. See also [195].
[92] PCSC Act, ss 37(6) and 37(7).

include examining the suspect's device instead of capturing screenshots.[93] Additionally, investigators may not use anticipated delay as a reason to pursue extraction from a complainant's device over other alternatives.[94] In sum, the PCSC Act and draft code of practice go beyond existing law by explicitly stating that extraction of data from complainants' devices is an act of "last resort" and not just one investigative tool amongst others.[95] This consideration is especially important in the investigation of serious sexual offences given the invasion of the complainant's privacy which can result.[96]

The PCSC Act and draft code of practice give specific consideration to confidential and protected information, which might incidentally be extracted or disclosed. This consideration is not disconnected from existing standards under the CPIA and *Bater-James*, but its specific mention is novel. Under the PCSC Act, certain privileged material, journalistic information, and information from other protected trades must be given specific protection when the PCSC Act powers are used.[97] In particular, PCSC Act powers cannot be used to extract such privileged or confidential material, even via consent or agreement; another power must be used.[98] Investigators must assess the risk of obtaining such material inadvertently through the use of PCSC Act powers, may proceed only if such risk is minimal, and any such material must usually be expressly deleted once an officer realises they have (inadvertently) obtained it.[99] While the consideration of confidential and protected information is in any event encompassed by the overall proportionality inquiry, the PCSC Act and code of practice thus also recognise the specific concerns surrounding this data.

Finally, the draft code of practice lays out operational guidance for using and approving the PCSC Act s 37 power. An officer at least one rank or grade above the requesting investigator should approve the use of the power.[100] Their approval should be granted in line with an agency policy outlining the procedure for seeking approval and should be documented in writing.[101] While these provisions do not necessarily outline the details of any particular approval process nor give substantive guidance as to when use of the power ought to be approved, they do set the expectation that police and investigative agencies should have clear

[93] Draft Code (n 76) [50].
[94] ibid [51].
[95] Ibid.
[96] ibid [129].
[97] PCSC Act, s 43.
[98] Draft Code (n 76) [58]–[59].
[99] ibid [62]–[73].
[100] ibid [76].
[101] ibid [74]–[75].

and consistent procedures around this type of data extraction and that these will be subject to documentation and review.

## II. OUTSTANDING PROBLEMS

At first glance, the enactment of the PCSC Act may be thought to have clarified police searches of complainant devices. On closer reflection, however, much remains unsettled. This section of the report raises—but does not attempt to resolve—several outstanding theoretical and practical issues relating to both consent searches and the operation of the necessity and proportionality analysis.

### A. Consent Searches

Despite the PCSC Act—alongside Part 3 of the DPA 2018—contemplating consent searches in this context, there remain lingering questions as to the extent to which police can legitimately request that complainants voluntarily provide access to their personal mobile phone data, given the position of power police inherently have in such conversations. This section considers three ways in which consent may be insufficient, or illegitimate, in this context. It also raises questions as to the extent to which this Part 3 of the DPA 2018 itself is consistent with the EU instrument it purports to implement, the LED.

*To what extent can complainants meaningfully consent?*

*Compelled Searches*—At least historically, one of the primary practical difficulties in establishing lawful consent to both taking possession of a device and extracting data from that device is the requirement that consent be genuinely freely given. First, the possibility, likelihood or even certainty that an investigation into, or prosecution of, the crimes allegedly committed against a complainant will not continue unless they consent to handing over their mobile device and extraction of data from the device means that—in many cases—complainants may feel compelled to give their consent. The discontinuation of the investigation or prosecution is a "detriment",[102] and the inability of a data subject to refuse consent without suffering this detriment results in a presumption that consent was not freely given. This is a concern in all cases, whether this detriment is expressed, implied or perceived by the complainant. However, it is a particular concern when consent has been granted under a Digital Processing Notice that specifically states that refusal of consent may result in the discontinuation of investigation or prosecution of the offence. Under the PCSC Act, however, the opposite will be mandated: police would be required to give written notice that the

[102] See UK GDPR, Recital 42.

investigation or enquiry will *not* be ended due to a refusal to agree.[103] It is hoped that the PCSC Act will therefore mean this first difficulty no longer arises in practice, albeit it is possible that complainants will not believe such written notice.

Second, since there is generally an imbalance between a complainant data subject and the data controller in this context—the latter a public authority with substantial powers—consent will seldom provide a genuine legal ground, in and of itself, for processing personal data. Although consent is expressly listed as a ground for extracting information from a mobile device in both Part 3 of the DPA 2018 and the PCSC Act, genuine, uncoerced consent is required in both cases. Both Article 8 ECHR and the LED's recognition that consent to data extraction by police will seldom be truly voluntary, as discussed above, appear to suggest a stricter interpretation of the provisions establishing consent as a lawful basis for extracting information from a mobile device is required. In other words, if there is any doubt about whether, in certain types of circumstances, consent can serve as a lawful basis for data extraction (i.e. whether the agreement was truly voluntary and fully informed), it should be assumed that it cannot. A restrictive interpretation is presumably also appropriate in accordance with s 3 of the HRA, which requires legislation to be read and given effect in a manner compatible with the ECHR.

The ICO has emphasised the dilemma posed by potential coercion due to the power imbalance, arguing that consent is an inappropriate basis to process data if the data will still be processed—on another lawful basis—if consent is refused or withdrawn.[104] The ICO explains that seeking consent, in these circumstances, "is misleading and inherently unfair", as it "presents the individual with a false choice and only the illusion of control".[105] To prevent misleading an individual, and to ensure their choice is voluntary and informed, the individual should be notified that the refusal or withdrawal of their consent may influence but not deter a decision to extract their personal information. However, as discussed in the LED Recitals, notifying such persons of these alternative legal bases can be construed as a kind of threat (i.e. "consent or we will extract your data coercively"), undermining the potential for genuine consent.[106]

These issues will likely be exacerbated when the complainant is a 'vulnerable victim', such as a sexual assault complainant, as described in the PCSC Act's draft code of practice. In a vulnerable state, the power imbalance between the complainant and public authority will often

[103] PCSC Act, s 39(3)(e).
[104] ICO, *Who's Under Investigation?* (n 3) 26.
[105] ICO, 'Guide to the General Data Protection Regulation (GDPR)' (1 January 2021) 63.
[106] LED, Recital 35.

be greater. The ICO thus recommends that institutions in positions of power, including public authorities, should generally look for a legal basis aside from consent for data processing.[107] In terms of Part 3 of the DPA 2018, that would be strict necessity.

*Uninformed consent*—As noted, mobile phones have large amounts of data stored on (or potentially otherwise accessible from) them, which a person may not even remember exists. This may impact a complainant's ability to provide truly informed consent. As a result, the more targeted the extraction, the more likely it is that the person will be providing informed consent. Indeed, the PCSC draft code of practice recognises this, noting that some users might not know if their devices contain confidential or privileged information.[108] In addition, since there is a likelihood that at least some of the data on mobile devices is sensitive or Special Category Data, which requires explicit consent for processing, blanket 'consent' to process all unspecified data on a device will likely fall foul of s 42 of the DPA 2018.[109] In other words, the requirement of *informed* consent is linked to the requirement of *specific* consent, particularly in this context. Since the default position is that processing of Special Category Data is prohibited, if consent is the basis for processing such data, that consent must be specific and explicit.

Furthermore, linked to the issue of compelled consent above, where victims are 'vulnerable', it is less clear whether their consent has truly been informed. These individuals are often in shock, such that they cannot comprehend what is being asked of them, and an investigator's determination that they have had sufficient time to consider the request for consent and that they understand the purpose and implications of taking possession of their device and extracting their data may not reflect the reality of their mental state. As a result, what an investigator may determine to be voluntary, informed consent may be unintentionally compelled and uninformed, and thus invalid consent. While the PCSC draft code of practice recognises the existence of this heightened vulnerability,[110] more specific training and guidance for investigators on how to account for that scenario and empathetically obtain valid consent is needed.

*Inability of third parties to consent*—Consent must be provided by the individual whose personal data is being processed. Thus, if the complainant's device contains personal data about other individuals, such as friends, family members, co-workers, clients or business

[107] ICO, *Who's Under Investigation?* (n 3) 26.
[108] Draft Code (n 76) [63].
[109] See also UK GDPR, arts 9(1) and 2(a) (applicable by default where data is processed for purposes other than law enforcement).
[110] Draft Code (n 76) [116]–[127].

partners, these individuals would need to be informed of the extraction and processing of their personal data and agree to it if consent was to be relied on as the legitimate basis for processing. In the context of sexual assault investigations, the police may be particularly interested in records of communication between the complainant and suspect, if any exist, which may include sensitive personal information about the suspect. As a result, the consent of the complainant may not suffice to extract and process this type of information.

It is worth remembering that sensitive data, including health data, and data concerning a person's sex life or sexual orientation, may only be processed in certain limited circumstances (including explicit consent). A complainant's device is likely to contain such information about other individuals: this could be a partner's sexual preferences or performance, a parent's medical test results, or a friends' political views.[111] For example, in *R v Mohammed* (the companion case to *R v Bater-James*), targeted search terms used to review the plethora of messages extracted from the complainant's phone identified a particular exchange of messages "which appeared to reveal an unsatisfactory encounter between the complainant and a male friend".[112] This arguably reveals sensitive information about the friend in question. It will often be impractical and inappropriate to attempt to obtain third parties' consent to the processing of this sensitive information, given the number of individuals likely involved, and the fact that requesting consent from them could place the complainant in an uncomfortable and overly exposed position (they may not want to share with all these individuals that they have been assaulted, for example, and are making a complaint to the police). This is a further factor suggesting that consent may not be an appropriate basis for processing in this context.

The PCSC Act seeks to provide clarity on the conditions under which police may extract information stored on a user's device. It does not rely on third party consent to processing personal data relating to them; rather, in short, it ensures that personal data will only be processed where strictly necessary for a specified purpose (crime prevention, locating a missing person, protecting a vulnerable person from harm) and in a proportionate manner,

[111] See for example Big Brother Watch (n 3) 12 ("Much of this information is incredibly personal, including private conversations with friends, family members and partners; personal and potentially sensitive photographs and videos; personal notes; financial information; and even legally sensitive work-related information such as in emails. Most people's phones and communications contain sensitive information classed as 'special category data' under data protection law: information about an individual's race, ethnic origin, politics, religious or philosophical beliefs, health, sex life or sexual orientation, and as such data extraction from phones requires robust safeguards.").

[112] See *Bater-James* (n 1) [46].

having consideration for other means of obtaining the information sought that would avoid obtaining more information than necessary.[113]

Complainants should be assured that the police will only extract the data that is strictly necessary for the investigation, and that care will be taken to minimise the invasion of privacy suffered by their loved ones as well as themselves. Indeed, complainants (and potential complainants) may feel deeply uncomfortable or distressed at the thought that their decision to file a complaint could result in information that their loved ones had shared in confidence being made available to the police. The following quote from a complainant who could not sleep at night thinking of all the information on her phone, including information about her friends and family, that was now in the hands of the police, illustrates this issue:[114]

> Six months ago, I was seriously sexually assaulted by a complete stranger. Two months after the assault, the police demanded full access to my phone, including my Facebook and Instagram passwords, my photos, stretching back to 2011, notes, texts, emails and the full history of 128 WhatsApp groups and individuals' conversations stretching back over five years. I had no prior or subsequent contact with my attacker. I lie awake at night worrying about the details of private conversations with friends, boyfriends, business contacts, family that are now in the hands of the police. It is a gross intrusion into my privacy and theirs. I feel completely as if I am the one on trial.

The concern that a complainant's fear of exposing friends or family might prevent a case from going ahead, thereby obstructing justice, surfaced in parliamentary debates about the PCSC Bill (as it then was).[115]

It should also be borne in mind that the IPA provides greater protections for third parties in these circumstances: as noted above, if communications are intercepted, either the consent of both the sender and recipient is required, or a directed surveillance authority is required. This 'two party consent' approach contrasts with the 'one party consent' approach adopted in the PCSC Act—the latter offering lesser protection for third parties. Since the IPA does not regulate extraction of stored information from a device itself, it does not apply to the process contemplated by the PCSC Act. However, the IPA's greater protection of third party privacy

[113] See PCSC Act, ss 37, 37(6)–37(10). See also s 37(11) (referring to the authorised person's obligation to have regard for the code of practice, which, in draft form, identifies the 'collateral intrusion on the privacy of third parties' as a key consideration, as explained above).

[114] The complainant described her experience to Harriet Harman MP, Chair of the Joint Committee on Human Rights, who recounted it during a parliamentary debate. See HC Deb 29 April 2019, vol 659, col 45 (quoted in Big Brother Watch (n 1) 43–44).

[115] Police, Crime, Sentencing and Courts Bill Deb 27 May 2021, cols 280–281.

rights raises questions about why no such protections are required when stored communications are extracted directly from a device. While the greater level of protection presumably relates to the fact that interception in real-time is perceived as a greater intrusion into privacy than accessing stored communications, this distinction arguably fails to give due weight to the huge amounts of highly personal sensitive data now commonly stored on mobile devices that a consent search could obtain.

*Is Part 3 of the DPA 2018 consistent with the LED?*

There appears to be some confusion concerning the extent to which consent from the data subject may serve as a legal basis for processing their data in a law enforcement context, under the LED. The main current of thought seems to be that consent may not, in and of itself, serve as the legal basis for processing personal data, especially in relation to special categories (sensitive) data. This potential inconsistency should be borne in mind by prosecutors whenever consent is a legal basis for police data processing in this context, as it may ultimately require courts to resolve difficult issues of statutory interpretation post-Brexit. Details are outlined below.

The concepts of consent and agreement come up in Recitals 35 and 37 of the LED, yet the word 'consent' does not appear in the substantive provisions of the LED. UK courts have acknowledged that Recitals of the EU LED may be useful in interpreting Part 3 of the DPA 2018, shedding light on how its provisions ought to be understood by explaining the reasons behind the substantive provisions of the EU LED from which they originate.[116] Recital 35 notes that when competent authorities perform tasks relating to the prevention, investigation, detection or prosecution of criminal offenses, they are in a position to request or require that individuals comply with their demands or orders. In such circumstances, consent would be inappropriate as a legal basis for processing a data subject's personal data, as any choice is illusory. Indeed, as the Recital explains, in that context:

> [T]he consent of the data subject, as defined in Regulation (EU) 2016/679 [the GDPR], should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes.

[116] *Elgizouli v Secretary of State for the Home Dept* [2020] UKSC 10 [10]–[14] (Lady Hale), [157] (Lord Kerr dissenting on other grounds), and [215]–[226] (Lord Carnwath); and *R (M) v Chief Constable of Sussex Police* [2021] EWCA Civ 42 [27]–[32], [85]–[88], [113], and [133]–[134].

The Recital goes on to add:

> This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

Recital 37, which concerns the specific protection to which 'sensitive' personal data should be subject, poses a similar challenge. It states that sensitive personal data should not be processed unless (i) the processing is specifically allowed by law and is subject to appropriate safeguards provided for by law; (ii) if not specifically allowed by law, the processing is necessary to protect the vital interests of a data subject or another person; or (iii) the processing concerns data which the data subject manifestly makes public. The Recital further notes:

> The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

Again, the Recital suggests a distinction between permitting processing (here, of sensitive data) where the data subject agrees to such processing while reiterating that their consent shall not serve, in itself, as a legal basis for the processing.

This view finds support from the Article 29 Working Party—since replaced by the European Data Protection Board (**EDPB**)—in its analysis of the LED.[117] The Working Party emphasised that "[t]he consent of the data subject can never in itself constitute a legal ground for the processing of special categories of data in the context of the Directive".[118] The Working Party noted that this was a major difference with the GDPR, "stressed explicitly in Recital 35 which considers that Member States may provide by law, that the data subject may agree to the processing of his or her personal data for the purposes of [the LED]".[119] Accordingly, the Article 29 Working Party concluded:[120]

[117] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' 17/EN WP 258 (29 November 2017).
[118] ibid 9.
[119] ibid.
[120] ibid (emphasis added).

> [V]oluntary agreement should only be considered as an additional safeguard under the law in cases in which processing that is particularly intrusive to him or her are envisaged by law[.] Therefore, it is for the national legislator to decide whether and to what extent to allow for data processing under the precondition of the data subject's agreement and whether to include special categories of data (see on this Recital 37).

In considering the prohibition against solely automated individual decisions set out Article 11 of the LED, the Working Party noted that that provision does not contain the same references to exceptions as those provided for in the GDPR mirror provision—Article 22(2), which includes an exception where the automated decision-making is based on the data subject's explicit consent.[121] This led the Working Party to reiterate that "consent could never work as the legal basis as there is a clear imbalance of powers between the data subject and the controller".[122]

One may wonder whether the UK's implementation of the LED in Part 3 of the DPA conforms with this interpretation. The issue was addressed tangentially by the European Commission in its assessment as to whether Part 3 of the DPA 2018 provided protections essentially equivalent to the LED.[123] After explaining that processing is lawful under section 25(2) of the DPA 2018 only if it is based on law and either the data subject has given consent to the processing for that purpose, or the processing is necessary for the performance of a task carried out for that purpose by a competent authority, the Commission noted that personal data transferred pursuant to an adequacy decision would not be processed on the basis of consent in any event as it would not be collected directly from data subjects by UK competent authorities:[124]

> [C]onsent does not appear to be a legal basis relevant for the processing operations falling within the scope of the present decision. In fact, the processing operations covered by the present decision will always concern data that has been transferred under Directive (EU) 2016/680 by a competent authority of a Member State to a United Kingdom competent authority. Therefore, they will typically not involve the type of direct interaction (collection) between a public authority and data subjects that can be based on consent under Section 35(2)(a) of the DPA 2018.

---

[121] ibid 12.

[122] Ibid.

[123] European Commission, 'Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom' C(2021) 4801 final (28 June 2021).

[124] ibid [35].

Nevertheless, for the sake of completeness, the Commission commented on the role of consent:[125]

> While reliance on consent is thus not considered relevant for the assessment carried out under this Decision, it is worth noting, for sake of completeness, that in a law enforcement context processing is never based solely on consent as a competent authority must always have an underlying power that enables it to process the data. More specifically, and similarly to what is allowed under Directive (EU) 2016/680, this means that consent serves as an additional condition to enable certain limited and specific processing operations that could otherwise not be carried out, for example the collection and processing of a DNA sample of an individual who is not a suspect. In this case, the processing would not be carried out if the consent is not given or is withdrawn.

The Commission repeated a similar refrain with respect to the processing of sensitive data.[126] It has also reiterated these views recently in its first report on the operation of the LED.[127]

The EDPB's accompanying opinion, critiquing the Commission's draft UK LED adequacy decision, suggested that it would be appropriate for the Commission to consider the role of consent in a law enforcement context when assessing a country's LED adequacy.[128] The EDPB also commented:[129]

> Consent in the law enforcement context can be relevant as a legal basis for data processing, *as an additional safeguard, or more generally as a basis to execute investigative powers* that lead to the acquisition of personal data, for example the consent of a third party to search their premises, or to confiscate data storage.
>
> […T]he use of consent, as framed in the UK regime, would always require a legal basis to be relied upon. This means that even if the police have statutory powers to process the data for the purpose of an investigation, in certain specific circumstances (for example to collect a DNA sample), the police may consider appropriate to ask for the consent of the data subject.

---

[125] ibid [36] (emphasis added and references omitted).

[126] ibid [38]–[42].

[127] European Commission, 'First Report on Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (LED)' COM (2022) 364 final, 14 ("It is important to recall that, while Member States are not precluded from providing in their national law that the data subject may agree to the processing of their personal data for LED purposes, this consent can only serve as a safeguard and cannot constitute the legal basis for such processing.").

[128] European Data Protection Board, 'Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom' [37].

[129] ibid [33]–[34] (emphasis added).

This would suggest that the different terms were chosen deliberately, with consent referring to a legal basis for processing, and agreement referring to an *additional* safeguard that may be required in certain circumstances, separately and as a supplement to the legal basis for processing. Interestingly, it seems that this terminological difference is not reflected equally in all linguistic versions of the LED—notably, there is no sharp distinction between the terms used in the French version of Recital 35[130]—which casts some doubt on the statement that consent and agreement are meant to have different connotations in the law enforcement context.

This issue requires further research. For present purposes, it would be prudent for police to exercise caution before relying on consent when seeking complainant data given the possibility this would be inconsistent with the LED. While consent is one of the six lawful bases for data processing under the GDPR, processing for law enforcement purposes under the more specific LED is only permitted on one ground, namely necessity for a task performed in the public interest, by a competent authority, for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[131] Part 3 of the DPA 2018 similarly provides for police data processing on this basis, as an alternative to consent.[132] There is a risk that, if consent is requested and given, it will not be genuine, as individuals do not have a real choice—given the possibility police could presumably rely on necessity to process this data in any event. Nonetheless, in certain instances (i.e. for certain types of data), domestic law may require agreement of the data subject as an additional safeguard. This agreement would not be a lawful basis for data processing, and withdrawal of agreement would not preclude authorities processing the data on another basis. However, if agreement is withdrawn there may be practical implications, like reassessment of the processing, or use of less restrictive means.

Additionally, since the LED is useful in this context only as an interpretive tool,[133] the precise implications of the Recitals need not be established here. What is important is that the Recitals

[130] The French version of Recital 35 states that '*le consentement de la personne concernée [...] ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes*' but that '*Cela ne devrait pas empêcher les États membres de prévoir par la loi que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de la présente directive*'. In the Spanish version of Recital 35, the wording difference seems to reflect that in the English version (*el consentimiento* vs *el interesado pueda aceptar el tratamiento de sus datos personales…*). We have not consulted other linguistic versions.

[131] LED, arts 1(1) and 8(1).

[132] See DPA 2018, s 35(2).

[133] See n 116 above.

acknowledge the difficulty of obtaining genuine, voluntary consent from an individual in circumstances where their refusal does not preclude the authority from nonetheless processing their data on other grounds. As such, when interpreting and applying Part 3 of the DPA 2018—including in the context of exercising the new PCSC Act powers—these concerns should be borne in mind, and consent should only ground extraction of information in circumstances where there is no reasonable doubt that the individual genuinely consents to that extraction.

**B. Necessity/Proportionality Analysis**

As discussed in section II.C, the PCSC Act and code of practice do go beyond pre-existing law in defining and refining the reasonableness, necessity, and proportionality requirements for data extraction from complainants' devices. These new parameters, though, still leave several important gaps. We focus on three. First, the new law and guidance, while it calls for a proportionality test, does not adequately tell investigators what considerations ought to be weighed in that test. Next, while requiring the consideration of all reasonably practicable alternatives to data extraction from complainants' devices, the code of practice should provide more specific guidance on how far that search for alternatives must extend. In particular, the final code of practice ought to give a bit more pause to the enthusiasm with which it recommends the search of a suspect's device as an alternative. Finally, the current draft code of practice lacks guidance on the scenario, raised in *Bater-James*, of when investigating a complainant's device might be necessary and proportionate in the context of a defence raised by the suspect.

*What Goes on the Scales in the Proportionality Balancing Test?*

Under the PCSC Act, an investigator's use of the s 37 power to take possession of a device and extract information from it must be "necessary and proportionate to achieve the purpose [the investigation of crime]."[134] In essence, this provision calls for a balancing test between the invasiveness of the search on the one hand and the investigatory need on the other hand. The code of practice provides good guidance on what considerations are to be weighed on the intrusiveness side of that test. For example, the investigator seeking to use the power must account for the privacy of the data holder, any third-party data which might be accessed, and any potential confidential or privileged information.[135] The code of practice is less clear, though, on what goes on the other side of the scale. The authorised purposes of the data

[134] PCSC Act, s 37(5)(c).
[135] Draft Code (n 76) [46] and [68].

extraction include the prevention, detection, investigation, and prosecution of crime.[136] All criminal investigation (or prevention, or detection, or prosecution) is not equal, though. The code of practice ought to give guidance on what facts about a criminal inquiry are relevant to this determination of proportionality.

Several likely candidates for consideration include the severity and nature of the alleged offence, the need for broader public protection, and the likelihood of successful investigation and prosecution. As to the first, the seriousness of the offence might dictate how great an invasion of privacy could be justified. The context in which this power has usually been discussed—serious sexual offences—is not the only one in which police might seek voluntarily obtained digital evidence from victims or witnesses. For comparatively severe offences, a greater interference with privacy may ultimately be justified since the retributive, deterrent, and public safety interests in investigating the alleged offences are presumably greater. Where investigations focus on comparatively less serious offences, a less intrusive investigation will likely be warranted. The final code of practice might set out how the investigator should weigh the offence seriousness in the proportionality inquiry, if at all. If so, the appropriate metric, such as the maximum statutory sentence or whether an offence is indictable, should also be defined. This assessment would likely also include how culpable the suspect is and the harm caused, in line with the assessment of offence severity used in the public interest test for crown prosecutors.[137]

Connected but distinct from the seriousness of the instant offence, police might also consider the need for broader public protection. One might imagine a scenario in which data on the complainants' device might provide evidence not only of that offence but of other offences by the same suspect too. For example, a victim of a sexual assault might have communicated with another person also victimised by the same offender. Similarly, police might believe that a suspect is involved in other criminality that could be disrupted by the successful investigation and prosecution of the instant offence. This consideration is not dissimilar from the notion of sustained public protection in armed policing risk assessment; that is, the mitigation of risks from police action in the short-term might unintentionally exacerbate the risks from long-term criminal activities.[138] Analogously, in the context of data extraction, short-term intrusiveness might sometimes be justified by the longer-term prevention of future offending. The draft code of practice falls short in not laying out how an investigator should consider this broader need for public protection. It is silent on whether the proportionality inquiry can extend beyond the

[136] PCSC Act, s 37(2)(a).
[137] CPS, 'The Code for Crown Prosecutors' (October 2018) [**CPS Prosecutors Code**] [4.14].
[138] College of Policing, APP, 'Armed Policing: Command' (25 March 2021).

investigation at hand to these wider concerns. Ultimately, whether such a broader investigation will ultimately be justified—in particular, whether the potential difficulties of police engaging in 'fishing expeditions' using complainant devices can be sufficiently guarded against—requires further consideration.

Finally, should police consider the likelihood of a successful prosecution in determining whether data extraction is proportionate? One can imagine a complainant would be even more dismayed at the intrusiveness of digital data extraction when it does not result in a successful prosecution. Hence, one might view data extraction that is unlikely to result in a prosecution to be more disproportionate and hence unwarranted under the PCSC Act. The draft code of practice gives no consideration to this point, though. Crown prosecutors generally consider both evidentiary strength and public interest factors in determining whether to prosecute.[139] It will presumably often be difficult for police to consider the strength of the evidence before seeing the evidence from a data extraction but, at the very least, the early involvement of a prosecutor could help investigators assess whether their inquiries are likely to lead to prosecution. Indeed, coordination between investigators and prosecutors is recommended in cases with complex digital evidence.[140] Such involvement, and the consideration of a prosecution's likelihood (and likelihood of success), could help minimise undue intrusion and ensure the use of the PCSC Act s 37 power is proportionate.

*What Does "Reasonably Practicable" Mean?*

Another area in which the PCSC Act draft code of practice falls short in giving adequate guidance is the consideration of reasonably practicable alternatives to data extraction from complainants. Reiterating the holding in *Bater-James*, the draft code of practice states that "[t]he authorised person must assess whether it would be reasonably practicable to use the other means in the circumstances."[141] The draft code explains that delay alone does not render an alternative impractical but it gives little concrete guidance as to how far afield an investigator must look before resorting to data extraction from a complainant's device. One key consideration here may be whether reasonably practical alternatives are limited to the agency and jurisdiction undertaking the investigation. If an investigator believes similar information might be obtainable from another police agency in the United Kingdom without using PCSC Act s 37 powers, must they seek out that alternative first? What about if the evidence could be obtained via a foreign jurisdiction? Similarly, while delay alone does not equal impracticality, delay can lead to investigative issues, such as declining quality of witness recollection and,

[139] CPS Prosecutors Code (n 137) [4.2].
[140] CPS Disclosure Manual (n 46).
[141] Draft Code (n 76) [51].

with some offences, running up against limitation periods. Could delay, through these indirect channels, ever render an alternative means of data-gathering impractical? Finally, the code of practice could elucidate whether there is a hierarchy of intrusiveness and practicality amongst varying uses of the PCSC Act s 37 power. For example, would using that power on a potential witness be a reasonably practicable and less intrusive alternative to using the power on a victim? While it is beyond the scope of this report to answer these questions, we recommend that the final code give greater consideration to these questions, drawing where appropriate on existing law applicable to general policing.[142]

One concrete aspect of guidance from the current draft code of practice is that resort to the suspect's device is preferable to extracting data from a complainant's: "in all cases, extracting information from a device (other than a suspect's device) should be the last resort".[143] On its face, this guidance appears sensible. If the same data can be obtained from a complainant's device and a suspect's device, and the police have a legal power to take possession of and inspect both devices, then the investigator is certainly free to choose the suspect's device—and the use of compulsory powers to obtain a suspect's device may be preferable to using consent to obtain a complainant's for reasons set out above. It is essential, though, that investigators do not construe this provision as a mandate to pursue legally tenuous means of access to a suspect's device rather than ask a complainant for access. Investigators must comply not only with the PACE powers to seize a device but also with all the same authorities that govern data processing outlined above, including the DPA 2018 and ECHR, when accessing a suspect's device. The desire to avoid intrusion into a complainant's device must not prompt police to seek out data from suspect's devices when it is not independently legally justifiable to do so.

*What Does Proportionality Mean in the Context of Seeking Exculpatory Information?*

*Bater-James* establishes, and the PCSC Act does not claim to overrule, a general principle that the police and prosecutors are not obliged to chase down every fanciful claim a defendant might raise as part of their disclosure obligations. *Bater-James* notably referred to the House of Lords judgment *R v H* on this point, which explained that "[t]he trial process is not well served if the defence are permitted to make general and unspecified allegations and then seek far-reaching disclosure in the hope that material may turn up to make them good."[144] At the

[142] See for example *Güzelyurtlu v. Cyrpus and Turkey* [GC] App no 36925/07 (ECtHR, 29 January 2019) [191] and [235]–[238] (recognizing that Member States may have ECHR obligations to seek to obtain evidence from a foreign jurisdiction during law enforcement investigations).

[143] ibid.

[144] *R v H* [2004] UKHL 3 [35].

same time, the CPIA requires that police pursue every reasonable line of inquiry.[145] One area in which the PCSC Act code of practice could bring clarity is by setting out when and to what extent investigators should use defences offered by the suspect to justify the extraction of data from a complainant's device. Such scenarios are not difficult to imagine: e.g., in the case of a serious sexual offence where the suspect offers a defence of consent in interview, the suspect might suggest, and investigators could reasonably suspect, that the complainant might have sent messages supporting that defence. In such a scenario, how are police to interpret the requirements of the PCSC Act and code of practice in determining whether to rely on s 37? This issue again deserves further study.

The consideration of reasonably practicable alternatives, as required by the draft code of practice, would likely mean that if the suspect's device were available and the alleged evidence were also accessible to the suspect (e.g. messages sent between them and the complainant), investigators should access the data from the suspect's device.[146] In other cases, though, the alleged evidence might take the form of messages between the complainant and a third party, for example, or otherwise be inaccessible via the suspect's phone. Should a proportionality inquiry consider the source of the request—the suspect's offered defence—in deciding whether extraction is warranted? The complainant's feelings of vulnerability and intrusion will likely be heightened, given the near inevitability of disclosure of their data to the alleged assailant in this event. On the other hand, the police are duty-bound to pursue this line of inquiry if it is reasonable. Particularly with regards to serious sexual offences between suspects and complainants who are known to each other, such scenarios are likely; the code of practice would do well to give more specific guidance on how proportionality and necessity come into play in such sensitive circumstances.

## IV. RECOMMENDATIONS AND HYPOTHETICAL SCENARIOS

The final part of this report is practical. While it is beyond its scope to resolve the uncertainties in the existing legal framework addressed in Part III, this Part IV attempts to identify key areas where guidance should be given to police on how to operate within the existing framework in a rights-protective manner. It then works through a series of hypotheticals to evidence how these guidelines should be applied in practice.

[145] CPIA, s 23(1)(a).
[146] Draft Code (n 76) [51].

**A. Police Guidance**

All relevant officers who might be "authorised persons" under the PCSC Act ought to receive initial and refresher trainings on the PCSC Act, its powers, and the code of practice.[147] This training ought to be accompanied by jurisdiction-wide guidance, possibly in the form of an authorised professional practice from the College of Policing. This guidance will be particularly important for those expected to review and sanction the use of PCSC Act powers, likely officers around the inspector and chief inspector ranks. While failure to comply with best practices may not necessarily doom a prosecution, it can be considered in staying a prosecution or quashing a conviction.[148] Proper police training mitigates the risk of conviction-jeopardising errors as well as investigative mistakes that ensnare the innocent.

This training should cover the complete lifecycle of an investigation using PCSC Act-based data extraction. This would begin with the threshold inquiry whether data extraction is likely to be needed. It then ought to cover the necessity and proportionality tests, including what practicable alternatives might be available within a particular area and what alternatives might be available via mutual aid from other agencies. Next, all investigating officers should grasp the process of seeking informed consent from victims to ensure they understand the specific data being sought from their device, how this data will be searched for and extracted, their right to refuse a digital search, and the consequences of their refusal. In line with the PCSC Act code of practice, officers should be trained on special considerations for dealing with vulnerable complainants and ways they might make the process easier.[149]

Record-keeping will also be vital to good police practices in this area. Not only should records of training be kept, but an audit trail or record for every process of data searching and extraction applied to a complainant's digital device should be recorded.[150] Record-keeping obligations of this type are separately required by Part 3 of the DPA 2018[151]—it is disappointing to see that the UK government has recently proposed weakening these.[152] Practically, another investigator should be able to understand and follow the method used to retrieve the same information. Where there are large quantities of data, the investigating officer in charge should form a search strategy around how data is to be analysed or searched. Audit trail or records should include analytical techniques, including software; date and time the

[147] PCSC Act, sch 3.
[148] *R v E* (n 6) [41].
[149] Draft Code (n 76) [111].
[150] Association of Chief Police Officers, 'APCO Good Practice Guide for Digital Evidence' (March 2012) 37.
[151] DPA 2018, s 62.
[152] See DPDI Bill, cl 16.

search was conducted; details of the individual completing the search; extent and manner of the search; and rationale behind decisions and searches.[153] We recommend a template is created and implemented across police forces in England and Wales. This will ensure consistency across forces in evidencing these requirements. While it is beyond the scope of this report to recommend specific training materials or practices, what is clear is that police training on this issue must reflect the law. Many difficult experiences for complainants pre-PCSC Act stemmed not from legal barriers but from investigating officers who were unfamiliar with the law or operating under misconceptions of what the law required with regards to reasonable lines of inquiry. In the final subsection of this report, we present several hypothetical scenarios an officer might encounter along with relevant guidance.

### B. Hypothetical scenarios

*Complainant reports sexual assault by a stranger*

Based on the requirement that data should only be extracted when absolutely necessary, even where consent is provided, it is unlikely that there will be a lawful basis to extract data from a complainant who alleges sexual assault by a stranger. This is supported by the statements of the Court of Appeal in *Bater-James*.[154] The Court held that there are some "cases where there is no requirement for the police to take the media devices of a complainant or others at all".[155] These include "sexual offences committed opportunistically against strangers".[156]

One may wonder, then, whether a complainant's assertion that their aggressor was a stranger should be the end of the matter. In general, there will likely be no reason to disbelieve the complainant's assertion, and thus no reasonable ground for requesting that the complainant surrender their phone. In the event that something uncovered during the course of an investigation puts that assertion into doubt, suggesting that the complainant did in fact know the aggressor/suspect, the police would revisit the need to request access to their phone in order to pursue a reasonable line of enquiry. In such circumstances, the police would need to keep in mind alternative, less intrusive means of pursuing this reasonable line of enquiry. For example, if the suspect claimed that they knew the complainant and suggested that information on the complainant's phone would demonstrate this, the police could ask the suspect to provide proof of this relationship, as this would likely allow for a more targeted, less intrusive manner of obtaining the information.

[153] See CPIA Code (n 7) [4].
[154] *Bater-James* (n 1) [76] (citing CPS, *Disclosure* (n 43)).
[155] ibid.
[156] ibid.

*Complainant reports historic allegations*

Amongst "cases where there is no requirement for the police to take the media devices of a complainant or others at all", *Bater-James* also referred to "historic allegations where there is considered to be no prospect that the complainant's phone will retain any material relevant to the period in which the conduct is said to have occurred and-or the complainant through age or other circumstances did not have access to a phone at that time".[157]

Imagine, for example, that a young woman comes forward with an allegation that she was assaulted by a family member as a child, before she had her own phone—anything on her current phone will likely be irrelevant to the investigation. Similarly, if a person alleges domestic abuse relating to events that took place 15 years ago, the phone they had at the time, if they had one, might be long gone. Again, it would likely be inappropriate to request access to the complainant's current phone in such circumstances without particularised knowledge that it might contain relevant information to a reasonable line of inquiry.

*Complainant consents to police processing their data, but refuses to hand over her device, as it will be for such a long period*

Where the complainant refuses to consent to hand over their device, the police should:

(i) seek to understand the refusal, reassure the complainant as to the process, see if the complainant would agree to providing screenshots of certain message or to allowing police to view or copy specific information;[158]

(ii) consider whether less intrusive means are available to obtain the evidence, which would potentially alleviate the complainant's concerns;

(iii) again, seek to obtain the information from a different source (which should be done in any event). Such sources may include friends or family members of the complainant,[159] witnesses of the incident, where relevant, and the alleged offender;

(iv) determine whether the information must be obtained despite the complainant's refusal due to an overriding public interest (for example, to 'prevent a dangerous offender from committing further offenses')[160] in which case the police may seek a witness summons to obtain the device. It is important to recall that public interest in law enforcement is not enough, because this interest must be balanced against the person's right to a private life. As a result, the competing public interests must be weighed against each

[157] CPIA Code (n 7) [75].
[158] See Coalition (n 79) 6–7 (citing *Bater-James* (n 1) [77]–[79].
[159] See *R v Charnok* [2021] EWCA Crim 100.
[160] See APP, *Extraction of Material* (n 10) 6.

other,[161] and an investigator must show that the public interest served by the coercive extraction of information outweighs the public interest in privacy. It would need to be shown that acquiring a device without agreement is necessary, and is not excessive in the circumstances (proportional); and

(v) in the same vein, determine whether the case can proceed without the witness's device, considering notably whether the trial process, including cross examination of the complainant, can compensate for the missing evidence (the same question will be posed where the allegedly relevant information on the complainant's phone has been deleted or lost).

If a complainant is a vulnerable victim, their phone should ideally be retained for no more than 24 hours. If it must be retained for longer than 24 hours, another device should be given to that complainant in the interim.

*Complainant consents to handing over their device and for data to be extracted, but they are emotional and distressed after a traumatic incident or after recounting painful memories*

In accordance with the PCSC Act's code of practice, the complainant should be given sufficient time to think about whether they wish to consent.[162] It must be clear that they genuinely understand what is being asked of them and the Digital Processing Notice must be read aloud and explained in simple terms if necessary. The investigator should consider whether another person should be included in the discussions who can support the complainant and assist with the explanation of what is being asked of them. An interpreter should be included, if that will assist properly informed consent. These additional measures may not always be necessary, and—if it is clear that a complainant does not require additional time or assistance—should not be carried out as a checkbox exercise, which would unnecessarily draw out the process for an already-traumatised complainant. Ultimately, the goal is to ensure genuine, voluntary, informed, and specific consent, and these additional measures for vulnerable complainants are means to that end.

*Complainant consents to their device being handed over, and information being extracted from it. However, after a few days, they return and withdraw their consent, and demand the return of their device*

The investigator should try to understand the reasons for the withdrawal of consent, and attempt to allay concerns and explain why the information being extracted is necessary for the

[161] ibid.

[162] Draft Code (n 76) [123].

investigation. It is not permissible to threaten to close the investigation due to the withdrawal of consent, unless the device is indeed the only remaining reasonable line of inquiry, in which case the circumstances and actions taken to that point must be explained to the complainant.[163] Less restrictive means to access the information while maintaining the integrity of the investigation should be considered again at this stage (for example, screenshots taken in the presence of the investigator and the complainant).[164]

If consent is withdrawn, any information obtained while consent was in place may be retained as part of the investigation records and may be disclosed if necessary, but further information may not be extracted and the device should be returned.[165] However, the investigator may retain possession of the device and continue with the extraction on another lawful basis (being strict necessity, under Part 3 of the DPA 2018), if that course of action is necessary to fulfil their obligations CPIA to obtain and retain materials and pursue reasonable lines of enquiry; or if there is a risk of harm to the device user or others that cannot be mitigated through other less restrictive means.[166]

## V. CONCLUSION

Police investigating serious sexual offences, particularly between complainants and suspects known to each other, face the difficult and sensitive task of conducting a thorough and fair investigation as the law requires while respecting the privacy rights of suspects and victims — as the law also requires. The stated aim of the PCSC Act was to "provid[e] clarity" to a particularly murky area of this legal landscape, the extraction of data from complainants' digital devices.[167] While the PCSC Act did not supersede any of the pre-existing statutes concerning criminal investigation, disclosure, and data processing, it provides a specific statutory framework and accompanying code of practice for extracting data from devices voluntarily given to police. The legislation and draft code of practice recognised the complexities of gaining freely-given consent from complainants in such scenarios, and these documents laid out clearer guidance for when such data extraction would be necessary and proportionate.

Despite this welcome clarity, the PCSC Act and current draft code of practice leave several key areas unaddressed. With regards to consent, particularly as it intersects with the requirements of the LED, the PCSC Act and code of practice do not fully address issues of

[163] Draft Code (n 76) [86].
[164] See Coalition (n 79) 6-7.
[165] Draft Code (n 76) [96].
[166] See APP, *Extraction of Material* (n 10) 46–47.
[167] HC Deb 5 July 2021, vol 698, col 604.

voluntariness, informed consent, and the information of third parties. In describing tests of necessity and proportionality, the legislation and draft code similarly fall short in addressing what concerns, precisely, officers should account for in such a balancing test. Finally, as we hint at in Part IV above, little of these legal developments to date will be of any use to complainants and suspects if not properly implemented by front-line police officers. We close on the hope that, with widespread training and adequate resourcing for investigations, the PCSC Act and final Code of Practice might indeed bring more clarity and fairness to this area, both for complainants and suspects and the public generally.