This contribution was provided on a voluntary basis (i.e. not remunerated), unlike the other country contributions which were paid work.

Like all other country reports, this contribution does not necessarily represent the complete or fully up to date legal position on the mentioned topics and does not constitute legal advice.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

The FORMOBILE project is aimed at creating better mobile forensic tools to help combat crime more efficiently, enlarging the capacities of both first responders, common forensic laboratories and highly specialised laboratories and experts by providing them with better tools to acquire, decode, and analyse data coming from mobile devices. The majority of these tools will be integrated in the existing suite of MSAB software (XRY). Please refer to the FORMOBILE website for more information and especially to the work package breakdown of WPs 4-6: https://formobile-project.eu/project#.mod-wp-steps. It is essential to have this background to be able to accurately answer this questionnaire.

One of the aspects of the FORMOBILE project is to make sure that these tools are able to be used in the EU for the collection, decoding and analysis of information from mobile phones in a way that makes the obtained evidence admissible in court ("from crime scene to courtroom").

Hence, the questions that make up this questionnaire in essence aim to understand how mobile forensic tools aimed at retrieving, decoding and further analyzing information from a mobile device (e.g. a smartphone), are allowed in your jurisdiction under the applicable criminal law. We are especially interested in:

- whether technical measures may be used (and to what extent) to bypass security;
- to what extent the data on the mobile device may be read, searched, used and copied etc.;
- what the formal conditions are for accessing data on a mobile device;
- who must order such actions and in what level of detail the mandate must describe the authorized actions;
- in what scenarios this is permissible (only in certain scenarios, only if the phone belongs to the accused?), as well as the potential differences between scenarios;
- existing limits on the access to or further analyzing and use of the data on a mobile device.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

In addition, we want to know under what conditions information on the Cloud can be accessed and if this is possible by technical means. We are also interested in any human rights' impacts, existing guidelines and issues in practice, existing case law and any other elements you deem relevant.

As we want to be able to compare answers across jurisdictions, we have drafted this request for information in a questionnaire format. This, however, does not mean we are looking for simple yes/no answers. Most questions are open questions and naturally invite an elaborate answer. Some questions may perhaps in theory be answered as yes/no question, but **please give as much guidance and details as possible within every question, to enhance our understanding of the legal system in your jurisdiction. Always cite the provision of the law or the case law you are relying on in providing an answer and please try to be exhaustive or at least as complete as possible. If you are relying on practical guidance or other informal rules and practice, please also refer to this and, if documentation on this is available, provide the link to where we can find this documentation.**

Please feel free to give additional guidance in the comments section at the end, in case you feel we did not sufficiently cover certain elements throughout the questionnaire.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

The questionnaire is made up of 61 questions, in the following sections:

- ☐ Introductory questions
- ☐ Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices
- ☐ Section 2: Criminal procedure rules on analysis of data from mobile devices
- ☐ Section 3: Admissibility of evidence before court
- ☐ Section 4: Interpretation and presentation of evidence from mobile forensics before the Court
- ☐ Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial
- ☐ Section 6: Comments

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Introductory questions:

1. **Question:** *Please identify your organisation and your individual position?*

Answer: I am a Senior Lecturer in Policing at [an UK university], although I am participating in a purely independent capacity, unrelated to my professional position.

2. **Question**: *Where is your organisation based?*

Answer: UK.

3. **Question:** *Do you have a legally defined term for a "mobile device"? If yes, what kind of devices are included within it? (e.g. Smartphones, Tablets, Smartwatches, Cameras, MP3-players, Navigation devices, Drones)*

Answer: The main law is the Computer Misuse Act 1990 (CMA). The law and case law refers to the functions and capability of devices rather than the size or ease of transporting. The CMA does not provide a definition of computer because rapid changes in technology mean any definition would soon become out of date. Definitions are left to the courts, who will interpret the legislation appropriately, given the degree of technological development at the given time. In *DPP v McKeown, DPP v Jones ([1997] Cr. App. R. 155, HL)* a computer was defined as "a device for storing, processing and retrieving information".

In the case of using a mobile device whilst driving, which is an offence under the Road Traffic Act 1988, s41D refers to *driving or supervising the driving of a motor vehicle while using a hand-held mobile telephone or other hand-held interactive communication device* …., a hand-held device in this instance is something that 'is or must be held at some point during the course of making or receiving a call or performing any other interactive communication function'. The offence applies if a phone has to be 'held' while making or receiving a call. However, this offence relates to the distraction and lack of control creating a danger rather than information on the device.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices

Question: *Mobile devices (e.g. a smartphone) may enter investigations in a variety of scenarios. A suspect or a witness may have a smartphone on them during questioning or at the scene, mobile devices may be found during the search of a home or other premises, a suspect caught in the act may have a mobile device in use etc. We want to know for all these scenarios (and others you may be able to identify) what the applicable national rules are, namely answering the following questions:*

N.B In light of the above answer relating to the definition of 'mobile device', the below answers are based upon a common understanding of mobile device.

Mobile device not seized

4. *Under what circumstances can a mobile device be read or searched without seizing it?*
5. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*
6. *Is it allowed to use technical tools to bypass security?*
7. *Can information be copied or only read at this stage?*
8. *Is consent of the owner/person in possession of the mobile device necessary?*
9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*
10. *Must the owner/person in possession of the mobile device be informed?*
11. *Who can order a search and what are the formal requirements, if any?*
12. *Does it matter whether this person is the accused or witness/third party or the victim?*
13. *What about data stored in the Cloud, what is the procedure to access/read this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order (hereinafter: EIO) or Mutual Legal Assistance Treaties (hereinafter: MLAT) the only route or do other options exist? Please elaborate.*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

14. *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

15. *Does not following the applicable rules always lead to inadmissibility in court of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

In relation to the scenarios outlined above, if officers were searching premises this would be under a legal power. The Police and Criminal Evidence Act 1984 provides various powers to search a premises without a warrant. The powers only extend to items of evidential value in relation to the subject of the search.

Personal note: I do not entirely understand what these questions are aimed at. If devices are examined this is usually carried out after they have been seized and they only would be seized if they contained evidence or information / material pertinent to the purpose of the enquiries. The questions seem to be asking whether mobile devices can be examined outside of usual police powers and whether this can be done by bypassing security measures. This is not something that would happen. However, I have set out some information below that might be useful.

Where individuals are stopped by police officers under 'stop and search powers' the primary purpose of using these powers is to allay or confirm suspicions that unlawful items are being carried without necessitating a formal arrest. In the majority of cases these items are either offensive weapons or drugs. Therefore, the primary actions would be in relation to finding the items not going through their mobile devices, which wouldn't contribute to the purpose of the stop. The legal basis for the use of stop and search in the majority of cases is either the Police and Criminal Evidence Act 1984 or the Misuse of Drugs Act 1971. Consent is never a legal basis.

Under **s43** of the **Terrorism Act 2000**, police officers have the power to view digital images contained in mobile telephones or cameras carried by a person who is being searched under this power, to discover whether the images constitute evidence that the person is involved in terrorism. Officers also have the power to seize and retain any article found during the search which the officer reasonably suspects may constitute evidence that the person is a terrorist. This includes any

mobile telephone or camera containing such evidence. Officers **do not** have the power to delete digital images or destroy film at any point during a search. (deletion or destruction may only take place following a seizure if there is a lawful power, such as a court order, that permits such deletion or destruction.

Police officers in the UK have the power to stop and search under various pieces of legislation, one of them being the Terrorism Act, as outlined above. The other powers of stop and search are related to the article or action that forms the basis of the officer's suspicion. The most commonly used reasons are for offensive weapons or drugs. In an ordinary stop and search, officers are not entitled to routinely examine mobile phones for IMEIs without having reasonable grounds to suspect that the mobile phone is stolen.

In all situations, the mobile device must be pertinent to the enquiries being made or the offence that is suspected of being committed. Searching a mobile device is intrusive and additional considerations must be made if the person is considered vulnerable. As well as complying with police legislation and procedures, the fundamental right to privacy must also be factored in. Police officers must always consider whether the action is proportionate to the aim being pursued, whether it is lawful and necessary (or whether the same objective can be achieved in a less intrusive way) and whether they can justify their actions.

Mobile device seized

16. *Can the mobile device (e.g. a smartphone) be seized?*

17. *What are the conditions for this, who can order it and what are the formal requirements?*

18. *If seized, can the mobile device always be searched, information copied etc?*

19. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*

20. *Is consent of the owner/person in possession of the mobile device ever a relevant element?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

21. *Can the owner/person in possession of the mobile device (if identified) be forced to unlock the device?*

22. *Must the owner/person in possession of the mobile device be informed? If so, about what exactly?*

23. *Is it allowed to use technical tools to bypass security measures and/or anti-forensic measures?*

24. *Does it matter whether this person is the accused or witness/third party or the victim?*

25. *What about data stored in the Cloud, what is the procedure to access this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order or Mutual Legal Assistance Treaties the only route or do other options exist? Please elaborate.*

26. *What about data stored in the Cloud, where you are unable to determine the location of the server or the identity of the service provider?*

27. *Can you legally access data in the Cloud, even if there is no app that links to this data or other direct link from the mobile device?*

28. *How is the access to data kept by a Service Provider related to the device regulated? Is it performed upon a Court order, or also through other means?*

29. *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

30. *Does not following the applicable rules always lead to inadmissibility of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

Please, answer all these questions separately for each scenario or instance which, in your opinion, is (partially) subject to different rules than other scenarios. At least, make the difference between the scenarios where a mobile device is seized and where it is not. If all sub-scenarios in one of these scenarios are the same, it suffices to only answer the questions once. However, most jurisdictions have different situations in which seizure is possible (e.g. in the context of a search of premises vs. not in the context of a search), so please differentiate between these scenarios, as well and answer the questions for them separately. If you prefer, you can answer the questions in their

totality in an integrated explanation, as long as all elements are covered and again, various scenarios are differentiated between.

Please, give as much guidance as possible to enhance our understanding. Always cite the provision of the law or the case law you are relying on (legal basis) and mention conditions, people involved in the action, formal requirements etc., even if not specifically asked.

Answer: Indication of length of answer: at least a couple of pages, as this is the main overview question.

31. **Question***: In cases where the examination or data acquisition is not possible without changing the configuration of the device, is there a strict protocol that should be followed (e.g. procedure and changes should be tested, validated, and documented)? If yes, please specify on what rules this is based and what the requirements are. Please also provide examples.*

Answer: Indication of length of answer: 1-2 paragraphs.

32. **Question:** *Are there any specific rules in criminal procedure that regulate the use of mobile forensics tools using/deploying AI technology? Are there any conditions which need to be met so AI-powered tools could be applied in the process of evidence collection?*

Answer: Indication of length of answer: 1-2 paragraphs.

33. **Question:** *What are the main legal issues in your jurisdiction in the cases when mobile devices are involved in crimes across geographical boundaries? What procedures are foreseen to tackle these multijurisdictional issues? Should the forensic examiner be aware of the nature of the crime and the regional laws/legislative framework?*

Answer: Indication of length of answer: couple of paragraphs

34. **Question:** *Is there an established procedure/course of action to decide whether to apply the EIO or another instrument for cross-border gathering of evidence within the EU?*

Answer: Indication of length of answer: 1-2 paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***35.* Question:** *Since, the abovementioned Directive does not preclude the application of MLAT by judicial authorities under some circumstances, what is the practice in your jurisdiction?*

Answer: Indication of length of answer: 1-2 paragraphs.

***36.* Question:** *Are you aware of any existing cooperation mechanisms and practices with the private sector?*

Answer: Indication of length of answer: 1-2 paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 2: Criminal procedure rules on analysis of data from mobile devices

***37.* Question:** *When data has been made accessible through mobile forensics, are there any rules on how the data must be analysed, especially to take into account:*

- *Data protection concerns (Law Enforcement Directive 2016/680 and implementing national law)*
- *Privacy concerns and respect for core area of private life (i.e. how is it guaranteed that very sensitive information, not relevant to the investigation is not used)*
- *Human rights such as the right to a fair trial (tools may deliver faulty results and methods used are often untransparent) and the right to non-discrimination (tools that are untransparent may contain bias)*
- *What information can be retained/copied? For how long?*

Please elaborate on both criminal procedure law, relevant data protection law and any other measures or guidelines that may exist. Please also cite and explain relevant case law.

Answer: Indication of length of answer: couple of paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 3: Admissibility of evidence before court

38. **Question:** *Are there general rules or guidelines on the admissibility of electronic evidence in your jurisdiction applicable to mobile forensics, not yet discussed above?*

Answer: Indication of length of answer: 1-2 paragraphs.

39. **Question:** *Are the criteria for admissibility of evidence collected through mobile forensics the same as for the other types evidence? Please elaborate in any case.*

Answer: Indication of length of answer: 1-2 paragraphs.

40. **Question:** *What if procedural rules are not followed? Can evidence from mobile forensics still be submitted to the Court in certain circumstances, balancing out the interest of the criminal justice with the severity of the procedural breach?*

Answer: Indication of length of answer: 1-2 paragraphs.

41. **Question:** *Specifically, if data in the Cloud is accessed according to criminal procedure, but it turns out to be located outside your jurisdiction does this mean it is not admissible at all? Is it relevant that there was reasonable doubt about the location of the data at the time?*

Answer: Indication of length of answer: 1-2 paragraphs.

42. **Question:** *What are the consequences if mobile evidence are altered either intentionally, or unintentionally due to their dynamic nature during the investigation process? Note that intentional alteration refers to using a process to uncover data which is known to alter some (meta)data, not to the falsification of evidence. The question is more whether any alteration, even on small and not relevant data may render the evidence inadmissible.*

Answer: Indication of length of answer: couple of paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

43. **Question:** *Specifically, are there rules on the used technology, methodology or standard, such as for example that this must be forensically sound as a prerequisite for admissibility? If yes, please elaborate.*

Answer: Indication of length of answer: 1-2 paragraphs.

44. **Question:** *Are you aware of existing case-law in your jurisdiction, dealing with the admissibility of evidence produced using mobile forensics? If yes, please elaborate.*

Answer: Indication of length of answer: 1-2 paragraphs.

45. **Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the evidence to be admissible? (as critical to the validity of evidence, their quality and impact evidence's acceptance by the courts)? If yes, please elaborate.*

Answer: Indication of length of answer: 1-2 paragraphs.

46. **Question:** *Is a failure to comply with Data Protection law, or privacy rules in itself, enough to refuse admissibility of the evidence, even when procedure is otherwise followed?*

Answer: Indication of length of answer: 1-2 paragraphs.

47. **Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because the admissibility was questioned? If yes, please elaborate on at least 3 cases.*

Answer: Indication of length of answer: 3+ paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 4: Interpretation and presentation of evidence from mobile forensics before the Court

48. **Question:** *Are there general rules or guidelines on the interpretation and presentation of evidence from mobile forensics, such as:*

- *Is mobile forensic evidence given a certain probative value?*
- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*
- *Must such evidence be examined by an expert witness?*
- *If not obligatory, is this a common practice?*
- *What are the requirements for experts (experience, independence, training, etc.)?*
- *Is there a centralised management of mobile forensic operations in your jurisdiction to ensure the work is compliant with standards and can be presented in court in a consistent manner?*

Answer: Indication of length of answer: couple of paragraphs.

49. **Question:** *Are you aware of existing case-law in your jurisdiction dealing with the interpretation and presentation of evidence produced using mobile forensics? If yes, please elaborate.*

Answer: Indication of length of answer: 1-2 paragraphs.

50. **Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the interpretation and presentation of evidence before a court? Or alternatively which is not obligatory but considered as critical for the validity of evidence, its quality or the impact of the evidence and its acceptance by the courts? If yes, please elaborate.*

Answer: Indication of length of answer: 1-2 paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***51.* Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because of interpretation issues or presentation issues (e.g. considered admissible but not reliable)? If yes, please elaborate on at least 3 cases.*

Answer: Indication of length of answer: 3+ paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial

52. **Question:** *Are there rules or guidance, or is there case law in your jurisdiction on how to respect the right to a fair trial in case of evidence extracted via mobile forensics? What practices are established in view of the respect of the principle of equality of arms?*

Answer: Indication of length of answer: couple of paragraphs.

53. **Question:** *Is there any training required by law for the judges, prosecution, expert witnesses, lawyers involved in cases with evidence coming from mobile forensics?*

Answer: Indication of length of answer: couple of paragraphs.

54. **Question:** *Is there a pre-determined time duration/limitation period required for the extraction of evidence from mobile devices, time for decoding, reviewing and analysing of the data, time for reporting that data in a form that prosecutors and others can use?*

Answer: Indication of length of answer: 1-2 paragraphs.

55. **Question**: *What are the procedural rights inherent to the different participants in a criminal procedure (i.e. the prosecution, the court, the defendant, the witness, the victim, etc.)?*

Answer: Indication of length of answer: couple of paragraphs per different participant.

5.1 The Prosecution

56. **Question:** *Are there any requirements or guidance provided to the prosecution as how to control and deal with mobile forensics and evidences?*

Answer: Indication of length of answer: couple of paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

5.2 The Court

57. **Question:** *Is there judicial control over the approaches and methods used for acquiring, collecting and analyzing evidence? Please refer to case law if possible.*

Answer: Indication of length of answer: couple of paragraphs.

58. **Question:** *How does the Court assess the evidence obtained via mobile forensics? Please refer to case law if possible to illustrate the approach.*

Answer: Indication of length of answer: couple of paragraphs.

5.3 The defendant and defender

59. **Question:** *Are there rules and standards regulating the defendant and his/her defender's rights to access and to make copies of the acquired mobile evidence? Are they able to get any information on the process used to acquire mobile forensic evidence (e.g. information on how the tools work, the procedures used, the parties involved and how the validity of the results is guaranteed)? Please refer to case law if possible.*

Answer: Indication of length of answer: couple of paragraphs.

5.4 Witnesses

60. **Question:** *During the pre-trial stage, how is the right to privacy of the witnesses preserved? Are there any practical steps taken to exclude certain types of information which are cumulatively non-relevant to the case and too private? Are there particular requirements for witnesses regarding their capability to testify in terms of mobile forensics both in the pre-trial and the trial phase of the criminal proceedings? Please refer to case law if possible.*

Answer: Indication of length of answer: couple of paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

5.5 The Victim

***61.* Question:** *How are the victim's/victims' rights ensured during both the pre-trial and the trial phase of the proceedings? How is their privacy preserved? Can they use the evidence obtained via mobile forensics when exercising their rights? Please refer to case law if possible.*

Answer: Indication of length of answer: couple of paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 6: Comments

If you feel some important elements of your national law relating to the use of mobile forensics in criminal investigations have not sufficiently been covered, please explain them here. If you feel an overview is missing, please also provide guidance on this below.

Answer: Indication of length of answer: few paragraphs up to a couple of pages.

It may be helpful to provide here the formal definitions of 'digital forensics', which encompasses some of the activities in question:

The **National Police Chiefs' Council** (NPCC) portfolio board has defined digital forensics as:

The application of the science to the identification, collection, examination and analysis of electronic data whilst preserving the integrity of the information and maintaining the chain of custody of that data.

The **Forensic Science Regulator** defines it as:

Digital forensics is the process by which information is extracted from data storage media (e.g. devices, remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement [including CCTV], audio analysis, satellite navigation, communications), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings. The definition is intentionally wide, and any exclusions will be explicit. […]

In the UK, there are several oversight bodies that provide standards of best practiced and approved methods relating to digital forensics. While these don't have statutory powers (there is legislation for police powers), they provide important guidelines relating to this area. In general, the 43 police forces in England and Wales have autonomy, although they will comply with the national guidance and approved practices as below:

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

College of Policing have no statutory power of enforcement but do set the national Authorised Professional Practice (APP) for policing. APP is regarded as the official source of professional practice on policing. Police officers and staff are expected to have regard to APP in discharging their responsibilities. There may, however, be circumstances when it is perfectly legitimate to deviate from APP, provided there is a clear rationale for doing so. The purpose of the College (that was created by statute) is to provide those working in policing with the skills and knowledge necessary to prevent crime, protect the public and secure public trust.

The National Police Chiefs' Council (**NPCC**) has several functions but in particular, guide the national operational implementation of standards and policies as set by the College of Policing and Government. It also works with the College of Policing to develop joint national approaches in various areas, including technology. The body has no statutory power of enforcement but is seen as setting standards that individual forces are expected to follow.

The **Forensic Science Regulator** (FSR) works with the Home Office to ensure that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards. This includes digital forensics. The FSR provides comprehensive guidance for all participants in the criminal justice process, in relation to best practice in the area of forensics. The FSR can set standards but has no statutory powers to enforce them.

General Powers

There are a range of powers under various laws, depending on the nature and purpose of the enquiries being carried out. Going through them all would take a disproportionate amount of time, so some of the main ones are referred to here. Of note, there is currently a review of search warrants by the Law Commission, instigated by the Home Office. The outcome of the inquiry and recommendations are due to be published later in 2020. This should initiate actions that will result in a less complex and simplified legal landscape in relation to police powers and will extend protections for citizens as well as increase oversight and judicial scrutiny.

Under s19 of the Police and Criminal Evidence Act 1984 if an officer is lawfully on premises they may seize anything that is on the premises if they have reasonable grounds for believing that it was obtained as a result of the commission of an offence or it is necessary to seize it to prevent it from being concealed, lost, damage, altered or destroyed. Also, s20 and s21 apply these powers specifically to the seizure, access and copying of computerized information, including that on mobile phones.

Under ss50 and 51 of the Criminal Justice and Police Act 2001 police can remove items from premises or people for the purpose of sifting or examination elsewhere (e.g. where a device may hold bulk material). The Police and Criminal Evidence Act 1984, Code of Practice B also applies, see below.

Where material is removed for this purpose a written notice should be provided to the occupier or person from whom the material has been seized, setting out:

- What has been seized
- Grounds for seizure
- How a person with relevant interest can apply under ss 59 to 61 of the Criminal Justice and Police Act for material to be secured or returned

The person may wish to be present or represented during the examination. Officers must not remove more material that is necessary. The examination must be carried out as soon as reasonably practicable after seizure and should be limited to whatever is necessary to

determine how much of the material can lawfully be seized. Anything that falls outside of the terms of the warrant must be returned as soon as possible.

Police and Criminal Evidence Act 1984, Code B applies to police powers in relation to searching premises and seizing and retaining property found on premises and persons. Those powers may be used to find property and material relating to a crime. Search and seizure powers can also be derived from a justice of the peace issuing a warrant.

The Criminal Procedure and Investigations Act 1996 and its code of practice, sets out how officers should record, retain and reveal to the prosecutor, material obtained during a criminal investigation that is relevant to the investigation. Under this legislation, there is also an obligation to pursue all reasonable lines of enquiry and gather and retain all relevant materials.

Investigatory Powers Act 2016 (IPA) makes provisions about the interception of communications and how to handle intercepted material. An interception can be either during the transmission of the communication or through accessing stored communications. Police must have 'lawful authority' to carry out interception of communications, under s6 of the IPA. This Act also sets out the circumstances in which there can be lawful authority without a warrant. Chapter 12 of the Interception of Communications code of practice issued under Schedule 7 of the IPA summarises the requirements for the lawful interception of communications without a warrant. These include:

- The sender and intended recipient have consented to the interception
- Either the sender or intended recipient have consented and a RIPA authority is in place
- There is a statutory power in place
- There is a court order in place

SMS messages on a mobile device are included in the reference to telecommunications service. It is important to note that a person's consent alone would not constitute lawful authority to intercept communications.

In respect of obtaining certain types of electronic evidence from overseas, which is currently very challenging, there is a recent piece of legislation, the Crime (Overseas Production Orders) Act 2019. The Act enables officers of specified investigative agencies to apply to a Crown Court

judge for the production of stored electronic information located or controlled outside the UK for use in the investigation and prosecution of indictable offences (that is, serious offences). This power can only be exercised where a designated international cooperation arrangement exists between the UK Government and the government of the country in question. The Act is intended to address the constraints of existing domestic court orders and the limits of MLA in being able to compel the production of evidence from another jurisdiction and being able to obtain it quickly. According to the UK Government, it takes an average of 12 months for an MLA request sent to the USA, which is where many servers are situated. An application for an OPO must be made to a Crown Court judge by an appropriate officer. The application must state the existing cooperation arrangement with the country in question and specify or describe the electronic data subject to the order. The order does not encompass confidential personal information, except where the offence in question is terrorism. The Crown Court judge must be satisfied that there are reasonable grounds for believing:

- The person who is the subject of the order operates or is based in a country outside the UK which is party to, or participates in, a designated international cooperation agreement
- An investigation has been instituted or proceedings commenced in respect of an indictable offence (or terrorism)
- The person has possession or control of some or all the electronic data
- The electronic data is likely to be of substantial value to the investigation or proceedings
- All or part of the electronic data is likely to be relevant evidence in respect of the offence
- It is in the public interest for all or part of the electronic data to be produced or accessed

Generally, the provisions are specific and detailed but can be largely thought of as reflecting nature of the provisions in the Police and Criminal Evidence Act 1984.

A list of the UK's bilateral mutual legal assistance treaties is published at: https://www.gov.uk/government/publications/bilateral-treaties-on-mutual-legal-assistance-in-criminal-matters

Digital Devices

Of note is that mobile phones or other digital devices are not examined as a matter of course; they should only be examined in investigations where the data on the device could form a reasonable line of enquiry, which police are obliged to carry out. They may also be examined where they are relevant to the case, in that they have a bearing on it, and where content may undermine the prosecution case or assist the defence. There is a legal obligation for the prosecution to disclose such material to the defence.

It has recently been clarified that victims are not obliged to hand over their mobile devices to the police for examination and the NPCC have recently re-issued the relevant consent form for this purpose, which clearly sets out the relevant information. Seeking consent for digital examination applies to all crimes but will only be used where necessary and proportionate. It will most likely be used in investigations where the complainant and suspect are known to each other and past communication is a reasonable line of enquiry. It will also be used in other cases where digital evidence may be crucial, such as malicious communications, stalking and harassment and violent crime including homicides.

When a crime is investigated, police will regularly seize devices of those accused and will seek to obtain information related to a reasonable line of enquiry using this data. This is done using police powers and suspects are not required to consent. Coercive police powers are clearly not appropriate for use against complainants or witnesses and access to their devices should be on the basis of specific, free and informed consent.

There is formal guidance in relation to seizing, examining and extracting data from electronic devices, including mobile phones. In particular, there are four principles that are applied to this area:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied on in court
2. In circumstances where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Subscriber information for e-mail, webmail, voicemail, text message or other internet connection is telecommunications data subject to a RIPA authority.

PACE provides that seized property can be retained for as long as necessary in the circumstances (s22(1)). Any kit seized for the purpose of a criminal investigation can be returned for forensic examination and as an exhibit at trial as long as a copy or photograph of the document or item would not suffice. If the original must be retained until the conclusion of the trial, the police should provide a copy of, or allow access to the item, to the person from whom it was seized.

Under s59(7)(a) of the Criminal Justice and Police Act 2001 an investigator can apply to retain unlawfully seized property to prevent the collapse of a criminal investigation as a consequence of the unlawful seizure of evidence. If investigators were not permitted to retain that which had been obtained by the execution of an unlawful warrant and the seized material was compelling evidence of criminality, the person to whom it was returned may seek to destroy that material if it were returned to them. It is in these specific circumstances that retention may be authorized.

One of the main issues arising from mobile devices is that they have evolved to contain or have access to, such a large amount of personal, confidential and sensitive information that the collateral intrusion when they are used or examined by police is significant. This extends to people connected to the individual who are not subjects in investigations or enquiries. As well as privacy and other fundamental rights, data protection is an important factor and examining mobile devices involves data processing by police, so is subject to the requirements set out in the Data Protection Act 2018, Part 3, which applies to processing personal data for criminal justice purposes. This legislation gives effect to the Law Enforcement Directive 2016/680.

The police powers that provide authority to seize and examine mobile phones is distinct from the data protection law that provides lawful basis for the subsequent data processing that takes place when information is examined, accessed, retrieved or retained, or otherwise processed. This also requires full information to be provided to individuals, including what information is being examined, what the lawful basis is and what their rights are in relation to the information in question.

Digital evidence and communications data can be obtained directly from Communication Service Providers (CSPs) as well as from computers and digital storage devices. Investigators have the power to serve orders on CSPs that oblige them to disclose communications data. Many CSPs are based in the US and may be obtained through MLA or the new orders outlined above.

The particular circumstances of the case may determine whether the offence in question comes within the jurisdiction of England and Wales, an example is the case of *R v Sheppard and Whittle (2010) EWCA Crim 65*, in which the defendant posted racially inflammatory material to a website, registered in his name and operated by him but based in California. Once the material reached the server in California, it was posted online and made available on the internet to all those visiting the website, including people in the jurisdiction of England and Wales. The court came to the conclusion that jurisdiction was governed by the substantial measure principle. Everything in the case related to England and Wales except for the server being in California.

Specific Situations

In relation to **business crime** and investigations, when searching business premises investigators may seize mobile phones if it is considered relevant to the investigation, therefore it depends on the offence in question. However, if the mobile phone is the personal property of an employee, an investigator does not have the power to seize it, as it is not company property. An investigator would need a production order to seek access to information held on a personal mobile.

In relation to company property in this scenario, subscriber information for e-mail, webmail, voicemail, text message or internet connection is telecommunications data subject to the Regulation of Investigatory Powers Act 2000 (RIPA) and therefore needs a specific

authorisation to access this material. where a suspect refuses to disclose a password or decryption key where an order has been obtained, that is an offence under RIPA, subject to a maximum penalty of two years' imprisonment on conviction or maximum five years where the offence alleged is one of child indecency.

General Principles / Requirements

Because of the nature of mobile devices, they have the potential to contain evidence relating to a wide range of criminal offences each one with different points to prove. Therefore, it is difficult to generalize about the powers in relation to their seizure and examination. There is also the overriding consideration that police powers can only be exercised in a way that is proportionate to the aim to be achieved and must use the least intrusive means to achieve that objective.

Also pertaining to the nature of mobile devices is the fact that they commonly and increasingly contain enormous amounts of personal, confidential and sensitive data, so the requirement for seizure and examination to be confined to what is relevant to the case is even more important.

As well as evidence, mobile devices can contain material that is relevant due to it undermining a prosecution case, including rebutting evidence. There has been particular focus on this aspect in recent years as high-profile miscarriages of justice has led to reviews of the police aspect of the criminal justice process.

In relation to the questions about not following procedures I would first point out that the legal and authorized procedures have been developed largely to avoid miscarriages of justice and to create a balance between police powers and fundamental rights, therefore not following them would have far wider implications that simple inadmissibility in court proceedings.

The person dealing with the seizing of digital evidence must follow certain procedures. This will impact on the admissibility of evidence or any legal or misconduct proceedings. Special procedures are in place due to the volatile nature of digital evidence and the increased ability for it to be altered. There are specialist units to support police actions. They are specially

trained and recognized as competent to seize or recover digital evidence in a way that retains its integrity and is acceptable in criminal justice proceedings.

The overriding concept in any criminal justice proceedings in the UK is that of fairness; the criminal justice and court procedure rules are founded on this concept. The court has discretion on the admissibility of evidence but the defence also has the right to challenge it. There also exists the Investigatory Powers Tribunal where legal procedures have not been followed, an important oversight element of the system in the UK.

Another important factor is the model in the UK is policing by consent. Actions outside of proper laws and procedures would negatively impact upon public confidence in both the legitimacy of the police and procedural justice. Evidence will be deemed inadmissible if it undermines the concept of fairness, one reason is if it has been obtained in a way that casts doubt on its integrity or credibility. The question of admissibility is in itself derived from the fundamental right to a fair trial and always to promote public confidence in the criminal justice system and procedural justice.

Criminal Justice Procedures

The Forensic Science Regulator publishes and regularly updates Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System. This includes digital forensic operatives. There are standards and accreditation requirements for most digital forensics. Where activities are excluded from the ISO accreditation requirement, they nevertheless should be conducted by competent staff using approved methods.

Incident scene activity – screening, capture and preservation or analysis of data from a device conducted at scene (included but not limited to routers): **ISO 17020** is relevant standard

Capture and preservation from digital media – creating a copy of the digital data in whole or in part from digital storage media and storing the copy in a manner that allows subsequent processing and analysis to take place in accordance with the relevant validated method being applied. This may be logical or physical: **ISO 17025** is relevant standard

Analysis of data from digital media – process of targeting and / or evaluating digital data via application of a predefined forensic strategy (either on a case by case basis or in a service level agreement). **a)** narrowing / filtering (i.e. findings from validated digital forensics

methods) and comparing them with other types of data e.g. communications data to support reasonable lines of enquiry; **b)** using forensic analysis and technical explanation of the data (using validated forensic methods) to deliver a defined forensic strategy; **c)** expert interpretation of digital forensic findings including but not limited to comparisons and evaluation of the findings as they relate to hypotheses or propositions. Methods shall be validated: **ISO 17025** is relevant standard.

Screening or recovery of data from a device using an off the shelf tool for factual reporting – the use of tools and methods by frontline non-practitioners is permitted but the organization needs to hold accreditation for at least one deployment. Further deployments of the method under central control may be permitted outside the scope of the accreditation provided that the method chosen can be demonstrated to have adequate configuration control (e.g. locked down data recovery methods and control) and that staff are competent: **ISO 17025** is relevant standard.

Network capture and/or analysis – the FSR Code of Practice apply for capture, preservation, processing and/or analysis of traffic data from a digital network. Also, under consideration for ISO 17020.

The Forensic Science Regulator Code of Practice also applies specifically to digital forensics. Individuals reporting scientific or technical work to the courts must declare compliance with FSR standards.

There are also **Criminal Procedure Rules** that are regularly updated, the latest version being 2020. And **Criminal Practice Directions**, which were also updated in May 2020. This set out the rules and regulations that apply to all participants in the criminal justice process and incorporate directions to those presenting evidence as well as cyber forensics expert witnesses, who are frequently engaged in criminal cases.