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: Managing Director, Elias A. Stephanou LLC; Elena Kapardis.

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

Answer: Nicosia, Cyprus.

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: There is no legal definition of a mobile device, there is however a differentiation between landlines and mobile phone in the Regulation of Electronic Communication and Postal Services Law 112 (I)/ 2004, and its secondary legislation and orders, however, without providing a succinct term as to what constitutes a mobile 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:*

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

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

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.*

Answer:

Mobile Device Not Seized: The basic premise on which a mobile device can be searched and read without a search and/or seizure order is through the consent of its possessor/owner. The limitations and content of these have not substantially been tested in the Cypriot courts, however, some preliminary points have been examined. There is no template statement by which a police officer informs an individual, even a potential defendant, of their rights, the ambit of their rights and consequences of their consent. To this end, the absence of a regulated protocol has brought into question, in the case of **Siamisi v Police (2011) 2 CLR 308** the imbalance that can occur in relation to the invasion of one's private life as well as defendants' rights. In this case, the complainant provided to the authorities, with her consent a mobile device, from which the content was made available to the investigative team. The Supreme Court ruled that despite the complainant's consent the investigative authorities had not acquired the consent of the defendant for that reason there was a violation of his constitutional rights. More specifically, a violation of Article 15, right to private and family life and Article 17, right to private communication. The details of these protections will be explored in greater detail in the next section.

As this case reveals there are significant gaps within the collection and processing of mobile devices without a search warrant. Due to the absence of a template statement, it is common, but not imperative, for investigative officers to request consent to read and process a mobile device and then make a record of the event and dicta used in an operations diary. However, it appears evident, from cases pending before the Assize Courts, **XXX Georgiou and Others v Republic** Case (1537/2019), **XXX Papadopoulos v Republic** Case (14015/2019)**,** the police teams are utilising consent to use technical tools to bypass security, make a forensic copy of the device and then read and process the information. The practices of the police authorities are, however, quite haphazard. Depending on the nature of the offence or investigation the police officer, or criminal

investigator, may simply require consent from the owner/possessor of the device to view specific content rather than acquire a forensic copy of the data. During later stages this can be requested or demanded with a warrant. However, it is important to note that without a warrant an individual has the right to refuse to hand over a mobile device, or simply unlock a device.

Similarly, if consent has been improperly achieved then this can result in a reversal of consent in the courtroom, as explained in **Siamisi** (above). Unfortunately, due to the absence of check and balances, of a prescribed procedure, the validity of consent commonly arises during the trial process, through an objection to the submission of the mobile phone as evidence on trial and/or through a trial within a trial (voir dire). This can occur in any criminal offence as consent is neither limited to any category or nature of offences nor to any classification of individual, i.e. witness or defendant. What the case of **Siamisi** has revealed, in conjunction with the rules on data retention, analysed below, what is crucial is that if the content of the mobile device relates to personal data then it is vital to acquire the consent for the access and processing of the said personal data by both data subjects. This can prove more complicated when the data is actually based outside the Cypriot jurisdiction, i.e. on overseas servers or iCloud. However, this does not necessarily make the data unreachable, if there are bilateral agreements for investigation requests, such as the European Investigation Order then police officers make a request for additional information via this route, approved by the Attorney General's Office, with the intention to access and process information (Law 244 (I)/2004, Law 181/2017). The competent authority who executes the EIO is the District Judge whose district the execution of the EIO is sought, in conjunction with the Attorney General, the Chief of Police, the Director of the Customs and Excise Department and the Tax Commissioner.

An additional scenario wherein a mobile phone may be seized without a warrant is provided in Article 25 of Criminal Procedure CAP155. This states that a police officer may enter upon a search whom he reasonably suspects of carrying, conveying or concealing any article or document in respect of which any offence is about to be committed or is being committed or has recently been committed. With certain preconditions relating to the entering and search of a place, without a warrant, the basic argument of this process is that an officer may seize said property and treat it as

if it were seized under warrant, as will be analysed below. Of course, after the seizure of the mobile device, the content of the mobile device can be only examined in pursuant to a court order.

A key point to note at this point is what can be accessed in relation to the contents of the mobile device. This issue is not differentiated between the scenario of a mobile device seized with the consent of the proprietor or via warrant. According to Article 17 (2) of the Constitution the communication content of a mobile device can only be made available on the basis of certain offences, namely (a) in the case of convicted or unconvicted prisoners (b) By a Court Order issued pursuant to the provisions of a law on the application of the Attorney General of the Republic and if the interference is a measure which in a democratic society is necessary only for the purposes of the security of the Republic or for the prevention, detection or prosecution of:

- Premeditated murder or manslaughter
- Trafficking of people (whether children or adults) and offences relating to child pornography
- Supply, trading, cultivation or production of narcotics or other psychotomimetic or dangers drugs
- Offences relating to the currency of the Republic
- Corruption offences for which on conviction the sentence provided is five year imprisonment or more

By a Court Order issued pursuant to the provisions of a law for the purpose of detection and prosecution of serious crimes for which the sentence provided in the event of conviction is five or more years imprisonment and when the interference relates to the traffic data and location data and relevant data required to identify the subscriber or the user. This restricts access to material such as call list register, messaging, messaging apps, internet browsing history, access)To this end all

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

other material is eligible for access via consent (this is inclusive of inter alia photos, videos, contact list) and is not in contravention with an individual's constitutional rights.

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?*

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?*

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

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.*

Mobile Device Seized:

A significant starting point for investigating the theory and practice that surrounds the seizing of mobile phones with a warrant is found in the Criminal Procedure CAP 155.

Art. 10 (1) of CAP 155 stipulates that when a person is arrested, the police officer who makes the arrest can utilise his/her discretion to seize any object or paper which the arrested person was in possession of when arrested- if this property is considered to be substantial evidence against the person arrested. This provision complements, Art 25 mentioned above. It provides a check and balance for the request and seizure of property, inclusive of mobile phones. (i.e. **Police v Jan Catalin Gindac, Criminal Appeal** 8960/17, dated 8/11/2017)

Additionally, the specific procedure for the acquisition of a warrant are set out in Art. 27 of CAP 155 (also detailed in **Psaras and Another v Republic** (1987) 2 CLR 132) . Where an investigator seeks to acquire a search warrant, through which to seize property, then this occurs through the transmission of an affidavit from the investigator stipulating anything in respect of the offence, the reasonable grounds believed to afford evidence and reasonable grounds for believing it is intended to be used. Additionally, it is required to bring before the Judge, upon execution of the warrant, anything that has been seized as part of the warrant. (Art 27 (c)).

Additionally, Law 183 (I)/ 2007 also provides for the acquisition of data relating to serious crimes, which could include mobile phones, and/or data arising from said devices. A "serious crime" is described as an offence that is punishable with a sentence of over 5 years of imprisonment or is stipulated specifically in this law. Article 4 of Law 183(I)/2007 sets out that a police investigator can, in the case of a person's abduction, the police investigator can send a letter to the network service provider and secure the data relating to the ongoing investigation, as long as this is done

with the Attorney General's permission. If in the period of 48 hours following such permission provided the police investigator applies for the Courts permission and is refused it, then the investigator must destroy all evidence obtained.

Article 4(2) specifies that the Attorney General can if the police investigator is investigating a serious crime, as outlined, give his permission for the request of a seizing warrant from the court. This is done using an affidavit by the investigator which lays out in full disclosure the facts and circumstances which the investigation is basing the request: these include the time period, the suspect's identity, name, address and occupation (if these are available), why there is reasonable concern that the person has committed the crime and why it is essential.

Article 4(4)- clarifies that the Judge will provide the order if there is reasonable suspicion or chance, that the person committed, will commit, or is expected to commit the crime, and that certain data are connected with the serious crime, or in conjunction with it.

On both aforementioned grounds, it is possible to search and read data included on devices. However, there are exceptions that have been evidenced through Constitutional protection, such as if data relates also to another data subject, their permission must also be acquired (**Siamisi** (above)). An additional situation is in the event that the data included relates to personal data and is thus governed by the EU Directive 2006/24/EC on Data Retention. Unfortunately, the precise impact of this Directive- specifically, in relation to time limits of access to data held by communications providers (guided by **Tele2Sverige** decision) is still undecided, with 8 appeals pending before the Supreme Court.

More generally, it is common practice for investigators to make a forensic copy of mobile device, if a warrant has been acquired by the owner/possessor of device. In doing so the police do use technical tools to bypass security. Additionally, there is no prescribed obligation to inform the owner that the device has been seized, the only obligation is to declare it as seized evidence before the Court. If, cooperation is required in relation to the detection of a server or data is located abroad this is achieved in the same way as in the previous scenario.

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

***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: No protocol is observed in court. In the case of **Penderhill Holding Limited ao v Ioannis Kloukinas**, Civil Appeal319/11 and 320/11, the Supreme Court simply stated the courts must be appropriately responsive to the technical changes in the area of digital evidence and forensics. In practice, because the authorities are not able to make replica forensic copies of a mobile device on another exact mobile device a forensic clone is made with a digital file analysis and retrievability. More specifically, the experts reproduce the device and its data with a software that is the 'copy' of the device for investigation and court processes. This reproduction occurs on the basis on internal police authority protocols that are not publicly available or accessible.

***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: This issue is not regulated or standardized in Cypriot courts.

***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: The main cases relating to mobile devices have already been cited.

***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: No standard other than guidance issued by European Judicial Network

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: Cyprus has commonly utilized EIO rather than MLAT for mobile device data, however, due to unofficial statistics meaningful response is difficult.

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

Answer: Depending on the difficulty of the case and the expertise needed, it is not uncommon for the Police to seek the expertise of the private sector. This is the case in very difficult cases such us the last case of mass interception of communication. Moreover, experts from private sector are called as witnesses in criminal cases. However, there is no existing cooperation mechanisms and official practices with the private sector.

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.

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

Answer: As mentioned above one of the key concerns at present relates to the proportionality and constitutional character of device access and processing in conjunction with balancing of Art 15, private life and Art 17, secrecy of communication, in pending appeals before Supreme Court full bench. Additionally, the scene has further complicated with the second case in the ECJ, **Ministerio Fiscal** C-2018/788, which added onto the possibilities wherein access can be achieved, not only in serious cases, but also in instances of detection, investigation and prevention of crime. With an additional case pending decision before the European Courts, it is unlikely that the Cypriot courts will proceed with judgments before that. Thus, it is evident that there is no clear legislative framework or case law development that can shed a direct light on the ability of the police to acquire, process and utilize said data. Similarly, there is also limited understanding in relation to the limits and checks and balances to this data. Influential, however, have been cases relating to other devices, such as computers and personal computers. In the certiorari appeal, before the Supreme Court, the case of **Petros Evdokas** (51/2017) it was decided that a guiding principle in the retrieval of data from a computer that although there was no prohibition from the police authorities to acquire data and then decide if said data was vital at a later stage in this particular case because the data relates to a specific nature of data- access to a publication made to a specific website, this meant that a proportionality test should be in force by the Courts. There are conflicting rights in these instances, the right to a private life of an individual and public order/ social good. In that case the first instance court had infringed article 8 of the Convention on Human Rights as well as the concept of proportionality. To this end, some guidance is available in the daily investigative practices of the police and the discretion of the Courts but future decisions will enlighten better and more precise practices.

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: No specific rules in relation to data evidence or forensic analysis.

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: Yes, the criteria for admissibility of evidence collected through mobile forensics the same as for the other types evidence, i.e. the judge must be satisfied through an expert testimony that the information detracted and presented to Court are those which in fact been in the mobile device.

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: If the evidential rules are not followed and the authenticity of the evidence produced to Court is not proved, then the evidence is not taken into account by the court.

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: The issue of jurisdiction can be ameliorated by requesting data officers from other countries to present evidence in court trials in Cyprus. It is not a matter of admissibility of the evidence. However, if there is any doubt as to the authenticity and truth of the evidence, the Court will not take into account this piece of evidence in its decision.

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

***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: Although there is no standard for the presentation of evidence, forensic experts presenting evidence, either on the part of the police or as experts refer to the principles of auditability, justifiability, reputability and reproducibility. The alteration of evidence, limits the authenticity of the evidence, limits the best evidence available and is thus less likely to be accepted in terms of relevance and reliability (Metaquotes Software Ltd v Dababou, Civil Appeal E324/2016, 14 November 2018).

***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: No specific rules exist, but it's a matter of judicial application the evidential best evidence rule.

***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: N/A

***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: No recognized standard

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

***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: The issue may be questioned through an objection pending trial or through reviews to the Data Commission officer. The Court, following the decision **Parris** (1999) 2 CLR 186 will balance the violation of Data Protection Law on one hand and the need for admitting the evidence in the interest of justice, on the other, deciding whether to accept or not the specific evidence.

***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:

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: No standardization of practices

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

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: N/A

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: N/A

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: N/A

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: N/A

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: Not yet but there is a potential course for forthcoming and current judges as part of the newly established judge school.

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: No standardised period.

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: The rights provided for all individuals in a court, are prescribed in the constitution. The Constitution does not provide for specific rights for different members of the Court process, however, the right to a fair trial guaranteed under Article 30 of the Cypriot Constitution is very much centered around the rights of the defendant. Inclusive of the rights mentioned is a fair and public hearing within a reasonable time by an independent, impartial and competent court established by law.

In the determination of his civil rights and obligations or of any criminal
charge against him, every person is entitled to a fair and public hearing within

a reasonable time by an independent, impartial and competent court. This has come under attack with the delay which is observed throughout the Cypriot court system, especially after the 2013 economic crisis. Additionally further rights are enshrined in Article 30 as follows: every person has the right
(a) to be informed of the reasons why he is required to appear before the court;
(b) to present his case before the court and to have sufficient time necessary for its preparation;
(c) to adduce or cause to be adduced his evidence and to examine witnesses according to law;
(d) to have a lawyer of his own choice and to have free legal assistance where the interests of justice so require and as provided by law;
(e) to have free assistance of an interpreter if he cannot understand or speak the language used in court.

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: No guidance provided

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: No approaches or methods assigned.

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: The admissibility of mobile forensics is at the discretion of the court, treating the evidence presented as falling under the general category of evidence presented by an expert witness (**Republic v Kittis ao** 693/14)

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

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: The defendant is entitled to all the evidence obtained as part of the case file, as stipulated in Art 7 of Criminal Procedure CAP| 155. This does not relate to additional information on how the tools work or procedures used, but are customarily made either in expert's report, usually provided as part of case file, or provided in in-court testimony of forensic expert. Again, due to the absence of standardized guidelines the validity is left to the Courts.

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:

The answer to this question is unclear and there is no legislative guidance on this issue. However, it can be drawn on the previous answers, that any information which does not relate to the contested issues in the question, and the strict approach taken by the Court in the case of **Siamisi** and **Georghiades**, that any information obtain which can be deemed as a breach of privacy, will not be permitted.

Also, the particular requirements for witnesses regarding their ability to testify, according to the general approach taken by the Supreme Court in the case of **Kayat Trading Limited v Genzyme Corporation** (No.1) (2013) 1(A) CLR 438 that the witness's criteria in providing evidence are based on the knowledge of that person surrounding the concerned issue, if that person is a specialist in that area.

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:

There is no legislative or case law guidance on the issue,

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.