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?*

Dr. TJ McIntyre, Associate Professor, Sutherland School of Law, University College Dublin.

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

Ireland

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)*

No. Irish law generally refers to "computers", a term wide enough to include mobile devices generally. Some legislation defines that term to specifically include mobile devices. For example, section 133 of the Finance Act 2001 (as amended) permits searches of computers, defined as follows: "'computer' means any electronic device used for information storage or retrieval and includes a mobile phone or any other electronic means of information storage or retrieval".

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?*

Consent

A mobile device can be read or searched without use of statutory powers of seizure with the consent of the owner. See (by analogy) *People DPP v. Eugene Kelly*[1] where evidence of phone calls and text messages on a phone taken from a person on arrest was admitted in evidence on the basis that the accused had consented to a search of his device by handing it over and failing to object to a search.

Examination as part of search

Where a search warrant is being executed a mobile device may be examined to see whether it falls within the scope of the warrant. This is outlined further in the answer to question 17 below.

Remote searches

Irish law permits remote searches of computers in some circumstances. For example, search warrants under section 7 of the Criminal Justice (Offences Relating to Information Systems) Act

[1] [2012] IECCA 71

2017 permit a member of An Garda Síochána (police officer) to "operate any computer at the place that is being searched".[2] However the section goes on to define "computer at the place that is being searched" to include "any other computer, *whether at the place being searched or at any other place*, which is lawfully accessible by means of that computer".[3] On the face of it, this permits "remote searches" or "network searches", including searches of devices which are in some way linked to the computer at the place being searched. In theory this could permit access to information stored on a mobile device where that information could be accessed through the computer which is being seized. However there is no evidence that I am aware of that this power has been used in this way. This power is more significant if a mobile device is seized, when it could be used to access remotely held information, and I will come back to it in that context later in this report.

Malware

Irish law does not expressly regulate the use of remote access malware ("government trojans"). In theory such malware might be permitted as a type of "surveillance device" regulated by the Criminal Justice (Surveillance) Act 2009; however, that Act refers to "surveillance devices" as an "apparatus" which appears to envisage a physical device only rather than software. In addition. section 2(3) of that Act precludes the use of surveillance devices in a way which would constitute an "interception" of communications,[4] which would seem to rule out most uses of malware against phones. I am not aware of any evidence that malware has been used in this way in Ireland and I will not consider it further for the purposes of this questionnaire.

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?*

[2] Criminal Justice (Offences Relating to Information Systems) Act 2017, s 7(4)(a).
[3] Section 7(9). Emphasis added.
[4] Which is regulated by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

There is no legislation or caselaw directly on this point. Where a search takes place on the basis of consent then in principle the boundaries of the search would be the limits of the consent together with the general rules under the Law Enforcement Directive (as implemented in Irish law by the Data Protection Act 2018), in particular that data is collected for specific, explicit and legitimate purposes, and is not excessive for those purposes. The limits to searches of seized devices are considered further below.

6. *Is it allowed to use technical tools to bypass security?*

Where a search is carried out on the basis of consent then it will depend on the nature of the consent as to whether technical tools could be used (assuming technical tools are necessary – if an individual consents then presumably they can unlock the device); failure to obtain consent would mean that the use of technical tools may constitute the offence of accessing an information system without lawful authority or reasonable excuse contrary to section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017. However, there is no caselaw on this point. The use of technical tools in the context of a compulsory seizure is discussed further below.

7. *Can information be copied or only read at this stage?*

There is no legislation or caselaw directly on this point. Again, this would depend in principle on the nature of the consent given by the owner. If a person were to give access to their device on a view only basis and a forensic image was taken without consent, that would not constitute the offence of accessing an information system without lawful authority or reasonable excuse,[5] as it would not involve "infringing a security measure", but it may mean that the data was not processed fairly within the meaning of the Law Enforcement Directive and may mean that the forensic image would not be admissible in evidence.

[5] Contrary to section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017.

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

8. *Is consent of the owner/person in possession of the mobile device necessary?*

In practice search by consent is the only way in which Irish police appear to examine mobile devices without seizure. There does not appear to be any caselaw on the question of *who* is entitled to consent; for example, where a person in possession of a phone is not the owner.

9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*

Where a search takes place on the basis of consent then unlocking can only take place on the basis of consent. Where a search warrant is in place then a person may in some cases be required to provide a password and this point is considered further below.

10. *Must the owner/person in possession of the mobile device be informed?*

Where a search takes place on the basis of consent then the person giving the consent must be aware of the search in order to consent. There is no requirement in law for notification of remote searches to the owner/person in possession of the remote device.

11. *Who can order a search and what are the formal requirements, if any?*

The power to search by consent does not have any statutory basis and as such does not have any formal requirements or rules regarding who may authorise such a search. In principle any member of the police force might carry out such a search without further authorisation.

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

The power to search by consent does not depend on the identity of the owner of the item being searched.

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.*

In practice police sometimes ask individuals to consent to their accessing information notwithstanding that this information is stored abroad. The issue does not appear to have been considered in detail, but there have been cases in which the courts appear to have accepted the practice. For example, in *People (DPP) v William Moran*[6] police accessed messages on a person's Facebook account with their permission, and the Court of Appeal did not disapprove of the practice. There do not appear to be any cases discussing the jurisdictional issues this might present.

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

Where searches are carried out on the basis of consent then the type of crime involved will not matter, save to the extent that the nature of the crime may affect the proportionality of the collection of data under the general rules of the Law Enforcement Directive and the Data Protection Act 2018.

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.*

[6] [2018] IECA 176.

The general rule for all the scenarios described throughout this questionnaire is that the admissibility of any evidence obtained improperly will depend on whether the evidence is found to be unconstitutionally obtained or merely illegally obtained.

The leading case in this area is *DPP v. JC*[7] in which the Supreme Court restated (and to a significant extent narrowed) the exclusionary rule in Irish law.[8] In the case of *illegality*, the Supreme Court confirmed that the trial judge has a discretion whether to exclude illegally obtained evidence, and in exercising that discretion the trial judge must bear in mind that:

> [E]vidence obtained illegally is also a matter with which the courts should be significantly concerned […] there is also an obligation on the courts to uphold the law and to discourage illegality. It should not, therefore, be taken that evidence obtained in circumstances of illegality should readily be admitted. Where the absence of legality arises in circumstances properly described as reckless or grossly negligent, then the relevant evidence should be excluded even if the illegality concerned does not result in a breach of constitutional rights.[9]

In the case of evidence obtained *in breach of constitutional rights*, the Supreme Court distinguishes between "deliberate and conscious" breaches and other violations. In the case of deliberate and conscious breaches then evidence obtained as a result *must* be excluded unless there are exceptional circumstances (such as the need to rescue a victim in peril). However, in the case of other violations, there is merely a *presumption* that evidence should be excluded and evidence may be admitted if the unconstitutionality was merely inadvertent. The Supreme Court has provided an authoritative statement of these rules in the following passage:

> Where evidence is taken in deliberate and conscious violation of constitutional rights then the evidence should be excluded save in those exceptional circumstances considered in the existing jurisprudence. In this context

[7] [2015] IESC 31.
[8] See Yvonne Marie Daly, 'Overruling the Protectionist Exclusionary Rule: DPP v JC', *The International Journal of Evidence & Proof* 19, no. 4 (1 October 2015): 270–80, https://doi.org/10.1177/1365712715601764.
[9] Judgment of Clarke CJ, paras. 6.1-6.2

deliberate and conscious refers to knowledge of the unconstitutionality of the taking of the relevant evidence rather than applying to the acts concerned. The assessment as to whether evidence was taken in deliberate and conscious violation of constitutional rights requires an analysis of the conduct or state of mind not only of the individual who actually gathered the evidence concerned but also any other senior official or officials within the investigating or enforcement authority concerned who is involved either in that decision or in decisions of that type generally or in putting in place policies concerning evidence gathering of the type concerned.

Where evidence is taken in circumstances of unconstitutionality but where the prosecution establishes that same was not conscious and deliberate in the sense previously appearing, then a presumption against the admission of the relevant evidence arises. Such evidence should be admitted where the prosecution establishes that the evidence was obtained in circumstances where any breach of rights was due to inadvertence or derives from subsequent legal developments.

Evidence which is obtained or gathered in circumstances where same could not have been constitutionally obtained or gathered should not be admitted even if those involved in the relevant evidence gathering were unaware due to inadvertence of the absence of authority.[10]

These principles have been applied to computer data in some cases in a civil law context. See for example *P. v. Q.*[11] – where a husband illegally accessed his wife's laptop and codes/password for her website accounts, the evidence acquired as a result was inadmissible in the main family proceedings (but was allowed to be admitted for the limited purpose of safeguarding the welfare of the children). While that is a civil law case, the same rules of admissibility would apply in a criminal law context also.

Mobile device seized

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

[10] Judgment of Clarke CJ, para. 7.2.
[11] [2012] IEHC 593.

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

Mobile devices can be seized in the same way as other forms of evidence; there are no special rules of law which apply to them.

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

Irish law has a range of powers regarding search and seizure of evidence including mobile devices. Unfortunately, these powers are not consolidated but are found "in a mixture of pre- and post-independence statutes and at common law".[12] As Walsh puts it: "current statutory powers to issue search warrants constitute an unwieldy collection of disparate provisions which have been developed in a piecemeal fashion over the past two centuries. Each authorises the issue of a search warrant only when its own peculiar requirements have been satisfied".[13] None of these search warrant powers has special rules regarding mobile devices, though some of the more modern powers do have specific rules regarding computers and encryption.

Search warrant powers therefore vary significantly depending on the type of crime being investigated, with differences regarding matters such as:

- Who can *apply* for a search warrant;
- Who can *grant* a search warrant (judge or peace commissioner);
- The *evidential criteria* to be met for the grant of a warrant;
- How *significant* material must be to an investigation in order to be seized;
- Whether a person executing a warrant can require *disclosure of a password* necessary to operate a computer; and

[12] Maeve McDonagh and Micheal O'Dowd, *Cyber Law in Ireland* (Alphen aan den Rijn, The Netherlands: Wolters Kluwer Law & Business, 2015), 384.
[13] Dermot Walsh, *Criminal Procedure* (Thomson Round Hall, 2002), paras 8–09.

- Whether a person executing a warrant can require that information be provided *in decrypted form*.[14]

In addition, there are separate powers regarding search and seizure incident to arrest.[15]

An example of a modern search warrant power is section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017, which applies to certain cybercrime offences. I have set it out below along with my annotations in italics, and will use this section as an example when answering subsequent questions. Note, however, that this section is limited to offences under the 2017 Act ("relevant offences") – it does not create a warrant power for other offences. Search warrant powers for other offences, such as offences against the person, will often be more limited and may lack elements such as a power to require passwords/decryption or the power to copy documents.

> 7. (1) If a judge of the District Court is satisfied by information on oath of a member that there are reasonable grounds for suspecting that evidence of, or relating to, the commission of a relevant offence is to be found in any place, the judge may issue a warrant for the search of that place and any persons found at that place.
>
> [*This, as with most warrants, is issued by a District Court judge on the basis of an application made by a member of the police force. Note that the warrant is territorial – it applies to a physical place and persons at that place at the time of the search. The standard for the warrant is reasonable grounds for suspicion that evidence is to be found at a particular place.*]
>
> (2) A search warrant under this section shall be expressed, and shall operate, to authorise a named member, accompanied by such other members or persons or both as the member thinks necessary—

[14] For a general discussion of these differences see Law Reform Commission, 'Report on Search Warrants and Bench Warrants' (Dublin, 2015), chap. 3, http://www.lawreform.ie/_fileupload/Reports/Report%20on%20Search%20Warrants%20and%20Bench%20Warrants%201%20December%202015%20-%20Final%20Version.pdf.

[15] Professor Dermot Walsh, *Walsh on Criminal Procedure*, 2nd ed. (Dublin, Ireland: Round Hall, 2016), para. 4.139-4.147.

[*This "accompanied by" formula permits members of the police force to be accompanied by technical experts.*]

(a) to enter, at any time within one week of the date of issue of the warrant, on production if so requested of the warrant, and if necessary by the use of reasonable force, the place named in the warrant,

(b) to search it and any persons found at that place, and

(c) to examine, seize and retain anything found at that place, or anything found in possession of a person present at that place at the time of the search, that that member reasonably believes to be evidence of, or relating to, the commission of a relevant offence.

[*This creates a wide power to examine and seize items, including mobile devices carried by individuals, which are reasonably believed to be evidence of or to relate to the commission of the offence. In some cases this may mean that a mobile device is examined but not in fact seized.*]

(3) The authority conferred by subsection (2)(c) to seize and retain anything includes, in the case of a document or record, authority—

(a) to make and retain a copy of the document or record, and

(b) where necessary, to seize and, for long as is necessary, retain any computer in which any record is kept.

[*This explicitly permits seizure, copying, or both in relation to information held on computers including mobile devices*.]

(4) A member acting under the authority of a search warrant under this section may—

(a) operate any computer at the place that is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and

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

(b) require any person at that place who appears to the member to have lawful access to the information in any such computer—

(i) to give to the member any password necessary to operate it and any encryption key or code necessary to unencrypt the information accessible by the computer,

(ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible, or

(iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.

[*This permits police to require either the disclosure of a password/encryption key, access to information, or production of the information itself, for the purpose of both examination and seizure of information. This would be wide enough to include unlocking a device through use of biometrics. Note however that this requirement is limited to "a person at that place" – i.e. a person who is present at the time of a search. Irish law does not have any general rule requiring a person to decrypt or provide a password in relation to data. It is as yet unclear how this type of provision might interact with the constitutional privilege against self-incrimination and there appears to be no caselaw on this point. In practice prosecutions for withholding passwords are not being brought because of this uncertainty*.]

(5) A member acting under the authority of a search warrant under this section may, for the purpose of investigating the commission of a relevant offence, require any person at the place to which the search warrant relates to—

(a) give to the member his or her name and address, and

(b) provide such information to the member as he or she may reasonably require.

[*This could include disclosure of information other than a password – for example, information as to where particular files are located or how to operate a particular application*.]

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

[…]

(9) In this section—

"computer" includes a personal organiser or any other electronic means of information storage and retrieval;

[*Expressly including mobile devices*.]

"computer at the place that is being searched" includes any other computer, whether at the place being searched or at any other place, which is lawfully accessible by means of that computer […]

[*As already mentioned, the "at any other place" provision will permit some remote searches, subject to comity issues*.]

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?*

I will address questions 18 and 19 together.

The starting point is that mobile devices can be examined and seized in the same way as any other form of evidence.

Legal privilege

In general, the only restriction on searches and seizures is in relation to items which would be protected by legal privilege and the usual formula in Irish legislation is to specify that such items may not be seized or retained on foot of a search warrant. For example, section 48 of the Criminal Justice (Theft and Fraud Offences) Act 2001 provides that:

> Where a member of the Garda Síochána has entered premises in the execution of a warrant issued under this section, he may seize and retain any material, *other than items subject to legal privilege*, which is likely to be of substantial value (whether by itself or together with other material) to the investigation for the purpose of which the warrant was issued.[16]

This has presented problems where computers or telephones have been seized as there is typically no mechanism in the legislation creating the search power to resolve disputes as to whether particularly files are legally privileged or to differentiate between privileged and non-privileged files, leaving police to create an ad hoc process to deal with cases where it is claimed that privileged material has been seized.[17]

Limits defined by the warrant

Aside from the area of legal privilege, the usual formula in search warrant powers is that items may be examined or seized if they are "reasonably believe[d] to be evidence of, or relating to, the commission of a relevant offence".[18] This limits the scope of the search by reference to the warrant: as Walsh puts it, "if a member was acting under a warrant to search for a stolen piano and proceeded to look under cushions and mattresses in a dwelling house, it can be argued that he has gone beyond the scope of his power".[19] This is, however, a weak restriction in the case of devices such as mobile phones or computers which, because of their central role in daily life and the information they automatically log, can be argued to be relevant in almost all cases.

Privacy limits

Search warrant powers do not provide any restrictions on the examination or seizure of items on the basis of privacy or confidentiality. Until recently, therefore, it seemed to be assumed that

[16] Emphasis added.
[17] See e.g. *Hussain v. Commissioner of an Garda Síochána* [2016] IEHC 612.
[18] Section 7(2)(c) of the Criminal Justice (Offences Relating to Information Systems) Act 2017.
[19] Walsh, *Walsh on Criminal Procedure*, para. 10.205.

devices appearing to contain relevant evidence could be seized, forensically imaged and searched on foot of a search warrant without any regard to considerations of privacy and the leading Irish texts in this area do not address the point at all.[20]

However a recent Supreme Court judgment, *CRH PLC, Irish Cement Limited and Séamus Lynch v The Competition and Consumer Protection Commission*,[21] casts some doubt on this position. That case involved a competition law investigation in which the Competition and Consumer Protection Commission (CCPC) carried out a "dawn raid" on a firm, seizing data including, *inter alia*, the entire email account of a former executive. The Supreme Court accepted that the seizure of an entre email account raised very profound privacy issues and found that the seizure of the account went beyond the scope of the warrant, noting in particular that the entire email account was seized without "any relevant dates […], target search terms or some other means of limiting the material proportionately to what needed to be taken".[22] It granted an injunction restricting the CCPC from taking action in relation to the email account without first agreeing a process with the plaintiffs to sift out the irrelevant material.

The effect of this case are as yet still unclear. On the one hand the judgment of Charleton J. stressed that different considerations will apply in the context of "traditional crimes" such as serious crime or terrorism and appears to endorse seizures of all data on mobile phones and computers in those cases:

> The problem which emerges is due to the scope of the seizure which the Commission decided to effect and the absence of justification. This may be a part of the uneasy intersection of the investigation of traditional crimes, such as drug dealing or murder, with crimes which of their nature tend to be evidenced not by physical items but by electronic communications. A police officer entering a home occupied by

[20] Rebecca Coen, *Garda Powers: Law and Practice* (Dublin, Ireland: Clarus Press Ltd, 2014); Walsh, *Walsh on Criminal Procedure*.
[21] [2017] IESC 34.
[22] Judgment of Charleton J., para. 30.

> a suspected drug dealer will immediately see what is relevant; the scales, the powder, the paraphernalia of dealing, the wads of cash. The intrusion involved in walking into a home is justified. The breach of privacy in seizing a mobile phone is necessitated by the search. Possibly, as well, it may be necessary to copy a computer hard drive. A police officer investigating terrorism may need to scope the seizure of electronic communications widely because a pattern needs to be established. In those cases, there will be a reason for the search and its ambit and there will be judicial oversight in the issuance of the relevant warrant. Hence, such actions may be amply justified. Here, the problem is in the seizure of an entire email account of many thousands of communications without justification for such an ample and undifferentiated seizure. Nor does the context necessarily, as in the examples just given, provide that justification.[23]

Against that, however, the logic of the decision – particularly in finding that the CCPC should have used keywords and date ranges to limit the data seized, and by treating searches of seized data as being a further infringement of the right to privacy – suggests that a similar challenge might be successfully made in future where the entire contents of a mobile device are searched without, for example, limitation by date range.

Evidence relating to other offences

Irish law provides a very permissive power for police, while executing any search warrant or other search power, to seize and retain anything that they believe to be evidence of *any* offence or suspected offence, regardless of whether there is any connection between the basis for the search and the other offence.[24] Consequently, if a mobile device is examined and it is found to contain information relating to a completely different crime then that device can be seized and used in a prosecution for that other crime.

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

[23] Para. 30.
[24] Section 9 of the Criminal Law Act 1976. See Coen, *Garda Powers*, 316–17.

As outlined in the answer to question 4 above, police may examine a device by consent without the need for a search warrant or other legal power.

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

Some statutory search powers do require individuals to unlock devices. See e.g. section 7(4) of the Criminal Justice (Offences Relating to Information Systems) Act 2017, discussed in the answer to question 14 above, which allows members of the police force executing a search warrant to require a person at the place being searched to provide password be provided or enable access to information on a device. However these provisions are the exception rather than the rule – for example, there is no general power to require a person to unlock a mobile phone which was seized on their arrest.

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

It is a general rule of Irish law that a police officer who is carrying out a search of a person without their consent must inform the person of the legal justification for doing so. See e.g. *People (DPP) v McFadden*.[25]

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

[25] [2003] 2 IR 105.s

There is no legislation or caselaw specifically on this point. However in *DPP v. Moran*[26] the Court of Appeal held that it was permissible to access a SIM card using a PUK code obtained from the mobile operator, holding that:

> It is the Court's view that the PUK (Personal Unlocking Key) which is a security feature on most mobile phones protecting SIM card data and is unique to each SIM card, may indeed be regarded as like a key to a house. When the Gardaí are entitled to enter a house by virtue of a search warrant, it matters not from where the house key comes.[27]

There is an argument that the use of technical tools may be permissible by analogy.

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

Generally not. Most statutory powers to issue search warrants are available as against third parties as well as those suspected of crime. As Walsh notes:

> it used to be the case that search warrants were confined essentially to suspects and proposed respondents in an investigation. Increasingly, however, legislation conferring a power to issue warrants is relating that power to the status of the material or the information being sought, rather than the status of the owner or occupier of the place or thing to be searched. This could encompass the use of warrants for the search of the premises of innocent third parties, including the offices of a solicitor, accountant, doctor, etc.[28]

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] [2018] IECA 176.
[27] Para 44.
[28] Walsh, *Walsh on Criminal Procedure*, para. 10.60.

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?*

I will address questions 25-27 together.

Remote searches

As already mentioned in the answer to question 4, some search warrant powers appear to permit access to data held on computers outside the State where it is accessible by means of a computer at the place being searched. Consider, for example, section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017. Search warrants under this section permit a member of An Garda Síochána to "operate any computer at the place that is being searched".[29] However the section defines "computer at the place that is being searched" to include "any other computer, *whether at the place being searched or at any other place*, which is lawfully accessible by means of that computer".[30] On the face of it, this permits "remote searches" or "network searches", including searches of computers located in other jurisdictions. It would, for example, seem to permit access to webmail hosted abroad where a device at the place being searched is logged in to that service, or access to Twitter DMs if a mobile phone had a Twitter client installed. However this does not appear to be an intended result of this provision and it presents difficult issues, particularly where such searches would not be permitted in those other jurisdictions. There does not seem to be any publicly available information as to whether and how this power is used in this way in practice, though the former Garda Computer Crime Investigation Unit indicated in 2017 that it does not carry out remote forensic examinations[31]

[29] Criminal Justice (Offences Relating to Information Systems) Act 2017, s 7(4)(a).
[30] Section 7(9). Emphasis added.
[31] Council of the European Union, 'Evaluation Report on the Seventh Round of Mutual Evaluations "The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime" - Report on Ireland', 2 May 2017, 73, http://data.consilium.europa.eu/doc/document/ST-7160-2017-REV-1-DCL-1/en/pdf.

International cooperation

Ireland has not opted-into the European Investigation Order and relies primarily on mutual legal assistance requests and the voluntary cooperation of service providers for access to data stored in the cloud. Service providers generally limit cooperation to non-content data – see e.g. the report of the Data Protection Commissioner into the 2011/2012 Audit of Facebook Ireland.[32]

Mutual legal assistance requests

The Criminal Justice (Mutual Assistance) Act 2008 provides the legal framework for access by Irish police to data held by foreign providers. The most important provisions are sections 62 and 73, which respectively provide for taking of evidence from a person in a designated state and searching for evidence at a place in a designated state. In each case, a request may be made in any criminal investigations or criminal proceedings, by either a judge or the Director of Public Prosecutions, and the letter of request to the Central Authority is required to set out:

- a statement that the evidence is required for the purpose of criminal proceedings or a criminal investigation,
- a brief description of the conduct constituting the offence concerned, and
- any other available information that may assist the appropriate authority in complying with the request.

When evidence is obtained under these sections, it may not be used for any purpose other than that permitted by the relevant international instrument or specified in the letter of request without the consent of the appropriate authority in the designated state. When the evidence is no longer required for that purpose (or for any other purpose for which such consent has been obtained), it must be returned to the appropriate authority unless the authority indicates that it need not be returned.

[32] Data Protection Commissioner, 'Facebook Ireland Report of Audit' (Portarlington, 21 December 2011), 98–100, Appendix 5, https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf; Data Protection Commissioner, 'Facebook Ireland Ltd Report of Re-Audit' (Portarlington, 21 September 2012), 34–36, https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.

Under both sections, there are provisions establishing the admissibility of evidence obtained through a request. Section 62 provides that:

> A statement of the evidence of a witness
>
> (a) taken in accordance with a letter of request, and
>
> (b) certified by or on behalf of the court, tribunal or authority by which it was taken to be an accurate statement of the evidence,
>
> is admissible, without further proof, in proceedings relating to the offence concerned as evidence of any fact stated therein of which oral evidence would be so admissible.

Similarly, section 73 provides that:

> In any proceedings relating to the offence
>
> (a) evidence (other than documentary evidence) which purports—
>
> (i) to have been obtained as a result of a request under this section, and
>
> (ii) to be certified by or on behalf of the appropriate authority to be such evidence,
>
> is admissible without further proof, and
>
> (b) documentary evidence which purports—
>
> (i) to have been so obtained, and
>
> (ii) to be so certified,
>
> is admissible, without further proof, as evidence of any fact stated in it of which oral evidence would be admissible.

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.)?*

I will address questions 28 and 29 together.

Service provider in Ireland

Where a service provider is based in Ireland then data can be accessed through either a search warrant or a production order. (A production order is a court order, akin to a search warrant, which requires an entity to produce documents or provide information in relation to the investigation of an offence. See e.g. section 15 of the Criminal Justice Act 2011.)

The availability of a search warrant or production order depends on the nature of the underlying offence. However there is also a general provision in Criminal Justice (Miscellaneous Provisions) Act 1997 (as amended) which permits a search warrant to be issued in relation to any arrestable offence – broadly speaking, this means an offence which carries a possible prison sentence of five years or more.

Service provider outside Ireland

Where a service provider is located in another jurisdiction then access to data will generally take place either on the basis of a mutual legal assistance request, or on the basis of voluntary cooperation of the service provider with a request made by a member of the Garda Síochána. The procedure in relation to mutual legal assistance requests is set out in the answer to questions 25-27, and there are no formal procedures prescribed by law in relation to requests for voluntary cooperation (though providers do, of course, set their own internal requirements for such requests).

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 see the answer to question 15 for the general position regarding admissibility of illegally or unconstitutionally obtained evidence.

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.*

There is no protocol prescribed by law in relation to this, and there is no published material as to how the Garda Síochána has adopted such a protocol internally.

The only case in which this issue has arisen appears to be *People (DPP) v. Rattigan*.[33] This involved a dispute as to the forensic integrity of a mobile phone where a garda had replaced a SIM card with a blank ("cloned") SIM card to keep the phone off the network pending forensic analysis. In addressing this point the Court of Appeal held that this type of dispute will generally go to the weight of evidence rather than its admissibility.

[33] [2018] IECA 315.

***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?*

There are no such rules in criminal procedure – there is no legislation in this area and there has been no caselaw on this point.

***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?*

The main issue in Ireland appears to be that of delay. In the 2017 European Council *Mutual Evaluation on Combating Cybercrime* the Irish authorities "stressed that the fact that the MLA process is time-consuming and the processes can be cumbersome".[34] This reflects a general view within Irish police; for example one garda (police officer) was recently quoted anonymously in the media as saying that social media investigations are significantly hampered by the delay in receiving responses to MLA requests:

> We have to write affidavits and then the Director of Public Prosecutions (DPP) & Chief State Solicitors Office outlines in a legal document what the offences are, they are then sent to the local district attorney where the head office of these social networks are located and they go to court for us to get the order to preserve the information if they are satisfied with the supporting documentation.

[34] Council of the European Union, 'Evaluation Report on the Seventh Round of Mutual Evaluations "The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime" - Report on Ireland', 109.

> This then has to be renewed every 90 days on a rolling basis. Very often you get some headway on an investigation and then you have to send off for this and the whole thing is parked as it's a long drawn out process.[35]

***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?*

***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?*

Taking questions 34 and 35 together: Ireland has not opted-into the EIO so these issues do not arise.

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

See attached draft book chapter discussing how voluntary cooperation developed in Ireland and the legal issues it now presents.

[35] Cathal McMahon, 'Gardaí Dealing with Avalanche of Social Media Complaints Claim "unnecessary Obstacles" Put in the Way by Management and Web Firms', Independent.ie, 29 April 2017, http://www.independent.ie/irish-news/news/garda-dealing-with-avalanche-of-social-media-complaints-claim-unnecessary-obstacles-put-in-the-way-by-management-and-web-firms-35664310.html.

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.

Data protection/privacy

There is an overlap here with the answer to question 19 and, as outlined in that answer, Irish law does not currently provide formal mechanisms for addressing privacy and data protection concerns in relation to seized data but this may change in light of *CRH PLC, Irish Cement Limited and Séamus Lynch v The Competition and Consumer Protection Commission*.[36]

Right to a fair trial and transparency of forensics tools

There are no legislative rules regarding digital forensics tools. There has been significant litigation regarding the analogous area of breath testing technology but with inconclusive results. In *Dowling v. Brennan*[37] the High Court held that a drink driving defendant was not entitled to have an expert review the source code of a breath testing machine without first demonstrating that there is a real

[36] [2017] IESC 34.
[37] [2010] IEHC 522.

risk of an unfair trial, while in *Oates v. District Judge Browne*[38] the Supreme Court held that a person charged with drink driving had a fair trial right to have an expert carry out a physical inspection of a breath testing machine, without the need to establish a particular fault in advance.

Retention of copied data

There does not appear to be any public material regarding Garda Síochána retention periods for digital evidence after the trial/appeal process has been concluded.

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?*

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.*

I will consider questions 38 and 39 together.

The criteria for admissibility of mobile forensic evidence are the same as for other forms of evidence. The general rule is that electronic evidence which is automatically generated (such as CCTV, video, or file metadata) is admissible as a form of real evidence.[39] The position was recently summarised in *People (DPP) v. Power*[40] as follows:

> The law in this jurisdiction, since *People (Director of Public Prosecutions) v. Murphy*[41] and *People (Director of Public Prosecutions) v. Meehan*[42] is that records generated by computer and information technology systems, either mechanically or electronically, without human intervention, are admissible as real evidence, provided the court has evidence concerning the function and operation of the system in question. In simple

[38] [2016] IESC 7.
[39] *People (DPP) v. Colm Murphy* [2005] IECCA 1.
[40] [2018] IECA 119.
[41] [2005] 2 I.R. 125.
[42] [2006] 3 I.R. 468.

terms what is required in that regard is evidence of what the machine does (as opposed to how it does it), and that it was operated (and prima facie was functioning) correctly on the relevant occasion.[43]

The requirement that the court has "evidence concerning the function and operation of the system" is relatively straightforward to meet – in *People (DPP) v. Power*[44] the Court of Appeal held that all that is required is that the witness is trained to operate the system and can describe what it does. It is not required that the witness is qualified as an expert, nor that the witness be able to describe the underlying principles or software by which the system works. An analogy relied upon by the Court of Appeal was that of "a radiologist giving evidence of an MRI scan or a CT scan or an X ray where there is no necessity for the radiologist to know the intricacies of the machine that conducts the work in order to give evidence of what it produces".[45] In that case, therefore, the evidence of a Garda sergeant as to a XRY report was admitted notwithstanding that she was not an expert in the operation of the software itself.

***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?*

I take this question as referring to procedural rules specific to forensics rather than illegality or unconstitutionality in the obtaining of evidence. It is unlikely that there will be any "procedural breach" given the lack of any legislative rules or published guidelines regarding mobile forensics in Ireland. However the judgment in *People (DPP) v. Rattigan*[46] (mentioned already in question 31) suggests that any issue as to the handling of mobile forensics will go to reliability rather than admissibility – that is, it will not make evidence inadmissible but may affect the weight to be given to it. This conclusion is supported by caselaw from other areas where the failure to follow

[43] Para. 100.
[44] [2018] IECA 119.
[45] Para. 94.
[46] [2018] IECA 315.

procedural rules for the forensic handling of evidence is not necessarily fatal – see e.g. *Health Products Regulatory Authority v Anne Rossi*[47] where the failure to follow statutory rules regarding the analysis of seized drugs did not itself make the results of that analysis inadmissible.

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?*

There is no caselaw on the admissibility of data obtained from the cloud which was located outside the jurisdiction.

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.*

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.*

I will take questions 42 and 43 together. There are no published rules regarding technology, methodology or standards used by the Garda Síochána in the examination of digital evidence. (There is, for example, nothing comparable to the Association of Chief Police Officers *Good Practice Guides for Digital Evidence*.) The issue of alteration of evidence does not appear to have been considered in the caselaw.

[47] [2019] IEHC 723

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

***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.*

There is a significant number of cases in which the admissibility of evidence taken from mobile phones has been challenged; however for the most part these challenges have been incidental to the case, have not been fully considered by the court, and have not resulted in any significant guidance on this issue. In addition to the cases already cited see e.g.:

- *People (DPP) v. Gavin Sheehan.*[48] In this case the prosecution relied on messages sent through Facebook Messenger, retrieved from a mobile phone using a XRY system. The forensic examiner admitted that he could not prove how the Messenger app operated, nor who had sent the messages, nor how Facebook generated the time next to each message. The Court of Appeal held that the messages were nevertheless admissible, holding that "we think that there is no distinction between what one might call reading the contents of a phone which can be seen with the naked eye or with the use of such equipment [the XRY system] to download the contents and view it with the naked eye thereafter".[49]
- *People (DPP) v. Gary Flynn*.[50] In this case the Court of Appeal held that the appellant did not have *locus standi* to rely on the constitutional right to privacy of third parties to challenge the admissibility of evidence discovered on their mobile phones, notwithstanding that the warrants used to seize those phones were invalid.
- *People (DPP) v. David Byrne, Mark Farrelly and Niall Byrne*.[51] In this case the Court of Appeal held that contact lists and text messages recovered through a XRY system were not hearsay evidence and were admissible in the same way as a private diary entry would be.

[48] [2020] IECA 142.
[49] Para. 62.
[50] [2018] IECA 39.
[51] [2020] IECA 108.

***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.*

No – there is no recognised standardisation of this sort in relation to any aspect of the digital evidence process.

***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?*

There is no reported caselaw on this point. There have been a number of criminal trials where trial judges have declined to exclude evidence based only on a failure to comply with data protection law.[52] Even in a civil law context Clark notes that:

> I have not found any cases in which the (prejudiced) data subject sought to successfully argue that because the data protection principles were breached, subsequent use of data or information was unlawful and/or unconstitutional.[53]

***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.

---

[52] See e.g. Olga Cronin, 'Special Criminal Court to Admit Recordings from Covert Audio Devices in Conspiracy to Murder Case', TheJournal.ie, 30 October 2019, https://www.thejournal.ie/secret-recordings-court-authorised-kinahan-4872784-Oct2019/; 'Prison Officer Accused of Assault Fails to Stop Case', The Irish Times, 11 February 2012, https://www.irishtimes.com/news/prison-officer-accused-of-assault-fails-to-stop-case-1.461388.
[53] Clark, "Data Protection and Litigation" (2009) 16(8) *Commercial Law Practitione*r 167.

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

There do not appear to be any reported cases in Ireland in which mobile forensics evidence has been found inadmissible.

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?*

There is no special rule of law or guideline on this point.

- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*

There is no special rule of law or guideline on this point.

- *Must such evidence be examined by an expert witness?*

As explained above at question 39, forensic evidence can be presented by a witness who is trained in the use of the relevant forensic tool but who need not be an expert.

- *If not obligatory, is this a common practice?*

In the majority of cases mobile forensic evidence is presented by Garda witnesses who are not experts.

- *What are the requirements for experts (experience, independence, training, etc.)?*

Experience and training

The leading textbook summarises the required expertise as follows:

> A witness who gives evidence as an expert must have sufficient expertise in relation to the matter upon which he or she is to give evidence to be considered an expert and the burden of establishing this rests on the party calling the witness. Such expertise may be acquired by reason of experience, training or knowledge. In *Galvin v Murray*, Murray J stated that, in general terms, "an expert may be defined as a person whose qualifications or expertise give an added authority to opinions or statements given or made by him within the area of his expertise". No formal qualifications are necessary if the judge is satisfied that the witness has the requisite expertise. Thus, in *McFadden v Murdock*, a shopkeeper was allowed to testify as to the amount of wastage that it was reasonable to expect in the course of a grocery business. Provided that an expert is appropriately qualified, the admissibility of his or her evidence does not depend on the court's view as to how expert the person is, that is a matter that goes to weight.[54]

A practical aspect of this is that the self-taught hacker may testify as an expert in appropriate cases notwithstanding that they do not have formal qualifications in the area.

Independence

McGrath summarises the requirements for independence as follows:

> [A] pre-existing relationship between an expert and a party will not disqualify the expert from giving evidence although it may affect the weight to be given to his or her evidence. In *Galvin v Murray* it was held that engineers employed by a County Council were experts for the purposes of disclosure obligations in a personal injuries action. Murphy J held that:
>
> > "The fact that an engineer is employed by one or other of the parties may affect his independence with a consequent reduction in the weight to be attached to his evidence but could not deprive him of his status as an expert."

[54] Declan McGrath, *Evidence*, 2nd ed. (Dublin: Round Hall, 2014), para. 6.36.

In Toth v Jarman it was held that the existence of a conflict of interest on the part of an expert does not automatically disqualify an expert but is likely to lead the court to decline to act on his evidence.

Any fact that bears upon the independence of the expert such as a prior relationship with the party calling him or her should be disclosed. In *ANZ National Bank Ltd v Commissioner of Inland Revenue*, MacKenzie J emphasised that an expert should "make clear the nature of the involvement with the affairs of the party calling the witness, and should not assert an independence which does not exist".

In order to ensure that the evidence of an expert is independent and uninfluenced by the exigencies of the litigation, it has been held that it is inappropriate for an expert to be remunerated on the basis of a contingency fee.[55]

- *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?*

Mobile forensics for criminal law enforcement are not centralised in Forensic Science Ireland but are the responsibility of the Garda Síochána. There is no publicly available information as to how mobile forensics are managed within the Garda Síochána except that there is a national forensics function within the Garda National Cyber Crime Bureau, a regional function with six divisional cyber crime investigation hubs currently being established, and on scene triage of digital devices by first responding Gardaí currently being introduced.[56]

[55] McGrath, para. 6.39-6.42.
[56] Michelle Hennessy, 'Gardaí Cut Backlog of Child Sex Abuse Case Analysis in Half, but Long Delays Remain', TheJournal.ie, 31 December 2019, https://www.thejournal.ie/child-sex-abuse-backlog-4919785-Dec2019/; Conor Gallagher, 'Over 200 Gardaí Begin Cybercrime Training to Speed up Online Child Abuse Investigations', The Irish Times, 20 January 2020, https://www.irishtimes.com/news/crime-and-law/over-200-garda%C3%AD-begin-cybercrime-training-to-speed-up-online-child-abuse-investigations-1.4144773.

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.*

I am not aware of any such caselaw other than the cases already set out.

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.*

There is no such standardisation of digital evidence – neither obligatory nor critical to the admissibility, etc. of evidence.

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.*

On searching the database of judgments for terms related to mobile forensics I found no cases in which such evidence was rejected.

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

51. **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?*

Equality of arms

It is a general rule in Irish law that a party should be able to challenge expert evidence put forward by the other side, including the opportunity to put forward its own expert witness.[57]

Legal aid

Where defence lawyers determine that a forensic expert is necessary for the adequate conduct of a defence then that cost will normally be covered by free legal aid under the Criminal Justice (Legal Aid) Act 1962.[58]

***52.* Question:** *Is there any training required by law for the judges, prosecution, expert witnesses, lawyers involved in cases with evidence coming from mobile forensics?* [59]

There is no legal requirement for specific training in this area in relation to judges, police or lawyers. The qualifications for a person to testify about the operation of a forensic system are set out in the answers to questions 38 and 39; the qualifications required of an expert witness are set out in the answer to question 48 above. Note that these are very different – a person may testify as to the output of a forensic system notwithstanding that they are a technician rather than an expert.

***53.* 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?*

There are no such time limits in Irish law.

[57] *JF v. DPP* [2005] IESC 24.
[58] Walsh, *Walsh on Criminal Procedure*, para. 16.69.
[59] Law Reform Commission, 'Report on Disclosure and Discovery in Criminal Cases' (Dublin, 2014), https://www.lawreform.ie/_fileupload/Reports/r112D&D.pdf.

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

***54.* 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.)?*

These are discussed in the questions following

5.1 The Prosecution

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

I am not aware of any publicly available material for lawyers representing the prosecution in relation to mobile forensics.

5.2 The Court

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

In the Irish model police investigation of crime is not overseen by the judiciary; however in the majority of cases search warrants and production orders must be issued by a District Court judge and there is a form of *ex post* control insofar as trial judges will determine whether digital evidence is admissible at trial.

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

As with all evidence, the prosecution must establish to the court that evidence obtained via mobile forensics is admissible and the court has a discretion to exclude evidence on various grounds – for

example, in addition to illegality and unconstitutionality, the court may exclude evidence where the prejudicial effect of the evidence would outweigh its probative value.

5.3 The defendant and defender

58. **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.*

There are no rules specific to mobile evidence, but there are some rules of general law which are applicable in this context also.

Duty to collect evidence

There is a general duty in Irish law on police investigating a crime to seek out and preserve evidence. This was summarised by the Supreme Court in *Braddish v. DPP*[60] by Hardiman J. who noted that Gardaí have a duty:

> arising from their unique investigative role, to seek out and preserve all evidence. This is so whether the prosecution propose to rely on the evidence or not, and regardless of whether it assists the case the prosecution is advancing or not.

This duty will extend to digital evidence, and failure to collect such evidence may lead to a criminal trial being prohibited. For example, in *RC v. DPP*[61] the applicant was accused of sexual assault. He claimed that the complainant regularly phoned him to invite him to her apartment, while she

[60] [2001] 3 I.R. 127.
[61] [2009] IESC 32.

claimed that he initiated all phone calls. However, due to an oversight on the part of police, the phone records of the complainant were not sought and were no longer available by the time of the trial. The Supreme Court found that the failure to collect this evidence had denied the applicant the opportunity to challenge the credibility of the complainant on a central issue and therefore it would be unfair for the trial to proceed. Per Denham CJ.:

> The prejudice alleged by the appellant is that the telephone records of the complainant, if available, would have corroborated his account of his contact with the complainant between May, 2001 and September, 2001. Such telephone records would confirm that the complainant regularly phoned the appellant and sent him texts during that period, and that this would corroborate his oral evidence. Thus they go to the core issue of the case, the credibility of the appellant and the complainant. […]
>
> In general the absence of phone records is not a reason to prohibit a trial. It is the particular circumstances of this case, including the approach taken in the investigation, and the questions asked and answered as to mobile phone use, together with the failure of the prosecution to seek the phone records of the complainant, while obtaining those of the appellant, which create circumstances where there is a real risk of an unfair trial.

Disclosure of unused material

The general rule in Irish law is that the prosecution must make disclosure of any information, including unused evidence, which is relevant to the proceedings and could assist the defence.[62] This extends to information obtained from mobile devices in the same way as any other information. However this duty is not codified by law. The Garda Inspectorate has found that there are significant practical problems in relation to disclosure generally, with Gardaí "generally untrained in disclosure issues, particularly in presenting evidence that is disclosable or non-disclosable and in preparing disclosure schedules for court".[63] The Law Reform Commission has also recommended that a statutory framework for disclosure should be provided.

[62] Walsh, *Walsh on Criminal Procedure*, para. 15.137.
[63] Garda Síochána Inspectorate, 'Crime Investigation', Dublin, October 2014, pt. 11, http://www.gsinsp.ie/index2.php?option=com_docman&task=doc_view&gid=243&Itemid=152.

Disclosure of methods

An expert witness may be required to disclose their methods where that is necessary for the purposes of a fair trial. An example can be seen in the context of the civil law in *Mulcahy v Avoca Capital Holdings*.[64] In that case the plaintiff was the subject of disciplinary procedures by his employer including allegations of "improper dealing with the e-mail inboxes of senior members of staff and ... improper dealing with the company's IT systems". He brought an action in the High Court seeking to stop the disciplinary process. In order to deal with the allegations against him, the plaintiff sought to have his computer forensics experts examine certain computers belonging to the employer. Access was granted by the court, but a dispute arose as to whether the plaintiff's experts would be entitled to keep secret their proprietary methods for carrying out the examination. Clarke J. held that while a court would not unnecessarily require an expert to reveal confidential methods, by acting as an expert witness a person exposed their methodology to scrutiny in court and fair procedures demanded that the other party be able to assess and challenge that approach in appropriate cases.

5.4 Witnesses

59. **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.*

[64] [2005] IEHC 136.

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

5.5 The Victim

***60.* 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.*

I will address questions 59 and 60 together as the privacy issues of witnesses and victims overlap.

There are no specific Irish rules regarding privacy rights in mobile forensic evidence and there has been no caselaw on this point. The recent UK debate on "digital strip searches"[65] – that is, excessive taking of information from victims' phones – has had no Irish counterpart.

In general, Irish law does not provide specific rules to protect the privacy rights of either victims or witnesses. There are some exceptions: for example, trials of sexual offences must generally be held with the public excluded[66] and victims of sexual offences are generally entitled to anonymity.[67] Similarly, there are specific statutory rules regarding access to counselling records relating to the victim in sexual offence cases where those records are held by third parties.[68] Outside of these relatively narrow cases, however, there is no formal protection for the privacy of either the victim or a witness.

[65] See e.g. 'Digital Strip Searches' (London: Big Brother Watch, 2019), https://bigbrotherwatch.org.uk/wp-content/uploads/2019/07/Digital-Strip-Searches-Final.pdf.
[66] Thomas O'Malley, *Sexual Offences*, 2nd ed. (Dublin: Round Hall Ltd, 2013), para. 17.14.
[67] O'Malley, para. 17.16.
[68] See generally William Abrahamson, James Dwyer, and Andrew Fitzpatrick, *Discovery and Disclosure*, 3rd ed. (Dublin, Ireland: Round Hall Ltd, 2019), chap. 25.

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.