"How many thousand pages?!" Digital Device Analysis and Public Interest Immunity in Family Proceedings

Mark Cooper & Emma Kelly

This article has been written for a forthcoming edition of the Family Law Journal.

Introduction

1. The first Apple iPhones went on sale in the UK in November 2007. Other smartphones had been on the market since the mid 1990s, albeit they were far less sophisticated. In September 2022, Apple released its fourteenth series of iPhone models. In addition to Apple iPhones, there are many other ranges of smartphone available. These phones have become our go-to devices for calls, messaging, web browsing, social media, streaming, gaming and many other activities.

   (1) Recent research[1] shows that:

   (a) There are 64 million UK internet users in 2022.
   (b) 94% of UK households have access to the internet.
   (c) 84% of UK adults own a smartphone.
   (d) Almost two thirds (61%) use Facebook on their mobile every day.
   (e) On average, they spend 3 hours 59 minutes per day online, which rises to 5 hours and 6 minutes for 18–24 year olds.
   (f) The top five daily smartphone apps for UK adults are Facebook (61%), WhatsApp (50%), Instagram (35%), Facebook Messenger (32%) and Gmail (27%).
   (g) Daytime internet usage has more than doubled since the Covid-19 pandemic, which has also led to a rise in the use of video conferencing apps, such as FaceTime, WhatsApp video, Facebook Messenger, Zoom, Skype, Houseparty and Microsoft Teams.

2. It is hardly a surprise, therefore, that mobile phone evidence (and evidence from other digital devices) is becoming so common in care proceedings. The story of every care case is a snapshot into the life of a family – whether it is a case about inflicted injuries, sexual abuse, FII, neglect, domestic abuse – it is likely that there will be mobile phone or digital evidence available which *could* be relevant to the just resolution of the case.

[1] https://www.finder.com/uk/mobile-internet-statistics

3. Sometimes, requests for disclosure of mobile phone evidence are met with an application for non-disclosure in order to preserve public interest immunity (PII). Clearly, PII is a huge topic, so this article will only address it in the context of mobile phone analysis (see below).

Disclosure and Inspection of Documents – Key Legal Principles

4. FPR Part 21: MISCELLANEOUS RULES ABOUT DISCLOSURE AND INSPECTION OF DOCUMENTS:

   (1) The FPR does not actually provide a formal code for disclosure in Family Proceedings (per Moylan J in ***Tchenguiz-Imerman v Imerman* [2014] 1 FLR 232, FD**). Instead, parties must use common law principles, which are best summarised in the Civil Procedure Rules.

   (2) In CPR Part 31, "*document*" means anything in which information of any description is recorded; and "*copy*", in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.

   (3) According to CPR PD 31B, the term "*documents*" extends to "*Electronic Documents*" (para 1). These are defined (para 5(3)) as "*any document held in electronic form*" including text messages, email and documents stored on any form of memory device computer drives, memory sticks and mobile telephones.

5. FPR Part 21 only really deals with terminology (r 21.1) and two other aspects of disclosure – namely, disclosure against a non-party under statute (r 21.2), which includes the police, and claims to withhold disclosure. However, the guidance in the Family Court Practice distils the following helpful principles:

   (1) *General rule* – the general rule is that a fair trial demands that the Court makes its decision on the basis of all available relevant evidence, which includes documentary evidence. Of course, certain documents may be exempt from production, e.g. due to being covered by confidentiality, privacy (including privilege) or by PII. In exceptional circumstances, sensitive material may be disclosed only to special advocates (see r 21.3 for controlled material procedures).

   (2) *Duty arises* – the law is unclear as to at what point in family proceedings a duty to disclose arises. For example, in financial remedies cases, the duty has been found not to arise until the Form E was filed (per ***Imerman v Tchenguiz and Others* [2010] 2 FLR 814, CA**).

(3) *Continuing duty* – once disclosure has begun, there is an ongoing duty throughout the proceedings. This common law rule is stressed in CPR r 31.11, "*disclosure continues until the proceedings are concluded*" (as explained by Stuart Smith LJ in ***Vernon v Bosley (No 2)*** **[1998] 1 FLR 304, CA**) and that common law applies equally to family, as to any other, civil proceedings.

(4) *Disclosure* – In this context, the term "*disclosure*" simply means that a party states that they know a document "*exists or has existed*" (CPR 31.2; FPR 21.1(1)). This includes electronic documents.

(5) *Inspection* – Following the *disclosure* of documents there follows the right of other parties to inspect them (CPR 31.3(1); FPR 21.1(2)). However, there are exemptions to the rule as to inspection, which can be summarised as follows:

(a) documents no longer in the possession or control of the disclosing party;
(b) documents to which a right to withhold is said to attach (e.g. privilege, confidentiality and PII); and
(c) documents where the inspection of which a party claims would be disproportionate to the issues in the case.

6. Regardless of the foregoing legal principles, the vast majority of situations where family practitioners have to deal with mobile phone evidence will be as a result of devices being seized by the police. However, there may be circumstances where the above procedures should be considered. For example, when representing a parent, if you have instructions that your lay client believes the other parent has relevant evidence on their mobile device (e.g. photographs of abuse), the disclosure/inspection process should be followed.

7. There is no expectation that parents routinely submit their devices for examination at the start of care proceedings, which would amount to a fishing expedition and – arguably – a reversal of the burden of proof. However, if a parent's mobile phone contains crucial evidence which they do not disclose and it is later uncovered through a police investigation, for example, a text message containing an admission of culpability, it is likely to affect their credibility.

8. The overriding objective set out in FPR Part 1 clearly applies.

Different types of Digital Evidence

9. There are many different types of digital evidence which can find their way into family proceedings.

10. Mobile Telephones:

(1) By far the most common type of digital evidence, which is the main subject of discussion in this article.

(2) As well as smartphones, there are also simpler devices, e.g. "*burner*" phones, which only allow calls and texts – i.e. with no *smart* features.

(3) As well as the internal memory on the phone, there may be additional data stored on the phone's SIM card. Most phones store data in the phone's own internal storage, but even iPhones have settings to allow certain information to be stored on a SIM card (e.g. contact information).

(4) Smartphones will also contain other sources of information, such as photographs, instant messages, GPS data, etc. – these are discussed in more detail below.

11. Tablets:

(1) The most well-known tablet device is an iPad. It is possible that the user of the device has synced their iPad with their iPhone, which means that an analysis of an iPad could be a substitute for a missing iPhone.

(2) The syncing of devices also means that evidence on a seized phone could be destroyed or amended remotely (risking incrimination) if the seized device is online. The police generally have methods to avoid this (e.g. by disabling internet access on the seized device), but this would be beyond the control of the parties to a family case.

(3) In circumstances where the police will not release a seized phone for expert analysis (see below), another option could be to inspect the contents of a synced tablet device. The obvious risk is contamination of the seized device, so this is best carried out by an expert.

(4) Other tablet devices include the Amazon Kindle range, Microsoft SurfacePro, Samsung Galaxy Tab, etc.

12. Computers:

(1) Like smartphones and tablets, computers (e.g. laptops and desktop PCs, iMacs, MacBooks, etc.) keep a record of communication evidence – such as emails, internet browsing history and searches – as well as stored *documents* (Cf. CPR Part 31), such as photographs and videos.

(2) Computers are frequently seized by police as part of criminal investigations. They can also form part of investigations by the National Crime Agency, who are known to monitor chatrooms for terrorist activity and sexual grooming of children.

13. Games consoles: Many modern games consoles (e.g. Sony PlayStation 5, Microsoft Xbox One, Meta Oculus, etc.) contain chat functions and the ability to store data, including text and images.

14. Voice-controlled devices: Even devices such as Amazon's *Alexa*, Apple's *Homepod* and Google's *Home* are now routinely seized by the police during investigations where digital evidence is thought to be probative. These devices store various forms of information, including a record of the search terms, e.g. "*Alexa, what causes bleeding on the brain*" or "*Hey Siri, what is the likely sentence for child abuse*".

Sources of Digital Evidence

15. Police Disclosure:

(1) Most digital evidence will make its way into family proceedings via disclosure from the police, usually when mobile phones are seized (or voluntarily surrendered) as part of an investigation. However, this is seldom straightforward and rarely – if ever – will parties be provided with a *gift-wrapped* complete analysis of all the relevant evidence on the device(s).

(2) Police disclosure orders should be drafted in such a way to make sure that digital evidence is specifically included, e.g. "*Copies of all digital exhibits generated as a consequence of interrogation of any electronic device, including any full analysis.*"

(3) If the police have not yet interrogated the devices, the PDO may not produce anything to reveal the existence of any seized devices. If there is no MG11 statement from the officer who seized the devices, the next best place to check will be the investigation log. From the log, it should be possible to ascertain when, where and by whom any devices were seized. A more targeted PDO can then be drafted.

16. Time considerations for police disclosure:

(1) No reliance should be placed on the police to provide a full analysis within the timescales for children in care proceedings, unless there is a clear commitment from the police to do so. For example, in ***Re CD* [2021] EWFC 112**, the officer responsible for interrogating the mobile phones was effectively trying to perform the task of Hercules. As HHJ Walker (sitting as a High Court Judge) put it:

> *"22. Despite having received the parents' mobile 'phones within days of the investigation commencing in October last year [2020], the material from those phones still had not been provided by the time I heard the case on the 20th August [2021]. As a result, I repeated the request from the family court for the material to be provided, or in the alternative, for the physical 'phones to be handed back to the parents, and approved the instruction of Evidence Matters in order for the analysis to be conducted in the event that the police had not been able to do so. Warwickshire Police then made an application to vary the terms of that order. I was informed that the officer in charge of the investigation only had access to one antiquated computer, and each time that she wished to view the material that had, by that stage, been downloaded from the 'phones by an external agency, it was necessary for the whole content of the CD to be uploaded, a task that took many hours."*

(2) In ***Re CD***, the officer in question was spending about one hour per month on the analysis, yet the police were refusing to allow the devices to be interrogated by an expert. There was a complete failure by the police to recognise the damage of delay to the welfare of the child in the family proceedings, which was compounded by their refusal to release the devices. This case is discussed further below in relation to PII.

17. Owner of the device:

(1) Sometimes digital evidence is provided directly by the owner of the device. For example, a parent may exhibit a screenshot of a Facebook message or an Instagram post to their witness statement. These are invariably without context and, if it is proportionate to do so, may lead to an application for further interrogation of the device (i.e. by an expert).

(2) The owner of the device may be willing to submit the whole thing for expert analysis, but this would need to be a proportionate step, bearing in mind the issues in the case.

18. Cloud-based storage (see below):

(1) Some mobile phone data is also available in the *cloud*, such as Apple's iCloud, which backs up emails, photographs, videos, contacts, etc. These are easily accessible via iCloud.com, but accessing backups of iMessages is a bit more complicated and would require an expert – not least of all due to the risk of contaminating/deleting the evidence.

(2) This is discussed in more detail below.

Methods of Analysis

19. Police Analysis:

(1) Where interrogation has taken place, it is often a preliminary process carried out by an officer and it can sometimes have the appearance of rough notes or copied and pasted messages, which have probably been prepared as a preliminary triage before a suspect interview. Sometimes the police disclosure might include extracted pages from a more detailed analysis, which is based on a download of the entire phone's contents. That is often a give-away that the police have already had the phones analysed and that they are sitting on thousands of pages of data (look out for a Cellebrite analysis, for example). Nevertheless, these initial documents from the police are often a helpful starting point, because they may include anything the police have (so far) spotted of relevance – e.g. a relevant internet search or a suspicious text message.

(2) In some instances, the police may have obtained their own expert report providing an analysis of the digital device. Such reports are disclosable within the family proceedings. Some forces use agencies like Cellebrite, and others use the likes of Cyfor and Evidence Matters who also work directly with the Family Court.

(3) Family practitioners should beware of complacency when looking at any analysis performed by the police, which can be no substitute for doing one's own analysis. The police may not, for example, note down things which undermine the investigation, or something relevant to a parent who is not a suspect in their investigation.

20. Expert Analysis:

(1) By way of a Part 25 application, parties in family proceedings can seek permission to instruct an expert agency to carry out an analysis of digital evidence. The usual Part 25 rules apply, but the following considerations are worth bearing in mind.

(2) HEALTH WARNING: the reports from these agencies are **not** infallible and can fail to include important details! Therefore, any such instruction is no substitute for an advocate's own analysis of the raw data – see below.

(3) The biggest advantage of using an expert agency is that they are extremely fast. The turnaround time is usually about a week, but it can be as quick as 24 hours in urgent situations.

(4) The cost is also remarkably reasonable – with a full analysis often costing less £1,000+VAT per device. The Legal Aid Agency will also pay, but prior authority may be required.

(5) Regard must always be given to the chain of evidence if the phone is in the possession of the police. The agency will normally require the original phone or at least a copy of the raw data from the phone (not in the analysed form, but as in a complete copy of the phone's digital storage in its original format). Some police forces will release the phones for this purpose or allow the agency to attend the station and take a copy of the contents under supervision.

(6) The agencies who do this sort of work are used to chain of evidence issues and understand the procedures required. Indeed, some police forces around the country actually use these agencies themselves. Some police forces have been known to welcome a Part 25 analysis of the devices in the Family Proceedings on the basis that they will later seek a copy of the report from via a disclosure application of their own.

(7) The letter of instruction is absolutely crucial when instructing an expert agency. It must be extremely clear as to what is required. For example, there is no point asking for "a complete analysis of the mobile device(s)", as you may as well just read the raw data. The letter of instruction should include things like:

(a) *All messages (via iMessage, SMS, WhatsApp, Facebook Messenger, Instagram, Snapchat, email, etc.) between Joe Bloggs and Jane Bloggs between 00:01 on 1st June 2021 and 23:59 on 17th January 2022.*
(b) *Full internet search history and browsing history of Joe Bloggs between 00:01 on 1st June 2021 and 23:59 on 17th January 2022.*
(c) *All photographs and videos containing images of children.*
(d) *GPS locations of Joe Bloggs on 16th January 2022 between 07:00 and 15:00.*

(8) If the parties do not already have (usually from the police) a complete download of the entire contents of the phone, that can be requested separately as well.

(9) It is also sometimes possible for expert agencies to recover data from damaged devices or even lost devices (via cloud-based services or analysis of broken pieces).

(10) In short, the use of expert agencies is a cost-effective and fast way of analysing digital evidence, but it is by no means a perfect solution or substitute for proper analysis by the trial advocates.

21. Advocates' Analysis:

(1) Ultimately, there is no substitution for an advocate looking at the raw data and extracting relevant times, dates, locations and data into a separate chronology. Only then can this evidence be seen in the context of the story of the case. However, an expert report can make this process much quicker as it allows for a more targeted reading of the searchable raw data.

(2) For example, an internet search for "*what is the maximum sentence for murder*" might be explained away as something the witness was looking for whilst watching Netflix. However, when the time and location of that search places the witness at the scene of the index incident, it takes on a whole different interpretation.

(3) GPS locations are discussed further below under 'Uses of Digital Evidence', but this can be an important part of an advocates' analysis, if only to make sense of what a witness says about their movements at a particular time.

(4) The process of analysing phone records takes time, but it is definitely time well-spent.

Uses for Digital Evidence

22. Previous inconsistent statements: this is perhaps the most obvious use for digital evidence. Once the witness has confirmed their evidence in the witness box and they are sure the account given in their statement is correct, they can be taken to a reference in the digital evidence which undermines their credibility.

23. Call logs: these are very helpful, particularly when trying to piece together the parties' movements and actions at a particular time. Calls are broken down into phone calls, FaceTime calls, WhatsApp audio/video calls, Facebook messenger calls. There may also be group calls.

24. Messages: these are generally the most important evidence to come out of an analysis of a mobile device:

    (1) There are numerous different types – SMS/text, iMessage, Facebook, WhatsApp, Instagram, Snapchat, Twitter, etc.

    (2) If looking for messages between two parents and only one phone is available for analysis, you can still piece together conversations.

    (3) Increasingly, couples send each other messages even when they are in the same house, but messages can also demonstrate when a person has left the property, e.g. "what time will you be back?" etc.

25. Emails: it might be rare to find an email from a witness in which they confess to something like child abuse, but email receipts can be evidence of contemporaneous activity. For example, a receipt for an online gaming purchase and for a food delivery can help create a picture of what was going on in the home.

26. Internet search history:

    (1) There are obvious uses for this sort of data, especially when there are messages such as "How long do bruises last?" or "Why won't my baby stop crying?"

    (2) It can also be the case that the absence of a search history is just as important. For example, the records may reveal that the search history for a particular day (or several days) has been deleted. You may find that the entire search history has been deleted.

27. Timing: a combination of all these different types of evidence can greatly assist when trying to work out the time at which an event happened. For example, an internet search such as "sentencing guidelines for child abuse" in an injuries case, might suggest the abuse had already happened or that point (or, more sinisterly, that it was being planned).

28. Photographs, videos and audio records:

    (1) These are excellent sources of primary evidence which can also be used to narrow windows of opportunity. For example, a photograph of a child with or without bruising at a particular time can be relevant, or a video of a child who looks injured or uninjured.

    (2) Sometimes there are videos not of the abusive incident itself, but something similar – such as a video of a father throwing a baby up in the hair or shaking them too roughly.

29. GPS data:

    (1) At various points in mobile phone data there are coordinates, such as "52.484208492264 79, -1.8954694648990442" (St Ives Chambers, Birmingham).

    (2) The coordinates can be copied and pasted into Google, which will drop a red balloon/pin on a location in Google Maps. This is particularly useful when preparing cross-examination in terms of trying to work out whether a witness is where they say they are at that particular time.

    (3) However, this process also comes with a few health warnings(!):

(a) An advocate's analysis of GPS locations is not expert evidence and, if the assertion is challenged, it may be difficult to rely upon Google maps or it may just be a matter of judicial notice being taken.

(b) GPS stands for "*Global Positioning System*" and is typically accurate to within a 4.9m (16ft) radius under open skies. However, the accuracy decreases near buildings, bridges and trees. Other factors, such as the triangulation of satellites, etc. are involved, which need not be discussed here.

(c) This analysis will not be useful to demonstrate, for example, where a witness is *within* a particular location, such as which room in the house or where on the street. However, it could be used to show they were in Birmingham rather than Wolverhampton.

Public Interest Immunity ("PII")

30. The seminal definition of the common law principle of public interest immunity is by Lord Templeman in ***R v Chief Constable of West Midlands, Ex p Wiley*** **[1995] 1 A.C. 274 (HL)**:

> *"Public interest immunity is a ground for refusing to disclose a document which is relevant and material to the determination of issues involved in civil or criminal proceedings. A claim to public interest immunity can only be justified if the public interest in preserving the confidentiality of the document outweighs the public interest in securing justice."*

31. The test (per Lord Templeman) is: "*Whenever disclosure in litigation is under consideration, the first question is whether a document is sufficiently relevant and material to require disclosure in the interests of justice…. If a document is not relevant and material, it need not be disclosed and public interest immunity will not arise…. If a document is relevant and material, then it must be disclosed unless it is confidential and unless a breach of confidentiality will cause harm to the public interest which outweighs the harm to the interests of justice caused by non-disclosure."*

32. Where PII is claimed, the Court must conduct the above balancing exercise and also consider whether arrangements can be put in place to mitigate any perceived harm caused by disclosure of the material (per ***R (Mohammed) v Secretary of State for Foreign and Commonwealth Affairs*** **[2010] EWCA Civ 65**).

33. The adoption and use of the above test in family law, and specifically care proceedings, is best exemplified by Pauffley J in ***Re C (A Child) (Care Proceedings: Disclosure)*** **[2016] EWHC 3171 (Fam)** at paragraphs 14-16…

"[14] The first step is for legal advisers to consider whether the material sought or held is relevant and material to the proceedings. In a case of this kind, it would only be disclosable if it is necessary to dispose fairly of the proceedings. To judge relevance and materiality, it is necessary to consider the issues in play in the proceedings, i.e. the orders and factual findings sought as well as the evidence already before the court.

[15] Step two requires officials, in the first instance, to undertake a more detailed assessment of the sensitivity of the information. The critical question is whether there is a real risk that disclosure would cause substantial harm to an important public interest. If disclosure would not cause substantial harm it would be made. If, however, the assessment was that disclosure would harm the public interest then material 'attracts' PII and a claim must be considered.

[16] The third step involves determining whether to claim PII or make an application under the 2013 Act. This is a decision taken by the SSHD assisted by advice from those involved at stages 1 and 2. The decision maker will have to consider the importance of the information to the issues the court has to decide, and form a view as to whether the public interest in non-disclosure is outweighed by the public interest in disclosure, in order to do justice within the proceedings: [quotes Lord Templeman, as above]."

34. …and by the same learned judge later in the same proceedings in ***Re C (A Child) (No. 2) (Application for Public Interest Immunity)*** **[2017] EWHC 692 (Fam)** at paragraph 29:

(1) *"[29] There are three required steps when the SSHD considers whether to make a claim for PII. First, whether the material is relevant and passes the threshold test for disclosure in the applicable proceedings – (certificate, para 11). Secondly, if the threshold test is passed, whether the material identified as relevant and subject to disclosure attracts PII. The test is whether there is a real risk that disclosure would cause 'real damage' or 'serious harm' to the public interest – (certificate, paras 13 and 19). Thirdly, if applying the 'real damage' test, the material attracts PII, the question arises as to whether the public interest in non-disclosure is outweighed by the public interest in disclosure for the purpose of doing justice in the proceedings."*

Mobile Phone Analysis and PII

35. As mentioned earlier, ***Re CD*** **[2021] EWFC 112** was a case where the police took a very long time to analyse the suspects' mobile devices due to the poor facilities available for interrogation and the sheer volume of devices (from other investigations) to inspect.

36. The parties in the family proceedings had tried to circumvent this problem by instructing an expert agency to analyse the devices, which were in the possession of the police. The police refused to provide the phones to the agency and asserted public interest immunity as a basis for doing so. This led to several hearings and a trip to the Court of Appeal, albeit the appeal was compromised such that no judgment was ever required. By the time of the PII application, the data had actually been extracted from the devices, but the police wanted time to review it and then interview the parents. Ordinarily, that would be a sound basis for a PII application. However, the Court was unimpressed by the police's delay in extracting the data and, in any event, the messages in question were still visible to the parents via Apple's iCloud. The judgment relating to the PII application (which the police sough to appeal) was not published. However, in her judgment at the end of the finding of fact hearing, HHJ Walker said:

> *"23. I refused an application by the police to assert public interest immunity over the material that they had, by that point, extracted from the parents' phones. I ordered them to disclose it, after giving them a period of weeks to interview the parents. It was still necessary for me to approve the instruction of Evidence Matters in order to analyse the material, as we were uncertain as to the format in which the mobile 'phone material would be provided. But it was agreed by all parties that Evidence Matters enquiry would be asked to concentrate on the window in which it was asserted that the injuries may have been caused. However, it is right to reflect that, in a closed statement which supported the police's application, the officer drew the court's attention to some text messages that she was already aware of, which might have suggested that there had been discussions between the parents about previous incidents of poor handling of the baby, and some relationship difficulties.*
>
> *The police appealed my order. That appeal was later compromised, but the effect of the delay caused by the listing of the appeal was that the 'phone material was late going to Evidence Matters and late being received by the parties. It is vast. And over the course of weekend before this hearing began, the parties were provided with copies of the parents' most recent police interviews, which took place on the 11th November. Both parents were asked about text messages, photos and videos that began only three weeks after C was born, outside of the Evidence Matters report."*

37. The key learning outcomes from this aspect of the case are as follows:

(1) The police can take a very long time to disclose digital evidence.

(2) Parties to care proceedings should not be shy in seeking to obtain the material themselves, if the police are unable to provide it within acceptable timescales for the welfare of the child(ren).

(3) Parties should be prepared to argue that the public interest lies in directing the disclosure of the evidence (and, in this case, provision of the devices to an external agency for rapid analysis).

(4) Even when an expert analysis is obtained, it is important to remember the parameters set in the letter of instruction. For example, in this case, the local authority questioned the parents about material which fell outside of those parameters (and thus not covered by Evidence Matters). Therefore, it important to have the full source material and enough time to consider it.

This article has been written for a forthcoming edition of the Family Law Journal.

Mark Cooper and Emma Kelly
ST IVES CHAMBERS