

Consilio Institute: Practice Guide

# COLLECTING DATA FROM MOBILE DEVICES AND THEIR APPLICATIONS

By **Sophie Beattie EnCE, CDFE, Certified GDPR Practitioner**  
*Senior Director - Forensic Investigation and Expert Witness Services, Consilio*

Consilio Institute: Practice Guide

# COLLECTING DATA FROM MOBILE DEVICES AND THEIR APPLICATIONS

## TABLE OF CONTENTS

Introduction .....	3
Mobile Device Imaging .....	3
Collection Methods.....	4
Mobile Device Models .....	4
Mobile Device Applications .....	4
Questions to Ask Mobile Device Custodians .....	6
Post-Collection Considerations .....	7
Conclusion .....	7
About The Author.....	7

### Disclaimers

The information provided in this publication does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this publication are provided for general informational purposes only. While efforts to provide the most recently available information were made, information in this publication may not constitute the most up-to-date legal or other information. This publication contains links to third-party websites. Such links are only for the convenience of the reader; Consilio does not recommend or endorse the contents of the third-party sites.

Readers of this publication should contact their attorney to obtain advice with respect to any particular legal matter. No reader of this publication should act or refrain from acting on the basis of information in this publication – without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.

Use of this publication, or any of the links or resources contained within, does not create an attorney-client relationship between the reader and the author or Consilio. All liability with respect to actions taken or not taken based on the contents of this publication is expressly disclaimed. The content of this publication is provided “as is.” No representations are made that the content is error-free.

# I COLLECTING DATA FROM MOBILE DEVICES AND THEIR APPLICATIONS

## Introduction

Are you reading this on your mobile device?

Mobile devices are used every day for business and personal communications by a large quantity of the world's population. According to [GSMA real-time intelligence data](#),<sup>1</sup> more than six billion mobile devices are utilised worldwide.

The number of mobile device models, and the technology related to mobile devices has rapidly grown over the last ten years. The basic functionality of simply calling and texting has long since been surpassed. Today mobile devices can be used to browse the Internet, send and receive emails, create and store documents, install and utilise many different types of messaging or social media applications (apps), and more. A mobile device can effectively be thought of as a portable computer.

On review of the most commonly used mobile device forensic tools, there are currently over thirteen thousand different mobile device models and over four thousand independent mobile device applications which are supported for data extraction from mobile devices. These metrics are constantly changing as new technology and applications are brought to the market.

Due to the popularity and volume of mobile devices being used throughout the world, they have become common sources of digital evidence in litigation proceedings. Data related to mobile devices can be stored on the device, within a backup stored on a computer, or in a cloud repository. The best source of collection will depend on the specific scope of your matter. It is important to understand the different types of data that can be extracted

from mobile devices, mobile device backups, and the cloud. It is also important to think ahead and understand how data extracted from mobile devices or applications can be presented and reviewed. Asking specific questions ahead of the data collection exercise and working closely with your eDiscovery provider will ensure you are well prepared.

## Mobile Device Imaging

Mobile device imaging can be thought of as creating a backup of the information stored on the physical handset. The process is comparable to a user creating an iTunes backup or Android backup of their mobile device.

Data visible through mobile device applications (apps), however, may not always be stored on the device itself, may be in an encrypted format, or may be excluded from backups by the application's developer. As an example, emails which can be sent or received and viewed within an email application on a mobile device may not be fully synced on the handset itself. Typically, email data is only partially synced to a mobile device to enable offline browsing, and the majority of the data is stored within the cloud (on a server) to which the user connects when logging into the app. Email data synced to a mobile device is stored in an encrypted format and is not able to be extracted from the mobile device itself. This means that backing up the mobile device or imaging with forensic tools would not capture email data. The email data would need to be captured directly from the email server or cloud account.

<sup>1</sup>The Mobile Economy, GSMA, <https://www.gsma.com/mobileeconomy/> (2021).

## Collection Methods

Traditionally, mobile devices are collected in person by a computer forensic specialist, using mobile device forensic tools to extract all available data from the device. However, when dealing with cross border matters, where distance may cause time delays and additional costs, or with custodians who cannot accommodate an in-person collection, it is possible to capture data contained on a mobile device remotely.

The remote collection methods utilised are forensically sound, defensible, and achieve the same results as that of an in-hand/in-person collection. The methods will differ based on the model of the mobile device that is in scope.

Mobile device data can also be backed up to the cloud. Apple enables iPhone users to backup data stored on their device to a cloud repository named iCloud. Android has a similar feature allowing users to back up their data to a cloud repository named Google Drive. Specific applications can also have their own cloud repositories for data storage, for example Telegram and Facebook data is typically stored on Telegram and Facebook servers.

Cloud storage repositories related to mobile devices (iCloud and Google Drive) are frequently updated for security purposes which can impact and limit the ability to collect data directly from these repositories.

When conducting data collections of data stored on mobile devices, it is best practice to collect from the device itself or from the specific application of interest.

## Mobile Device Models

There are many different types of mobile devices available to a user which run different operating systems, the most common of which are iOS and Android.

Different models run different types of operating

systems, and the operating systems differ in functionality and are updated regularly. Updates can affect the way in which applications store their data or how they are backed up. In other words, data that can be forensically extracted today, may not be able to be extracted tomorrow, or vice versa.

The type of mobile device and its operating system can have a direct impact on the types of data that can be extracted from it. For example, WhatsApp data is stored in an encrypted format on recent Android devices and cannot be extracted as part of a standard mobile phone imaging exercise. This is not the case with iPhone where WhatsApp data would be captured in a readable format.

## Mobile Device Applications

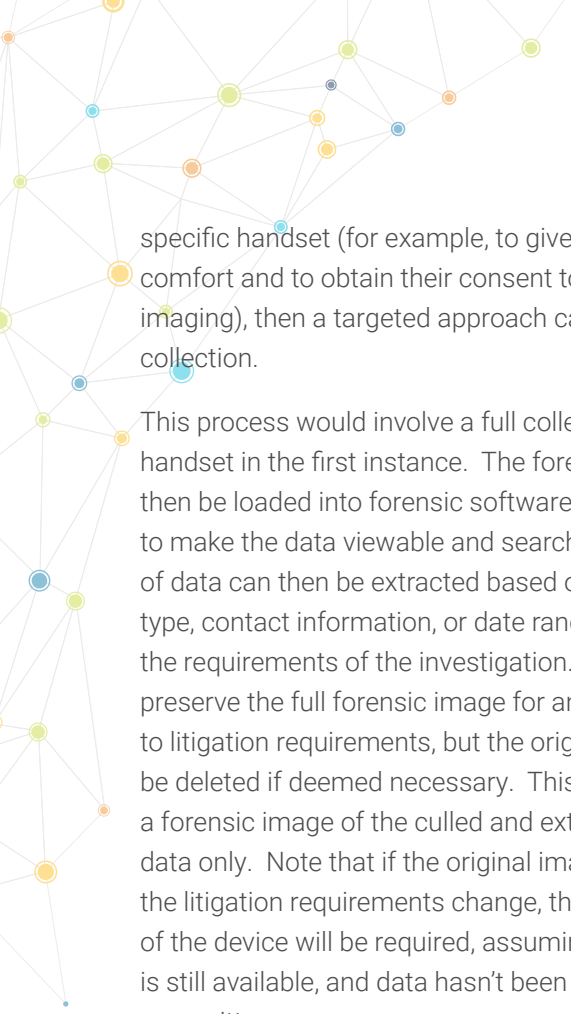
Determining what data can or cannot be extracted from a mobile device can be tricky, as capabilities differ across makes and models of devices, and it is unlikely that one can know what specific applications are in use on a particular user's handset before communicating or visually verifying on the device itself. Applications generally fall into two main categories: stock applications and third-party applications.

### Stock Applications

At a high level, applications that come pre-installed on a mobile device when you take it out of the box and power it on, such as Contacts, SMS, MMS, Calendar, Photos, and Video, will typically be extracted from the handset during a standard imaging process using forensic tools. These applications are known as "stock" applications.

When dealing with stock applications, unfortunately, it is not possible to be selective at the point of collection. It is not possible to simply extract SMS data or call data alone. The entire device must be imaged and processed before any culling or selective exports can be conducted.

If during your investigation it is deemed necessary to exclude certain types of application data from a

A decorative network diagram in the top-left corner of the page, consisting of various colored nodes (blue, green, orange, yellow) connected by thin grey lines, forming a complex web-like structure.

specific handset (for example, to give a user more comfort and to obtain their consent to mobile device imaging), then a targeted approach can be taken post collection.

This process would involve a full collection of the handset in the first instance. The forensic image would then be loaded into forensic software and processed to make the data viewable and searchable. A subset of data can then be extracted based on application type, contact information, or date range, which meets the requirements of the investigation. It is advised to preserve the full forensic image for any future changes to litigation requirements, but the original image could be deleted if deemed necessary. This would result in a forensic image of the culled and extracted device data only. Note that if the original image is deleted and the litigation requirements change, then a recollection of the device will be required, assuming the device is still available, and data hasn't been inadvertently overwritten.

A list of applications installed on the device will also be created as a result of a standard forensic imaging process. The installed application list can be a good starting point when determining what applications were commonly or previously utilised by a user. This list can shed light on potential sources of cloud-based mobile device data, where standalone collections could be conducted to obtain material potentially relevant to your matter.

It is also worth noting that the installed application list may indicate applications that are potentially no longer present on the device, possibly as a result of being uninstalled by the user. This may highlight further areas where data collections might be required through secondary sources, such as a web-based version of the application.

### **Third-Party Applications**

Third-party applications, which are applications that the user downloads onto the handset using facilities like the Apple App Store or Google Play Store, may or may not be extracted from the handset during a standard imaging process using forensic tools.

Some third-party applications store data within the cloud as opposed to the physical handset itself to save space on a user's device. A good example of this is the Google Photos application. This app allows the user to browse photographs they have stored in their Google account from their mobile device (or any device they log into), however, the photographs are not physically stored on the handset. As a result, data from this application would not be extracted from the handset as part of a standard imaging process using forensic tools. Applications that store data within the cloud require separate standalone collections to be able to extract the relevant data.

To add a little more complexity, even if third-party application data is stored on the physical handset and not in the cloud (e.g., as with the Signal app), data can be encrypted, or preferences can be set by the app developer to dictate whether data from the application can be backed up or extracted using forensic tools. This is often used as a function of data security. Banking or medical applications are good examples where this type of security feature is usually present.

Developers of these application types typically encrypt the data, or simply do not allow the data to be backed up, as a means of adding an additional layer of security. This results in data that cannot be extracted from a mobile device using forensic tools or collected through standalone methods. Communicating that these types of applications which contain personal or secure data cannot be captured, can be comforting to users of mobile devices when confronted with litigation requirements.

In comparison to stock applications, where culling is not possible pre-collection, third-party applications may offer a more selective approach. It may not be necessary to image a user's entire handset if the matter is focused on one cloud-based third-party application, such as the WhatsApp messaging application. Although WhatsApp data is stored on the handset, it is also possible to access the data



by linking the mobile device to the web version of the application and utilizing the web browser as a tool to view the data. It is possible to connect forensic tools to the account and capture this application's data. The encrypted messaging application Telegram also allows for selective imaging.

In short, the action of backing up or imaging a mobile device would only capture stock applications, as well as third-party application data that is stored on the

physical handset, that is stored in an unencrypted format, and that the application developers have allowed to be included in a mobile device backup. It may be necessary to image an entire mobile device to be able to obtain certain application data, and this will be certainly the case when dealing with stock application data. However, it may be possible to capture some third-party application data without imaging the entire handset with forensic tools.

## I QUESTIONS TO ASK MOBILE DEVICE CUSTODIANS

There are a huge variety of mobile devices and applications that can be utilised by a mobile device user. The device type can directly impact whether an application's data can be extracted with standard mobile phone imaging, and data may or may not be directly stored on a device. It is important to

consult with users to understand what type of devices and applications are being used to ensure that data collections can be conducted in the most appropriate, defensible, and forensically-sound manner.

### Ten questions that should be asked when consulting with the user of mobile devices:

1. How many mobile devices do you have and use for business?
2. Are your devices iPhone or Android or other?
  - ▶ Obtain the exact make and model of each device if possible.
  - ▶ It is also helpful to obtain the capacity of the device *i.e.*, a 16gb iPhone or a 128gb iPhone.
3. Are your mobile devices company-owned or personal?
  - ▶ It is helpful to ascertain if the company manage the device in any way. Do they have Mobile Device Management (MDM) software installed?
4. How long have you had these devices?
5. Do you ever back up your mobile devices, and if so, how?
  - ▶ If yes, are backups encrypted?
6. Do you migrate your mobile device data to your new device when upgrading your handset?
  - ▶ If you do not migrate your data, what do you do with your legacy devices?
7. Do you use email on your devices for business, and are these business email accounts or personal email accounts?
8. Do you utilise any messaging applications on your device for business, such as: SMS, iMessage, Telegram, WhatsApp, or Signal?
9. Do you utilise any other applications on your devices for business?
10. Do you create or store documents on your device?

The aforementioned questions will assist digital forensic specialists with the compilation of a workflow tailored to the specific device type and applications in scope for the collection. Seeking advice from experienced eDisclosure experts is advised. Experience, guided workflows, and assistance with technical consulting is invaluable at the outset of any litigation journey.

### Post-Collection Considerations

Generally, mobile device data is stored in a number of databases and system files that would not be easily reviewable without the assistance of specialist tools and technology. The data extracted from the device can be reviewed within an eDiscovery tool such as Relativity only once the data has been processed and formatted in a logical format.

Using specialist tools, it is possible to split text or chat messages extracted from a mobile device into threads running daily or weekly in a format that is easily reviewable and redactable. However, as discussed, some third-party applications may not be included in a standard mobile phone collection and may require

standalone collection directly from the cloud.

Third-party applications do not share a standard export function across the board. Export options and metadata extraction can vary. When dealing with third-party applications it is important to work with your eDiscovery provider to ascertain impacts to time and cost and to understand how best to review the collected data.

### Conclusion

Multiple factors need to be considered when mobile device data is in scope for collection. There are many varieties of mobile devices and numerous applications available to users. The type of device and applications utilised will directly impact how data can be extracted and how the data can be reviewed and produced. Consultation with the user or business owner is vital to obtain as much information as possible ahead of the collection exercise to ensure that your eDiscovery provider can create a tailored solution and advise on the best sources for collection whether that be from the device itself or a cloud-based application.

## ABOUT THE AUTHOR

Sophie is a Senior Director at Consilio, a global leader in Legal Consulting & Legal Services. Sophie runs the digital forensic and expert witness teams across Europe and APAC and has been working in the digital forensic industry for more than a decade. She holds a degree in computer forensics and is an EnCE certified computer forensic examiner, who is also a certified counter fraud specialist. She has worked on a variety of high-profile criminal and civil cases and has assisted in over 400 criminal and civil cases in the United Kingdom covering cases involving harassment, murder, child pornography and fraud. She has been independently responsible for the collection, preservation and analysis for digital evidence retrieved from electronic media, as well as producing technical reports on the findings for law enforcement, corporates, lawyers, and independent parties.

Sophie works with Consilio's clients from the outset of any given matter, to assist with data mapping and scoping. Sophie provides advice of the most efficient and cost-effective preservation/collection methods and offer her services as an expert witness.



### Sophie Beattie, EnCE, CDFE, Certified GDPR Practitioner

Senior Director - Forensic Investigation and Expert Witness Services

**m** +44 (203) 808.9622

**e** sbeattie@consilio.com

[consilio.com](https://www.consilio.com)