

SIM Cards

The Essentials

There are more mobile telephones in the UK than there are people – this pervasive technology impacts on almost all areas of industry and life. Unsurprisingly mobile communications have enabled old crime to be effected in new ways and mobile telephones are increasingly forming a part of criminal prosecutions, where linkages between individuals or evidence of being at the scene of the crime is provided by an analysis of the digital evidence available within the mobile phones.

At the heart of every mobile telephone is the [Subscriber Identity Module](#) (SIM), a small fingernail sized chip, responsible for service with a telecom network provider.

Digital Evidence

Despite limited memory capacity, the SIM contains a wealth of information that, when considered in context, can greatly aid solicitors in their case preparations:

- Stored telephone numbers/contacts;
- Listings of 'Last Dialed Numbers';
- Text messages received, sent, drafted or deleted;
- General location information from last use;
- References to overseas network providers that have been used.

Common Questions

Could the SIM card have been cloned?

SIM cards produced after June 2002 employ the [COMPv2 algorithm](#) which provides a number of technical and security safeguards to prevent unauthorised modification. Despite media reports, the cloning of modern SIM cards is an extremely rare practice.

Can my PIN code be cracked?

SIM card information can be locked using a four digit 'Personal Identification Number'. [RIPA](#) contains provisions to force disclosure of passwords, however, it is usually easier to request a '[Phone Unlock Key](#)' (PUK), enabling PIN settings to be overridden, from the Data Protection Officer (DPO) at the relevant network provider¹.

PAYG SIMs are untraceable!

With 'Pay As You Go' (PAYG) there is no formal contract with a network provider (e.g. Orange) to enable a customer look-up, however, 'Call Data Records' (CDRs) are still available from the network provider, providing information as to patterns of communication, calls to/from, time/dates etc². By mapping this information to known acquaintances of the defendant, considering the evidence in the context of other material (such as messages recovered from the telephone handset) and undertaking [Cell Site Analyses](#) (CSAs)³ it is possible to prove/disprove ownership of a handset.

¹ It is not recommended to force the data off a locked SIM – this can permanently damage the card and the resultant data extracted may be corrupted and thus inadmissible in court.

² Note that CDRs contain traffic information and do not contain content data. For instance, it can be shown that a text message was sent from mobile number 123 to mobile 789 at 2:37pm on Wednesday 15th June, but the textual content from that message is not stored or available.

³ Cell Site Analysis (CSA) is the process of mapping the relative geographic positions of a mobile telephone handset using information relating to the network base stations that the handset communicated with at a point in time.

Does the SIM reveal who I've been in touch with?

Even without the disclosure of Call Data Records (CDRs) from the network provider, the SIM provides a plethora of useful information relating to contacts in the form of 'Last Numbers Dialed' (LND) and sections of the 'Contacts Directory'. Numbers that haven't been saved may still show up in the LND.

Can a telephone handset be uniquely identified?

Mobile phone handsets are assigned unique 15-digit numbers, known as the [International Mobile Equipment Identifier](#) (IMEI), which is passed to the network provider before communication services can be utilised. This serial number allows specific handsets that have been stolen or blacklisted to be blocked from a network irrespective of what SIM card is inserted. Defences suggesting that a given handset has been 'found' and is not owned by the suspect are unlikely to hold water if Call Data Records (CDRs) show a pattern of usage that indicate the owners identity.

Sending anonymous texts

Are not really that anonymous... If they are being sent via an internet service, there is typically a log retained by the site provider as to the computer IP address that sent the specific message – this can ultimately be tied by to an Internet Service Provider (ISP), and in turn a specific subscriber. If anonymous texts have been sent from a mobile telephone – typically a PAYG handset/SIM – the uniquely assigned [International Mobile Subscriber Identifier](#) (IMSI) code embedded in the SIM can be used in concert with CDRs to provide compelling evidence as to the sender identity.

Can deleted text messages & numbers be recovered?

Data content (especially multimedia formats) is primarily stored on the handset or on a removable memory stick. The general rule of thumb is that any data that has been deleted can be recovered, however, if it has been over-written it does make the process more complex and the chances of success reduce with every over-write.

Is possession of multiple SIM cards indicative of wrongdoing?

Not at all - many individuals are discovering that they can benefit greatly from the free text and talk allowances granted on mobile phone contracts by having two or more SIMs (typically with different network providers). [Adapters are available](#) to connect multiple SIMs to a handset simultaneously.

Did you know?

The SIM card will often contain a reference to the last network base station that it communicated with before being disconnected from the telecoms network.

If the SIM card has been used overseas, it is possible to retrieve a reference code from the card that will indicate which national/regional network provider was used.

Language preferences can be stored on SIM cards – useful intelligence for investigators which can open up new avenues of enquiry.

Find out more...

- [Digital Evidence from Mobile Devices](#) – MS PowerPoint presentation
- [GSM Technical Specification & Tutorial](#)
- [History & Evolution of Mobile Telephone Communications](#)
- [GSM Security & Privacy Controls](#)