Can mobile phone records really offer your defendant a get out of jail free card? **Duncan Campbell** reports

Roaming charges

After an evening watching *Wired* or *CSI* – or, less convincingly, *Spooks* – viewers could be forgiven for thinking that mobile phones now provide instantly available and complete records of every user's position and actions.

Although the day when that happens is not far off, the digital age has not yet fully evolved into the transparent prison that 18th century philosopher Jeremy Bentham styled the 'panopticon' (a ubiquitous structure of observation and recording of movement and activity).

Answers to critical evidential questions are occasionally a keystroke or button push away, but most real-world cases are more complex and less tractable.

The welter of data generated in and from increasingly complex modern mobile phones has to be interpreted carefully, sometimes using a blend of art and forensic science. By 'art' I mean that successful analysis and convincing evidential results can on occasions better emerge from understanding the social and geographical spaces in which players and events are interacting, and testing these against competing hypotheses put forward by the adversaries, than from dry and mechanical analysis of data in the manner of a sausage machine.

A substantial forensic scientific industry and a host of new analytical disciplines with accompanying software and hardware have evolved over the last 15 years to deal with the digital mountains of call data records (CDRs) and data from phones that have to be drilled down into meaningful analyses to be made relevant to the issues in a case.

Increasingly, convergence between computers (especially wireless equipped laptops) and new generation smartphones with broadband data access built in, means that many phones are now fully fledged computers in their own right. This article focuses principally on communications aspects of digital evidence.

In any contemporary criminal investigation, digital media and devices which were once disregarded in search training courses have taken on paramount importance as sources of evidence as to who knows who, associated when, and perhaps some messages they exchanged. For 15 years, first as undisclosed intelligence but since about 2000 as admitted evidence, evidence from mobile phone networks has included data about the location(s) from which calls are made and received. Information is now supplied automatically over the internet from communications service providers to specifically trained and designated officers in organisations authorised to request communications data under the provisions of RIPA 2000. The receiving office is designated the single point of contact (SpoC). No other personnel are trained for or permitted to download communications data. The volume of requests made annually now exceeds half a million a year.

Interception

The information made available is call-related information only, such as times and dates, and calling and called parties. In the UK, the contents of calls and text messages, as they are transmitted and received by networks, are protected from all interception and analysis, save when a secretary of state has granted law enforcement or intelligence and security agencies a lawful interception warrant.

No such restrictions apply if the voice conversations or voice or text messages have been recorded at one or both terminal devices (whether phone or computer). The journalists and others now awaiting possible trial in the newspaper hacking scandal relied on the dubious doctrine that re-recording a recorded voicemail message, to which unauthorised access was obtain by using the legitimate user's compromised PIN, was not in breach of RIPA or other criminal law.

This view, adopted previously by the CPS, has been overturned by Attorney General Keir Starmer, leading to a hugely enlarged set of police investigations. The resulting cases may establish that the alleged practices breached the Computer Misuse Act, but may not affect many other criminal investigations or prosecutions.

Where lawful interception has taken place in the UK, the results of the interception cannot be disclosed or used in evidence. Questions put by defence representatives as to whether interception has occurred cannot lawfully be answered. Perversely, intercept evidence of UK telephone calls has been judged admissible if the tapping took place overseas. This practice has led to strange evidential practices and complex in chambers and ex parte arguments in several major UK narcotics distribution cases.

In a 2005 case, a group of alleged cocaine importers received substantial sentences based in part on mobile and landline phone intercepts said to have taken place entirely in Colombia. Their convictions were challenged on the basis, in part, that the chain of evidence for some of the Columbian intercept evidence was as at least as irregular as shipping methods used by narcotics distributors. After a series of appeal hearings, and rather than disclose the true source of their intercepts, the Crown withdrew its evidence, resulting in all convictions being quashed.

Evidence at trial

Even without the content of calls being available, analyses derived from communications data can range from simple demonstrations of association (e.g. A has exchanged calls or messages with B) to more complex analyses integrating call and geographical records analyses in detailed charts, sometimes called 'Anacapa' after a long-standing FBI practice. The analyses performed can include link or traffic analyses which automatically turn large volumes of information into clusters or pinwheels, suggesting and highlighting significant communications paths at significant times.

Increasingly sophisticated presentational tools are now in regular use, notably the widely used and costly British-American i2 charting system. These workhorse programs can be used to sort and sift large quantities of data, producing elegant results. The resulting charts and presentations can be beguilingly colourful and seductively definitive. More

recent programs have offered 3D virtual images of the march of time and events uncovered in an investigation.

If extended beyond a few hours, the presentation of such evidence at trial often challenges jurors' endurance and ability to reach a fair verdict. There is also potential inequity of arms, as the software used to generate the charts is prohibitively expensive for non-government users, often making it a financial and professional near impossibility to fully check charts or test alternatives.

Solicitors for criminal defendants are often confronted late in the day and shortly before trial with a vast array of call data record printouts, coupled with forensic reports and maps on the potential coverage of dozens of cells used over the time of the alleged offence(s).

When it has been possible to fully check analyses in some criminal cases, elementary and misleading errors have come to light. Simple counting errors by analysts, such as counting short and failed calls or text messages alongside significant and effective calls will generate highlighted and significant links which can vanish on cautious and careful analysis.

Often, data that is left out of an analysis on the basis of undeclared assumptions may be more significant than what is included. Such approaches are inherently unscientific. They happen nevertheless.

In a significant number of cases, especially in the earliest years of cell site evidence, practitioners carried out only minimal tests as to whether cell sites used might be 'consistent' with a prosecution case. It would be mischievous to suggest that this was merely asking whether the evidence could be trimmed to fit the case, but it can easily appear so. A better approach is to identify critical areas of interaction between the players, the locale and the digital evidence, and to document the range of possibilities.

At trial, evidence of the sequence of cell sites or 'mast' locations used can be highly probative of the guilt or innocence of an accused. The effective range of transmitters in the first generation digital phone network was fixed to have a range not exceeding 35km. Thus, if the geographical divergence between locations claimed in the prosecution case and defence alibi is greater than 35km, relevant call data records can be and have been decisive.

In a northeastern case, a defendant accused of participating in a murder in Leeds pointed to his use of several cells in Tyneside at the time of the offence. The records concerned had been produced by the prosecution and were not challenged. The defendant was promptly acquitted.

In an appeal against a murder conviction in 2005, the appellant asserted that he had been in Leicester at all times, including when it appeared the victim's body had been dumped in a Birmingham canal. Relevant cell site records supported this claim – save for one at a time soon after other forensics suggested the body had hit the water. This call had been made using a cell which provided some coverage to the motorway between Birmingham and Leicester, but which did not cover Leicester. The conviction was judged not to be unsafe.

In a widely reported Sussex celebrity murder trial, experts for the prosecution could offer no explanation for calls at highly significant times, shortly before the victim was murdered, and, later, when her body was dumped in Sussex woods to lie undiscovered for four months. The cell site data apparently put the victim in Kent and the murderer in Brighton at times when, on the indictment, they had to be together.

Evidence at trial also included a claim by the murderer that his (already) deceased wife was alive and travelling by car to London while he journeyed by train. The wife's phone had been used during the journey. The prosecution established that the wife's phone accessed cell sites covering the rail route and not the road, disproving the claim and suggesting that the murderer had operated her phone. But they were unable to explain the mystery calls located to Brighton and Kent.

The lacunae would have been solved had the investigators not relied on survey drivers to mechanically gather data, and visited the scenes associated with the crime. And had they taken walks in the woods, some way from the roads used by their survey drivers. In both cases, there were 'hot spots' of unusual radio strength nearby, which were likely to have been served by the Brighton and Kent transmitters. Bizarrely, the hot spots were like searchlights on significant places, including the track where the body was found.

Similar unusual features can often be found in urban environments, where the many stations and multiple pathways between users and base stations can result in a different analysis if a bus was passing by, or if a person walked one way or the opposite way down a street.

Communications data apparently putting an accused at a robbery or assault scene can produce wholly different conclusion when field measurements are compared with paper predictions.

The amount and likely accuracy of such data is likely to grow exponentially over the next few years. Commercial pressure for the deployment of location-aware mobile phones means that within the next decade it may be nigh impossible to have a device that it is not recording and, given the chance, transmitting a user's moment to moment location over the internet to central data repositories.

Historical cell site analysis

Rather less precise data of this kind first became available in the mid 1990s, when investigators suggested that the mobile phone companies records of which transceiver stations, or cell sites, had handled users' calls could point to their possible or probable location at critical times. This forensic method, known as historical cell site analysis (HCSA), started to be used openly in prominent cases such as the Omagh bombing enquiry and the 2002 Soham murders of schoolgirls Jessica Chapman and Holly Wells.

To use HCSA, investigators have to apply to one of the UK's four private mobile companies for call data records (CDRs) which show, for a specified period and a specified target number, what calls or messages were made or attempted. If asked specifically, the companies will include the identities of the cells used.

There is no standard across the industry. Some of the companies will normally record details of incoming as well as outgoing calls; some do not. One company records cell site locations at the start and end of each call. Some include locations used to send or receive messages, or when the phone is connected to or disconnected from the networks.

Defence teams and parties to civil cases can also apply for and use the same data, but have to rely either on Data Protection Act requests by users, or on an application to the court.

Other than firms representing News International or the victims of its irregular journalism, solicitors are unlikely to experience cases that involve hacking in the style revealed in recent reports and claims. Voice records of recorded phone messages are not maintained by networks after a few days, and are not available later even in response to official requests.

The recent forensic discovery that Apple iPhones automatically log their users' complete geographical movements without their knowledge and consent (even if the user has selected not to reveal location to others), and then load the data files to the Apple's iTunes program required on associated computers was not a complete surprise. But it is a harbinger of the future of enquiries and cases.

Duncan Campbell is a forensic expert witness on computers and telecommunications and an investigative journalist. Contact: iptv@gn.apc.org