The use of evidence generated by software in criminal proceedings

Response to MoJ call for evidence

Peter Sommer

1. This is a response to the Call for Evidence of 21 January 2025[1] . I argue that if long term solutions to the problems of using digital evidence in criminal proceedings are to be addressed the scope of the Call should be extended. I set out the current sources and forms of digital evidence and how they are processed before they are presented as exhibits in court. Chief among these are smartphones. Important data is obtained from online services while other data must be retrieved from cloud services. There is increasing use by law enforcement in the use of analytic and processing software. I review the means for testing reliability and determining what "reliability" means. My recommendation is against any new statutory admissibility test in favour of Codes of Practice supported either by existing legislation or Practice Directions. This route provides detail and flexibility; a requirement on tenderers of digital evidence to complete a questionnaire should reduce some disclosure problems. There are ways to improve the quality of digital evidence which do not involve legislation. Further judicial training and the availability of experts are additional concerns.

Scope

2. The call for evidence says: "We are keen that any changes to the current common law presumption are carefully defined to only include that evidence which is generated by software… We believe that evidence which is merely captured or recorded by a device should be

---

[1] https://www.gov.uk/government/calls-for-evidence/use-of-evidence-generated-by-software-in-criminal-proceedings/use-of-evidence-generated-by-software-in-criminal-proceedings-call-for-evidence#:~:text=Current%20principles%20around%20the%20use,is%20evidence%20to%20the%20contrary. In essence, what sort of replacement for the current rebuttable presumption that computer evidence is reliable?

excluded…. We welcome views on if these are the right boundaries, how these definitions should be drawn, and other examples of specific evidence types which should be in or out of scope."

3. Three of the examples of evidence potentially to be excluded are entirely capable of being presented in court while having substantial issues of unreliability. By "unreliability" is meant of appearing to be accurate and complete records of activity when they are not. They are: digital communications between people such as text messages, messages sent through web-based messaging services, social media posts, emails, digital photographs and video footage, and mobile phone extraction reports.

4. Increasingly crimes take place within remote online services such as websites and social media platforms. They include frauds, the spreading of terrorist information and other incitement material, the spreading of CSAM and harassment. In some instances cybercriminals have used remote cloud-hosted computers from which they have carried out activities such as large-scale computer intrusions. Significant crimes take place on the dark web, where evidence collection presents particular problems.

5. There are two main sources of error in those cases where the devices are located within UK jurisdiction and hence available for investigation: the methods used to extract and preserve the data from their original locations on the digital devices where they were located; and the subsequent processing by technicians and investigators in order to render them into forms suitable as exhibits in criminal proceedings. Both of these activities involve the use of specialist and potentially questionable software, some of it created for specific purposes during an investigation. Both these classes of software - acquisition/extraction/preservation and analysis - undergo frequent revises as the source devices are improved and upgraded and in the light of ongoing research by digital forensics academics and technicians.

6. Further problems relate to potential evidence which is online. In some instances it is possible to get the owners of services to provide material together with supporting witness statements.[2] But in others UK investigators have to attempt to collect the data direct online by executing commands including downloads and screen captures via a regular computer terminal. There are, at the moment, no standard procedures for ensuring that this is done safely and reliably. Among the problems is that data is being captured from live, running systems.

---

[2] It may be necessary for UK authorities to make use of MLATs, ILORs and the CLOUD treaty.

7. There is also the extent to which law enforcement uses software to combine various types and sources of evidence – digital, conventional and human testimonial – in order to build sequences of events. These tools are used not only for investigatory purposes but also to generate exhibits for court use. The product of these tools may be highly persuasive as they are graphic in nature but also misleading through unreliability.

8. As the aim of the Call is to decide the extent to which new primary legislation is necessary the danger is that new laws include definitions which do not reflect actual investigatory and prosecution practice. If the legislation includes an element of admissibility tests the danger is that poor framing of definitions leads to some types of evidence becoming excluded. There is a further danger which needs to be incorporated into policy formation: the limitations of the current Forensic Science Regulator and the tests being required under the current Code of Practice.

9. I will endeavour to address the questions in the Call but follow my own order.

Features of Computer-derived Evidence

10. Computer print-outs tendered as exhibits in evidence in litigation do not appear spontaneously. They are the product of decisions that it would be helpful to have a computer program to collect data, process it and present the results in useful ways. The concept of the computer program has to be turned into a detailed specification of what is expected of it and to identify wanted but also unwanted outcomes including flaws and security breaches. The specification is then subjected to coding, and the coding needs subsequent careful testing. Once in existence the program has to be managed within a human environment and run on available computer hardware and communications links. The data fed into the system has to be established as “clean” and “reliable”.

11. Most modern systems are not static, they are subject to constant improvements, and these new features require testing as well.

12. What is produced in court is a curated selection from the data processed by the resulting program.

13. In many circumstances computer-derived evidence can be trusted in assisting a court to reach legally-effective decisions, but when there is

doubt there is no option but to examine how a print-out exhibit came into existence.

Features of current Digital Evidence in criminal investigations and proceedings

14. The MoJ Call seems to be most interested in the situation where a single large computer system owned by an organisation produces computer output which is unreliable and as a result of which miscarriages of justice occur. The most obvious recent example of this is of course Post Office Horizon[3]. It is also the situation that appears to have been envisaged in the 1995-1997 Law Commission reports which gave rise to the current state of the law. Horizon was rolled out in 1999 and the first problems started to appear in 2000. We are thus concentrating on the preoccupations of a quarter of a century ago. Much has changed since then and although some of what appears immediately below will be familiar to many readers it is helpful to set them out so that the problems of revised doctrines of digital evidence reliability can be more fully addressed. The changes apply not only to the types and sources of digital evidence but how they are processed by law enforcement. A more useful case study of the variety of digital evidence and the associated reliability issues is provided by NCA Operation Venetic and EncroChat encrypted smartphones – see Appendix II below.

15. It is suggested that every "average" UK home has between 13 and 28 devices which contain some forms of digital evidence.[4] The NPCC *Digital Forensic Science* Strategy *2000* said that over 90% of all crime has a digital element.[5]

16. The most obvious of the "new" sources is the **smart phone**. The first Apple iPhone was launched in 2008; Android phones started to appear in 2013. At the start of 2022, there were 71.8 million mobile connections in the UK (4.2 million more than the UK population because many people have more than one handset)[6]. These devices are with their owners 24/7 and collect and contain many different types of highly personal and detailed potential

---

3 https://www.postofficescandal.uk/about/

4 https://www.statista.com/statistics/1107269/average-number-connected-devices-uk-house; https://www.nationalgrid.com/our-love-electric-research-reveals-uk-obsession-all-things-electric#:~:text=In%20fact%2C%20according%20to%20the,76%25%20and%2075%25%20respectively.

5 https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf

6 https://www.uswitch.com/mobiles/studies/mobile-statistics/

evidence – phone calls made and received[7], content of SMS text messages, social media messages and postings, photos, videos, notes and other documents. There is the task of the safe acquisition of as much of this material as possible plus hidden-from-the-user technical, configuration files and metadata which might assist in the reconstruction of events. Once the content of a handset has been acquired and preserved there are the tasks of examining the various files associated with particular types of activity - the raw "dump" of a phone is too voluminous to present unprocessed to an investigator let alone a jury. Each type of data within files associated with features and apps will require separate treatment in order to render it human-readable. Given the size of files they will require further processing refinement in order to find material of potential relevance to an investigation and eventual potential criminal charges.

17. **Integrated software** is used to achieve these aims by the likes of Cellebrite, Oxygen Forensics and Magnet AXIOM. Particular disciplines are required of technicians to avoid contamination during acquisition and to ensure complete download. Many "first stage" examinations are carried out using kiosks which automate many processes and can be used by less skilled staff[8]. In some investigations the results are immediately turned into exhibits for court use. The tools need to be updated frequently to reflect the appearance of new models of handset, new and revised versions of apps and new versions of operating systems – Android appears in formal new versions annually as does Apple iOS. The frequency of change on the handset, the constant updating of content and the consequential need for the forensic acquisition and examination software to keep up means that there is never a point at which smartphone evidence can be said to be presumptively "reliable" in any reasonable sense. It may nevertheless have probative value when considered with corroborating material, a theme explored later.

18. Smart phones and indeed older mobile phones generate another source of digital evidence – geolocation. This appears in the form of **Call Data Records** (CDRs) produced by mobile phone companies which include timed details of registrations and links to mobile phone masts. These are used in cellsite analysis which shows the movement of handsets and their owners over time. While there is now little doubt about the reliability of the CDR data[9] converting it on to maps requires reliable software and careful interpretation. The Forensic Science Regulator's guidance[10]

---

7 That calls were made but not usually their content

8 https://www.msab.com/products/platforms/; https://www.adfsolutions.com/; https://detegoglobal.com/mobile-forensics-tools/; https://www.bbc.co.uk/news/uk-scotland-51110586

9 This was not always the case but following a Home Office study clear procedures are now in place.

10 https://www.gov.uk/government/publications/cell-site-analysis

indicates the problems due *inter alia* to propagation and terrain and that the GSM network of masts is constantly being upgraded. As before, doubt about reliability may be overcome if there is corroboration from other sources of evidence.

19. Similar considerations apply to **personal computers, laptops and tablets**. These do not (usually) have connections to the telephone network for calls and SMS text but they do have access to Internet traffic. The way such devices are used, the range of software applications and the large quantities of local storage make these an invaluable source for investigators. Operating systems such as Windows have minor but potentially significant changes every 2 weeks as a result of manufacturer modification and corrections; most PCs will have malware detection software with daily updates to their signature database.

20. The analytic software used for PCs such as EnCase, FTK, X-Ways, Belkasoft attempts to provide a single platform upon which to identify and read the many different types of file and artefact generated during the daily operation of the PC. Artefacts include the PC registry, Internet history files, deleted but recoverable files and file fragments. With few exceptions the simple identification of a file is insufficient to satisfy the needs of a successful prosecution. As a common example: the discovery on a device of CSAM is enough for a "possession" offence under s 160 Criminal Justice Act 1988 as it is strict liability with the onus on an accused to prove one of a limited range of legitimate defences but the "making" and "distribution" offences under the Protection of Children Act 1978 require an examination of applications on a PC, time and date stamps on the stored images, possibly an examination of the Internet history associated with a browser and also possibly the review of any file-sharing software. As another example unauthorised access to a computer under Computer Misuse Act 1990 will seldom be demonstrated by the discovery of a single file. A reconstruction of events will require a review of many files including those that did not originate on the PC being examined. Forensic software may assist such investigations.

21. It should be noted that some of the digital forensic analysis software suites also allow investigators to write their own additional facilities in the form of "scripts". These can be very useful during an investigation but of course will initially be wholly untested and hence potentially unreliable.

22. **Link Analysis** software products are invaluable investigatory tools which combine many different forms and sources of evidence to create a more

complete picture. [11] The earliest such tools were able to map telecoms data showing phone calls in order to demonstrate the existence of possible conspiracies. More modern variants can map out narcotics county lines consisting of importers, wholesalers, distributors, couriers and end-sellers. Another use is in fraud investigations.

23. But once the investigation is over the products make vivid exhibits for court use. There are two issues – the quality and completeness of the data fed into the link analysis tool, and the way in which the tool can be trusted to perform reliably.

24. **Excel-created exhibits** A frequent tool of investigators is Microsoft's Excel spreadsheet. Data from various sources, including CDRs, is fed into Excel and then use is made of Excel's analysis facilities for sorting and creating charts. However it is all too easy for mistakes in data input and choice of formulae to occur but still produce output with the veneer of plausibility[12].

25. **Other Local Digital Evidence Sources** Further digital evidence sources are available to law enforcement officers via production orders, typically via PACE 1984 Schedule 1 paragraphs 4 and 5. Depending on circumstances these can become primary exhibits or used in collaboration with other forms of regular and digital evidence. Here are some examples, grouped on the basis of levels of presumptive reliability:

    a. **Very limited function computer devices** These include counting, weighing and measuring devices and where the computer activity is largely in hardware[13] which cannot be readily altered or contaminated. The outputs of these devices are likely to be highly reliable.

    b. **Relatively reliable sources because computer owners are well-established, computer systems stable and subjected to external audit**: These include financial transactions records from banks, etc, records from automatic teller machines (ATMs), records from point-of-sale terminals (PoS), telecoms CDRs, travel records activities, Automatic Number Plate Records (ANPRs), ISP/CSP records, including subscription data. logons to services and IP addresses/RADIUS logs

---

11 https://cambridge-intelligence.com/use-cases/law-enforcement/, https://i2group.com/law-enforcement, https://www.kaseware.com/link-analysis, https://www.cognyte.com/blog/link-analysis-software/, https://chorusintel.com/us/, CSAS, Belkasoft X, FTK

12 https://sheetcast.com/articles/ten-memorable-excel-disasters

13 Such as via the use of PLDs and FPGAs, Intoximeters, physical access control systems

c. **Sources where reliability depends on quality of management of computer systems**: These will typically be transaction records from retail and online merchants and email threads[14]

d. **Sources where techniques for data extraction and analysis are still being developed:** Internet of Things devices, smart home devices, vehicular forensics

e. AI-generated data A distinction must be made between reliably-sourced data where AI has been used as a search tool during an investigation and data which has been generated by an AI engine[15].

26. **Video and Audio** Video and audio used to be analogue, recorded on to magnetic tape. Although these older systems still exist most video and audio are now recorded digitally. This includes material from CCTV systems and vehicle dashcams. It would be a mistake to regard these data sources as presumptively reliable. Editing is easy. At the very least full continuity should be expected – with the source devices identified, how the data was collected and preserved and any subsequent selection and processing. If there is in-built timing information the source of the timing will need to be stated as well[16]. On occasion audio and video enhancements may be called for and these need to follow verified procedures. We are beginning to see the use of generative AI to produce fake videos and audios; we lack the tools that can reliably detect these.

27. **Online Sources** Many forms of criminal activity take place online. They include distribution of CSAM and terrorist material, media and IP piracy, frauds, sale of illegal items such as narcotics, firearms and pharmaceuticals and computer misuse In some instances records will be found on the devices of those involved – social media postings, chat logs, photos, use of file-sharing programs, the results of web browsing. Most of these can become available via regular digital forensics procedures on PCs and smartphones. There are a number of tools specifically designed to discover web browsing history[17].

28. But some online evidence remains online and attempts have to be made to retrieve it from remote locations not capable of being seized by law enforcement. Not the least of the problems is that it means retrieval is

---

14 Single emails are usually regarded as insufficiently reliable as they are easy to forge; proper acquisition/preservation procedures usually involve capturing whole archives, together with header information

15 https://www.everlaw.co.uk/blog/ai-and-law/unlocking-justice-ai-evidence-analysis-forensics/; https://www.oxygenforensics.com/en/resources/digital-investigations-with-ai/ ; https://explore.bps.org.uk/content/bpsadm/16/1/42

16 Eg if the timing comes from external sources as the GSM stream or if it is set up by the device's installer

17 Digital Detective NetAnalysis, Hindsight, KAPE plus some more general purpose PC forensic tools

from a live system which is running and altering all the time. A second set of problems arises if the investigation is covert and steps must be taken to avoid detection. Software acquisition tools alone are likely to be insufficient and at the very least very careful documentation of the actions and processes used by investigators will be needed.

29. In some instances it may be possible to obtain the co-operation of service providers – Communications Service Providers, controllers of Social Media, Website owners. Usually a legal process will be required to secure consent and co-operation, not the least because the businesses involved will have contractual and data protection/privacy obligations to their customers. Once agreement has been obtained investigators are in the hands of these entities in terms of the quality and reliability of the methods used to produce the requested records.

30. For other circumstances investigators must resort to going online from their own PCs and attempting to download material they believe to be of possible relevance. There does not appear to be a generally-accepted set of procedures to be followed[18].

31. There are tools to download whole websites[19] but for social media investigators must either use such tools as have been made available by the particular social media or resort to screen capture tools[20]. There has been some coverage of the problems in academic articles[21].

32. The problems are particularly acute when attempting to acquire evidence from the dark web where narcotics, illegal pharmaceuticals and firearms are among the items on offer. Dark websites can only be reached via the TOR browser; most of the time the only tools available to the technical investigator is to take a succession of screenshots or to video a visitor session[22].

33. In all these instances the main route to persuading a court of the reliability of acquired material is immaculate documentation of the processes involved, giving a

---

18 Investigators will also need a legal basis for capturing the data, the more so if it is not regularly on public view

19 HTTrack Website Copier (https://www.httrack.com/), Website downloader (https://websitedownloader.com/)

20 Eg Windows Snipping tool, Snagit, Fireshot

21 *From 'Capture to Courtroom': Collaboration and the Digital Documentation of International Crimes in Ukraine* , Koenig (https://doi.org/10.1093/jicj/mqac046); *A Forensic Framework for Screen Capture Validation in Legal Contexts*, Greco & others, (https://ieeexplore.ieee.org/abstract/document/10679466); *Web Browser Forensics for Retrieving Searched Keywords on the Internet*, Dija & others (https://ieeexplore.ieee.org/document/9725457); *A Framework for Browser Forensics in Live Windows Systems*, Dija and others (https://ieeexplore.ieee.org/document/8524412)

22 https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/darknet.html; https://www.college.police.uk/article/investigating-dark-web-new-training-available

possible expert instructed by the defence the opportunity to review, test and comment.

Reliability in the context of digital evidence

34. In developing future policy we need to think carefully about reasonable expectations of "reliability" in the context of digital evidence. There have been a number of useful articles explaining the problem and which I expect are being referred to in other submissions to this Call: *The Law Commission presumption concerning the dependability of computer evidence* by Ladkin, Littlewood, Thimbleby and Thomas[23] , *Robustness of software* by Ladkin[24], *Recommendations for the probity of computer evidence* by Marshall, Christie, Ladkin, Littlewood, Mason, Newby, Rogers, Thimbleby and Thomas[25], *Evidentiary Treatment of Computer Produced Material: a Reliability Based Evaluation,* by Spencely[26].

35. As a very brief summary: all but the very simplest of software packages will inevitably contain flaws and errors of some sort. There are some statistics to demonstrate the typical extent of these errors[27]. Writers of software rely heavily on libraries of functions written by others – to create on-screen input and results forms, to provide searchable databases, to communicate with the outside world, to collect data from external devices, to perform encryption and decryption. No software writer can check the reliability of all these function libraries and even the task of checking how they interact in very challenging. A smartphone with apps may have 13 million lines of code.

36. The articles all criticise the presumption of reliability. An article by James Christie[28] visited a number of the consultees to the Law Commission's 1995-1997 paper *Evidence in criminal proceedings: hearsay and related topics* [29] and found that their views had been misunderstood and misrepresented. It is this Law Commission paper which has given rise to the current doctrine of presumptive reliability. Christie's article also contains useful analyses and descriptions of sources of error.

---

23 https://doi.org/10.14296/deeslr.v17i0.5143
24 https://doi.org/10.14296/deeslr.v17i0.5171
25 https://journals.sas.ac.uk/deeslr/article/view/5240
26 https://core.ac.uk/download/pdf/41230154.pdf
27 Eg Bird J: How many bugs do you have in your code? *Java Code Geeks.* 2011
28 https://journals.sas.ac.uk/deeslr/article/view/5642/5310
29 CP138: https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2015/04/cp138.pdf

37. It is sometimes assumed that whilst software may be unreliable hardware is usually bug free. This is not the case[30]. Hardware bugs may be a particular concern in software where there are strong iterative qualities such as some forms of AI.

38. The practical problem for relying on a stream of digital evidence at trial is whether it is *sufficiently* reliable for the purpose to which it is being put. The reliability of digital evidence is not a binary concept, either reliable or not.

39. The difficulties for courts are at their greatest when there is reliance on a single stream of digital evidence coming from a single computer device. This was the position in the various Post Office Horizon cases. But there are often situations in which there are multiple sources of evidence, computer-derived, "real"[31] and testimonial. Here less intrinsically reliable digital evidence may acquire strong probative value because it can be corroborated.

40. The notion of evidence corroboration in criminal trials is hardly novel. There may have been a complex series of events viewed by a number of witnesses none of whom saw the entire circumstances and who had different perspectives. A careful reconstruction can show sufficient overlap so that a court can have confidence in being sure about what happened. This is how some of the defects in the EncroChat evidence in Operation Venetic cases were overcome in trials[32].

41. In a criminal trial the task of the prosecution is to prove to a court's satisfaction that an accused was responsible for events that took place and which amount to a criminal offence. The issue of the reliability of the elements that go to show that the events occurred are steps along that path.

Practicalities in Evaluation of Reliability

42. It is now helpful to look at the some of the routes to assisting a court in evaluating reliability.

43. Unless the digital evidence can be regarded as speaking for itself the most obvious means are the **expert witness statements** from the prosecution

---

30 https://sigops.org/s/conferences/hotos/2021/papers/hotos21-s01-hochschild.pdf, https://www.eejournal.com/article/hardware-bugs-afflict-nearly-all-cpus/; https://hal.science/hal-04577494/document

31 In the sense of real evidence, physical objects which can be said to speak for themselves

32 See Appendix II

and, should they decide to tender any, from the defence. The relevant Practice Direction is in Part 19[33]. 19.4 specifies the content of an expert's report [34]. Subsection (h) says it must "include such information as the court may need to decide whether the expert's opinion is sufficiently reliable to be admissible as evidence" There are arrangements for pre-trial meetings between experts to set out areas of agreement and disagreement – 19.6.[35] An extended explanation of the role of the expert witness is set out in guidance from the Forensic Science Regulator[36].

44. There is the option to use the **voir dire** procedure (mini trial before the main trial) but the arguments are about whether evidence should be admitted, rather than a review of its reliability. A voir dire may also be used to assess the competence of an expert witness. The usual legislative route is s 78 PACE 1984.

45. **Experts** There is no official means of designating some-one as an expert witness for the purpose of criminal (or civil) proceedings. The decision to accept such a witness is for the trial judge, based on the expert's CV and subject to challenge by an opposing lawyer.

    The general issues of expert evidence were reviewed in a report in 2011 by the Law Commission: *Expert Evidence in Criminal Proceedings in England and Wales*, LC325. It proposed a statutory admissibility test to cover expert reliability to appear in a new law, a draft of which was included in the report. A distinction had to be made between scientific findings and expert opinion. The government of the day decided not to accept the recommendation for new legislation but some of the Law Commission's suggestions have appeared in the Criminal Procedure Rules and accompanying Criminal Practice Directions. The report contains a number of examples where expert and scientific evidence has caused miscarriages, or at least deep concern, but none of them cover digital evidence.

    Law Commission report LC 235 suggested that there should be more but still limited situations where judges appoint experts to assist them directly, rather than the experts being appointed by prosecution and defence within the adversarial procedure, even if such experts have an

---

33 Formerly CrimPR 33.

34 See Appendix III

35 *Meetings between experts: A route to simpler, fairer trials?*. Sommer https://doi.org/10.1016/j.diin.2008.11.002

36 https://www.gov.uk/government/publications/legal-obligations-issue-8/legal-obligations-issue-8-accessible

over-riding duty to the court[37]. In the European inquisitorial system court-appointed experts are common[38].

A real difficulty is the extent to which the work of experts in digital evidence blur with that of the traditional detective/investigator, particularly where reconstructions of events are required. In the more traditional relationship the forensic scientistic/expert finds matches or traces (perhaps supported by opinion as well as scientific test) and passes the result to the main detective who absorbs the observation into the broader investigation. But, as we have seen, some critical events necessary for conviction take place solely within computer systems – hacking, distribution of terrorist material, CSAM, piracy and fraud. It is the expert's conclusions which may be central at trial.

The Forensic Science Regulator's (FSR) scheme is about laboratory procedures though an element in an accreditation process is the "competence" of scientists – the test for this is not specified. The last attempt at accrediting individual experts was via the Council for the Registration of Forensic Practitioners (CRFP) which closed in 2009 to be replaced by the FSR. Law Commission report LC 235 discussed a possible scheme. There are a number of membership organisations for expert witnesses some of which offer training[39] but these are in the role of an expert witness, not in the detail of a speciality. Training in digital forensics is supplied by a number of commercial companies and there are also university courses. It can be quite difficult to assess the value to the courts of these courses[40]. The National Crime Agency maintains a list of experts for the benefit of law enforcement but simply provides introductions and does not guarantee quality.

46. There is a practical problem that publicly-funded fees for experts in this area are approximately one-third of what is available for similar privately-funded criminal and civil work. A related problem for law enforcement agencies is retaining qualified officers and staff.

47. The **ACPO Good Practice Guide for Digital Evidence** [41] is still referred to as such although the Association of Chief Police Officers was replaced by the National Police Chiefs Council (NPCC) in 2015. The *Guide* originated informally in the late 1980s and has been updated though the

---

37 In Part 6 of the report. But there would need to be a properly vetted panel of such experts.

38 Eg "Netherlands Register of Court Experts (NRGD)

39 Expert Witness Institute, Academy of Experts, Institute of Expert Witnesses, UK Register of Expert Witnesses

40 *Accrediting digital forensics: what are the choices?* Sommer https://doi.org/10.1016/j.diin.2018.04.004

41 https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf

most recent one was signed off in 2011. The most important feature is the 4 Principles.

48. Principles 1 and 2 deal with evidence preservation, Principle 4 places responsibility for compliance on the officer in charge of an investigation. Principle 3 states:

> That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third party forensic expert should be able to examine those processes and reach the same conclusion.

49. The audit trail is absolutely critical to all forms of digital evidence. The *Guide* does not have any statutory basis and the detail needs updating[42]. The 4 Principles are reproduced in the CPS Disclosure Manual and the Attorney-General's Guidelines on Disclosure.

50. The **CPS Disclosure Manual** deals with digital material in chapter 30[43] : The focus is guidance for law enforcement and prosecutors. The primary concern is not reliability but on "reasonable lines of inquiry". The aim is to limit the quantities of disclosed material but also to protect, so far as possible, personal information which might be held in computer files. The wish is to avoid accusations of "fishing expeditions" and "digital strip searches". It also deals with documentation of decisions, legal professional privilege, retention and engagement with the defence. It does not cover directly disclosure by third parties whose computer systems are required as evidence in prosecutions.

51. The **Attorney General's Guidelines on Disclosure, 2024**[44] deals with digital material at its Appendix A. Again, as the title suggests the focus is disclosure not reliability. It includes the ACPO Guidelines; essentially it is a reinforcement of the criteria set out in the CPS Disclosure Manual.

52. **Kelman's Seven Statements** As long ago as 1982 the barrister Alistair Kelman wrote the book *The Computer in Court* and produced a Seven Statement Test[45]: qualifications of person in charge, description of system, technical components, testing, logging of updates, system security features, how print-out came into existence and statement that no faults were manifest. 40 years later it is difficult to find fault with these tests.

---

42 *ACPO principles for digital evidence: Time for an update?,* Horsman https://doi.org/10.1016/j.fsir.2020.100076 ; *Computer forensics and the ACPO guide,* Yapp, https://www.scl.org/12161-computer-forensics-and-the-acpo-guide/

43 https://www.cps.gov.uk/legal-guidance/disclosure-manual-chapter-30-digital-material

44 https://assets.publishing.service.gov.uk/media/65e1ab9d2f2b3b00117cd803/Attorney_General_s_Guidelines_on_Disclosure_-_2024.pdf

45 https://docs.google.com/document/d/1cGYi78H0K2pTvQmbdGVroMr7OWFryP5urisy0CYn4nY/edit?tab=t.0#heading=h.us1hhje6o2c8

53. **Academic tests for single source** A number of academics have looked at the problems of testing the evidential reliability of output from a single source large computer system. These are referred to in paragraph 34 above. Marshall, Christie, Ladkin, Littlewood, Mason, Newby, Rogers, Thimbleby and Thomas in *Recommendations for the probity of computer evidence* recommend a two-stage exercise:

> When determining whether a system is reliable …. the matters that may be taken into account include—
>
> (a) The errors that have been reported in the system, the actions taken to correct them, and any errors that remain uncorrected (these may be called the Known Error Log and Release Notices);
>
> b) The measures taken to ensure that the electronic evidence accurately records the facts that are being claimed (including measures to block, record and manage cyberattack);
>
> (c) The forensic measures taken to ensure that the electronic evidence has not been affected by privileged or unauthorised access (typically, logs of the use of privileged usernames by system administrators and other 'superusers', and the cybersecurity protections in place);
>
> (d) The route that the electronic evidence has taken from the originating system to the court and the measures taken to ensure its integrity.[46]

54. Item (d) is in fact an echo of the audit trail which appears as Principle 3 in the *ACPO Guide.*

55. A longer term approach is to set out criteria for systems that are specifically designed to produce reliable evidence – evidence-critical systems[47] . An established cyber security practice is the **Forensic Readiness Programme[48].**

56. The **Electronic Trade Documents Act 2023 S 2(2)** sets out the requirements for such documents and suggests (in effect, not explicitly) the use of **digital signatures** to authenticate the document and protect it from subsequent alteration. This is a formalisation of the technique for **file hashing** which is a key feature of digital evidence preservation.

57. **Compliance with international standards** One potentially interesting route to persuading a court that digital evidence is reliable is to see how far the tendered material complies with international standards.

---

46 Credit: Martyn Thomas summary of the recommendations

47 https://evidencecritical.systems/ Murdoch.

48 A Ten Step Process for Forensic Readiness Rowlingson, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=40baa64f868d9dc6c5a6111c4d3c757a7879754a; *Digital Investigation and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers*, IAAC. https://shorturl.at/Rzde9

ISO/IEC 27037 is *Guidelines for identification, collection, acquisition and preservation of digital evidence.* The limitations can be seen in the title; it merely deals with the first stage of evidence acquisition and makes no contribution to evaluating any subsequent analytic process. ISO/IEC 27041 is *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*. It concentrates on designing a process for an investigation and then validating it. There is no specific advice on particular investigations. ISO/IEC 27042 is *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence* but in its current form is a description of the processes involved. ISO/IEC 27025 is used as a set of requirements for forensic processes in general. It started life as a more general *requirements for testing and calibration laboratories.* It has some value for conventional forensics where laboratories run simple single tests to find "matches" or "traces" but does not assist when multiple sources have to be combined in order to reconstruct events – that task is better handled via the requirements of the Criminal Procedure Rules. ISO/IEC 9000 and 13485 are general quality systems and are suitable for frequently repeated processes.

58. **Forensic Science Regulation** The Forensic Science Regulator operates under an Act of the same name – FSR Act, 2021. It issued its Code of Practice with effect from October 2023. It relies on an interpretation of ISO/IEC 27025; a certification of compliance is carried out by UKAS – the United Kingdon Accreditation Service. Failure to comply with the code does not give rise to criminal or civil proceedings but "A court may in particular take into account a failure by a person to act in accordance with the code in determining a question in any such proceedings."[49] Failure to comply does not directly affect admissibility. The emphasis is on laboratory processes and the scheme does not provide accreditation for individual forensic scientists or experts who attend court.

59. Section 82 of the Code deals with *Data capture, processing and analysis from digital storage devices*, the first stage in digital evidence acquisition and also subsequent processing but it is unclear how in any specific instance an evaluation of compliance can take place. Sections 97 and 98 deal with communications data and how it might be captured. Cellsite analysis is in section 83.

60. Much of the Code is concerned with what is described as quality management and with a strong emphasis on documentation to support the various processes including the validation of tools, record retention and operating environment. The documentation is what forms the basis of the

---

[49] FSR Act, 2021, s 4

UKAS accreditation. The scheme is heavily orientated towards conventional forensic laboratories which carry out repeated individual single tests based on established science. Fitting these criteria into how digital forensics works has proved a challenge[50]. In effect because of the use of ISO 27025 it is only the first two stages of digital forensics – acquisition and preservation – which can be fitted into a laboratory-type evaluation; the later analytic and event reconstruction stages leading on to the production of exhibits have a better "fit" with the expert evidence rules in the criminal practice procedures and where there are detailed explanations. Strict interpretation of the Code would result in many forms of digital evidence being excluded; there is a sense of square pegs being forced into round holes The Code sets criteria for processes but gives no advice for specific situations in which reliability may be called into question.

61. **AI Support** The term artificial intelligence is highly fluid and is sometimes applied by way of a marketing operation to what is really very conventional IT processing. AI can appear in the context of digital evidence in a number of ways. Some forms of AI can be used to sort through vast quantities of data which might prove difficult for a human being[51]. Typical examples could include financial records, emails, text messages and social media chat logs. At the end of the process the actual located findings can become exhibits to show fraud, conspiracy, etc. A second use would be much more worrying when generative AI is used to create charts and other exhibits. The difficulty here is that processes involved are unlikely to be transparent with the result that testing is not possible.

    IPCO has identified four indicative features of AI which might impact its task of evaluating applications for the granting of investigatory powers: AI uses data science techniques in the processing of large volumes of information; it can operate without direct human control in a partially or fully autonomous manner, including making decisions or select; it can adapt its functions or outputs based on new information; and it can generate new information such as text, sound, or images, 'Generative AI'.[52]

---

50 *Quality standards for digital forensics: Learning from experience in England & Wales,* Tully and others , https://doi.org/10.1016/j.fsidi.2020.200905

51 Using manual techniques or *grep* for example.

52 https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCOs-Scope-of-Interest-in-AI.pdf

Disclosure

62. The main guarantor that a court is able to evaluate the reliability of evidence is the requirement to disclose material to the defence who can then mount challenges. The basic doctrine is well enough known and is set out in the Criminal Procedure and Investigations Act 1996. Section 3(1) sets out the requirement: "The prosecutor must disclose to the accused any prosecution material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused".

63. The overall problem is the lack of parity of arms – most defendants will be at a disadvantage when it comes to questioning the level of supplied disclosure and then understanding the implications of what has been disclosed. Not the least of the practical difficulties is for defence teams to know what to ask for in the first place. Questions about disclosure where important in the Post Office Horizon proceedings[53] but occur frequently in many less-well-publicised trials. Some situations are mentioned below. There can be particular problems with data from 3rd parties.

64. The CPS Disclosure Manual chapter 30 has already been referred to.

65. There are some limitations. First, the obligation is limited to material which is in the possession of the prosecutor and therefore may not include material in the hands of third parties or overseas law enforcement agencies, a topic explored below. Second elsewhere in the Manual at chapter 8 are the circumstances in which "sensitive material" is handled. Chapter 9 deals with "highly sensitive" material. This is "that which, should it be compromised, would be likely to lead directly to the loss of life, or directly threaten national security." Regular "sensitive methods" are likely to include methods of law enforcement access to hostile computer systems under "equipment interference"[54] and methods of decryption.

66. In Chapter 13 of the Manual there is guidance for prosecutors who wish to make an application for Public Interest Immunity (PII). The typical situation is where the prosecutor has identified material that fulfils the disclosure test, disclosure of which would create a real risk of serious prejudice to an important public interest, and the prosecutor believes that

---

53 https://www.guildhallchambers.co.uk/2024/03/11/the-post-office-disclosure-lessons-from-a-national-scandal/; https://www.computerweekly.com/news/366566395/How-legal-disclosure-failures-disrupted-the-Post-Office-Horizon-inquiry

54 Under Part 5 Investigatory Powers Act 2016; see also *Evidence from hacking: A few tiresome problems*, Sommer https://doi.org/10.1016/j.fsidi.2022.301333

the public interest in withholding the material outweighs the public interest in disclosing it to the defence. There are three categories of situations in terms of procedure – where the defence are put on full notice, where they are put on notice but not allowed specific detail and where the application is made without notice. One of the concerns is that in the end it is for a judge to decide whether to grant a PII certificate and it is unclear where a judge can turn to in resolving a difficult technical matter. A further concern is where a PII certificate has been issued – so that disclosure can be withheld – but where the prosecution want the benefit of the material as evidence as opposed to intelligence (which would be used to obtain disclosable admissible evidence)[55].

67. Even where sensitivity is not an issue there can be disputes between prosecution and defence over the "relevancy" of a requested disclosure and also over the need to protect personal and commercially confidential information. Another area of difficulty is in cases involving child sexual abuse and extreme pornography where "possession" is a strict liability offence. Some of these issues can be managed by obtaining undertakings from defence experts, perhaps bolstered by court orders.

68. **3rd party material** may not be in the immediate possession of prosecutors or been "revealed" to them by investigators. As such it falls outside the regular disclosure obligations. But such material may be essential to a prosecution. It can fall into one of a number of categories[56]:

    a. Material formally obtained by overseas law enforcement from well-established communications service providers and social media platforms. At a practical level the likelihood is that the overseas law enforcement agency will have acquired either under court order or by volunteer action on the part of the CSP or platform. It is also, for some countries at least, likely that proper acquisition procedures have been used and that there are witness statements in support.

    b. Material obtained from well-established overseas-based communications service providers and social media platforms. In this situation material will have been obtained either voluntarily or via an ILOR, MLAT or CLOUD-type treaty. There may have been some significant hesitation as the supplier would need to balance the expectations of their customers/clients for privacy.

---

55 A typical situation would be to withhold information about a specific method for equipment interference – hacking into a computer – but to use the intelligence acquired to arrange to seize the computer at which point its properly preserved stored contents could become admissible evidence.

56 Online material which has been obtained by UK law enforcement by means of direct access does not count as 3rd party material for this purpose as the law enforcement officer is responsible for the methods of acquisition and which should have been "revealed" to the prosecutor for the purposes of disclosure

Acquisition will have been by staff of the CSP or platform and hence may be more questionable

c. Material obtained from lesser-known overseas-based communications service providers and social media platforms The situation here is similar to that above but with less likelihood of useful co-operation

d. Material obtained from commercial organisations within UK jurisdiction who have either been alleged victims or whose systems have been used as a path to suspected criminality. Availability will have been either via compliance with a production order or voluntarily. The quality of acquisition will depend on the quality of the staff available to carry out the necessary actions. The path to acquisition may not be straight forward as organisations express their concerns about data protection obligations, commercial confidentiality and the scope of disclosure required.

e. Material obtained from commercial organisations outside UK jurisdiction who have either been alleged victims or whose systems have been used as a path to suspected criminality. There are many obstacles to obtaining this class of material. The quality of acquisition will depend on the quality of the staff available to carry out the necessary actions.

Formats for Reform

69. The current doctrine of a presumption of reliability in computer-derived evidence has no statutory basis. s.60 of the Youth Justice and Criminal Evidence Act 1999 simply revoked s 69 PACE 1984. The common law interpretation of presumptive rebuttable reliability seems to be based on Law Commission Report CP138.

70. One route to reform could be an updated and improved version of s 69 PACE: a certificate of reliability required to admit evidence but with better specific detail. The problem with a statutory approach is that that some material will then become inadmissible and others admissible and which will depend on definitions embedded in the law. The inevitable result will be disputes as to whether particular items are included or excluded. There may also be attempts at circumventing any operationally inconvenient definitions as we saw during this section 69 regime and the

"real evidence" exceptions[57]. A further problem will be deciding who would have the competence to issue such a certificate[58]. Not the least of the difficulties in locating such a person is the extent to which computer output may be the product of multiple data inputs from multiple external computer systems and software that has been compiled from third party libraries.

71. A much better approach is via a Code of Practice or Practice Direction. Either of these would have to have sufficient status so that judges could make orders indicating compliance or noncompliance. Appropriate routes for a Code of Practice would be via the Police and Criminal Evidence Act 1984[59] and the Investigatory Powers Act 2016[6061]. The advantage of this approach is that the emphasis is on weight of evidence as opposed to admissibility; under an admissibility regime decisions become binary whereas with a Code of Practice judicial pressure can obtain more flexible results, including over disclosure arguments. The same came said of a Practice Direction.

72. A useful element could be the requirement on the part of a tenderer of computer evidence to complete a questionnaire. An indicative model is to be found in the e-disclosure questionnaire under civil procedure practice direction 31B. It would not be necessary to answer all questions in all circumstances. Some suggestions appear below.

73. A judge's discretion to exclude evidence under s 78 PACE 1984 would remain: "if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it."

74. The new practice direction or Code of Practice would sit alongside the current directions for expert evidence – CrimPR 19.

---

57 R.v Wood (1983) 76 Cr App R 23; Sophocleous v Ringer [1988] RTR 52; Castle v Cross [1985] 1 All ER 87

58 R v Shephard [1993] AC 380

59 Ss 66 and 67

60 S 241 and Schedule 7

61 Could be a SI using the affirmative procedure

Ingredients for Questionnaire

The following is an indication of the types of questions that could feature in a questionnaire. The responses would have the status of a CrimPR 16 written witness statement and, if there is an expert element such as an expression of opinion, CrimPR 19 would apply.

1. **Provenance and Continuity** Questions to establish the data input sources to the digital evidence. Followed by an explanation of the method of acquisition so as to avoid contamination. Followed by the preservation method to avoid subsequent alteration – these might include the use of file hashing and write-once media. Followed by a description and justification of any analytic tools used to render the raw material easier to understand; if the tools are in any way non-standard – justifications for their use. Followed by the methods used to produce exhibits for court use. An audit trail for all of the above.

2. **Identification of processes claimed to be standardised and established**

3. **Identification of non-standard procedures** – together with explanations of testing for accuracy and security for these procedures. There should be an opportunity for defence testing if requested. Any tools used should be identified including any principles behind the tools. Any compliance with the FSR Code should be mentioned.

4. **Technician expertise** In so far as not covered by the requirements of CrimPR 19 the expertise of any technician appearing as a witness plus any training should be indicated

5. Thereafter, given that there are many sorts of digital evidence it might makes to have separate pathways for: Separate routes for:

    - Single purpose devices, e g for measuring, weighing
    - Video and audio
    - Evidence from individual PCs and smartphones
    - Evidence from large corporate systems
    - Evidence involving event reconstruction from multiple sources

Non-legislative encouragement for more reliable digital evidence

The availability of more reliable digital evidence to the criminal courts does not depend solely on legislative and regulatory measures. The following are activities which can be promoted by the Ministry of Justice and other

ministries including the Home Office and the Department for Industry and Trade:

1. The **NPCC/ACPO Good Practice Guide to Digital Evidence** appears not to have been revised since 2012. A new edition to reflect current types of digital evidence and how they are to be managed seems long overdue.

2. **Judicial training** The challenges facing judges in evaluating the reliability of evidence, handling expert evidence and ordering disclosure are considerable. While some judges are obviously able to meet the challenges this is not universally the case. "Judges" in this instance include tribunal judges, district judges and magistrates. An appropriate series of courses does not currently appear on the website of the Judicial Studies Board

3. It seems obvious that further **enhanced police training is required**. At a variety of levels. A 2022 report by HMICFRS [62] made 9 detailed recommendations – how many of these remain to be fully implemented? Career paths for specialist investigators should be reviewed in order to limit the current problems of staff retention.

4. There is currently no scheme to provide **certification for experts** in digital forensics or indeed other areas. Decisions to accept individual expertise and to impose limits on an expert if necessary are solely for judges. The Forensic Science Regulator scheme is optimised for laboratories and processes, not for individual who provide witness statements for court use.

5. The notion of a **Forensic Readiness Program[63]** is already well-established but needs more publicity. The aim is that organisations should consider what sorts of incident they might be involved in and to have plans to be able to produce the necessary evidence to support law enforcement, to become involved in civil legal proceedings and to make insurance claims. Such programs should be part of broader Incident Response Plans. At the moment the UK National Cyber Security Centre (NCSC) only provides indirect guidance.[64] A related notion is that of Evidence-critical systems[65]; individual systems which are designed to produce robust, tamper-proof records of their activities.

---

62 https://hmicfrs.justiceinspectorates.gov.uk/publications/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/

63 IAAC Guide. https://shorturl.at/Rzde9

64 https://www.ncsc.gov.uk/guidance/guidance-on-digital-forensics-protective-monitoring; https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

65 https://evidencecritical.systems/2021/04/27/evidence-critical-systems-designing-for-dispute-resolution.html; https://evidencecritical.systems/2020/06/19/evidence-critical-systems.html

Appendix I: Peter Sommer: brief CV

Professor Peter Sommer combines academic and public policy work with commercial cyber security consultancy, with a strong bias towards legal issues.

His first degree is in law, from Oxford University. He has recently retired as a Professor of Digital Evidence at Birmingham City University and is now a Visiting Professor there and a Visiting Professor at de Montfort University. Until 2011 he was a Visiting Professor in the Department of Management at the London School of Economics and before that a Senior Research Fellow. He has consulted for OECD, UN, European Commission, UK Cabinet Office Scientific Advisory Panel on Emergency Response, UK National Audit Office, Audit Commission, and the Home Office. He has carried out external audits of the Internet Watch Foundation hotline. The OECD work, written with Ian Brown, addressed the cyber aspects of Future Global Threats. He has given evidence to the Home Affairs and Science & Technology Select Committees, the Joint Committee on the Communications Data Bill and to the Intelligence and Security Committee. He was a Specialist Advisor to the old Trade and Industry Select Committee covering e-commerce and crypto and to the Joint Committee on the Draft Investigatory Powers Bill (now an Act).

During its existence he was the joint lead assessor for the digital speciality at the Home Office-sponsored Council for the Registration of Forensic Practitioners and has advised the UK Forensic Science Regulator and the Home Office on communications data. He has also advised the Netherland Register of Court Experts (NRGD), SWGDE, and ISC2 in developing syllabuses for digital evidence specialists.

For over 30 years he has acted as an expert in many important criminal and civil court proceedings in the UK and international courts usually where digital evidence has been an issue including Official Secrets, terrorism, state corruption, assassination, global hacking, DDoS attacks, murder, corporate fraud, privacy, defamation, breach of contract, professional regulatory proceedings, software and IP piracy, harassment, immigration issues, allegations against the UK military in Iraq, the International Tribunal on the Lebanon, "revenge porn" on social media, serious organised crime, IPT issues and child sexual abuse. Particular themes have been situations where technologies need to be interpreted in legal terms and assessments of quantum and extent of damage. He is instructed on occasion by both prosecution and defence interests as well as in civil proceedings.

He is the author, pseudonymously, of *The Hacker's Handbook*, *DataTheft* and *The Industrial Espionage Handbook*, and under his own name, *Digital*

Evidence, Digital Investigations and E-Disclosure (IAAC) now in its 4th edition and the *Digital Evidence Handbook*.

He is a Fellow of the British Computer Society and also a Fellow of the Royal Society of Arts.

Appendix II: Case Study: Op Venetic

The purpose of this case study is to show some of the variety and complexity of some investigations and trials in which digital evidence plays a significant part. The facts of each trial are different and most of the trials relied on more evidence than just that from encrypted smartphones. This account is simplified and generic and does not refer to any set of accusations past current or future.[66]

Between 2016 and 2020 a particular model of strongly encrypted highly secure smartphone became popular with many individuals engaged in serious organised crime. It was called EncroPhone. It was the subject of National Crime Agency (NCA) Operation Venetic and by April 2024 had led to the arrest of 2,864 suspects, the seizure of over £76 million in criminal cash, 170 firearms, 3,404 rounds of ammunition and 18 tonnes of Class A and Class B drugs. The handsets together with a six-month subscription cost £1500 with a further £800 needed for subscription renewal.

The smart phones were highly resistant to direct examination by law enforcement unless they had been able to obtain the necessary passcode. A solution was found by Dutch and French law enforcement. They made covert purchases of handsets and obtained legal access to a mediating server from which the Encro service was being run. They were able to devise an update to the handset system which could be sent "over the air" to each subscriber. The update was referred to variously as a "tool" or "implant". The effect was to enable the capture of messages and photos stored on each handset, typically seven days' worth, but also new messages as they were being originated and received. However the French, who had operational control, refused to provide any detail of the tool, citing national defence security.

---

66 There are a number of scholarly articles which provide more detail: *Encrochat*: *The hacker with a warrant and fair trials?,* Stoykova https://doi.org/10.1016/j.fsidi.2023.301602*; Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat: R v A, B, D & C ,* Griffiths & Jackson https://doi.org/10.1177/00220183221113455 ; *Digital evidence, police investigations, and lessons learned from EncroChat: Is it time for a new framework for the admission of digital and communication evidence?* Griffiths & Jackson Criminal Law Review, (7), 436–457.

Material acquired by the French from their tool was processed by them and then packaged up for distribution via Europol to international law enforcement partners including the NCA in the UK. The NCA opened up the packages and then distributed them to local Regional Organised Crime Units (ROCUs) for further investigation and action.

Initial legal concern in the UK concerned the admissibility of the acquired new messages - had they been acquired from some form of storage on the handset or had they been captured in the course of transmission between handsets? If the latter, under current UK law – s 56, Investigatory Powers Act 2016 - those messages would be intercept and hence inadmissible. If the French were not prepared to reveal their method, how could anyone determine? In the end the English courts decided to admit into evidence the notes a NCA officer had made of a conversation with a French law enforcement officer and which provided a brief explanation of the French method[67] [68]. In relation to the interception / storage arguments the interpretation taken was that since EncroChat used end-to-end encryption in which encryption and decryption only took place on the handsets it must be the case that the recovered messages must have come from storage. [69]

This left the problem of determining the reliability of the messages that were being supplied to UK law enforcement and being used in trials. Even on manual inspection the records of message and photo transactions showed anomalies. But computer-aided checks by a defence expert revealed much more. The evidence packs of two or more Encro handsets that had been in contact with each other were loaded into a database for comparison. If phone A sent a message to phone B one would expect to see copies of the message on both handsets. But very often this did not happen, messages sent appeared not to have been received while messages were received without appearing to have been sent. The computer analysis also showed that the French tool/implant stopped frequently and had to be restarted. There were other issues but at the very least the French tool/implant was producing incomplete records.

The NCA's own expert obtained similar results when he wrote his own software checker. Eventually the defence and NCA software was harmonised[70].

---

67 *R v A, B, D & C* [2021] EWCA Crim 128**;** https://www.judiciary.uk/wp-content/uploads/2022/07/A-v-R.pdf

68 At a much later stage the French produced a letter under a Mutual Legal Assistance Treaty (MLAT) but this provided very little additional substantial information and the refusal to provide copies of the tool and a means of testing remained unaltered.

69 There is an alternative hypothesis which is advanced by some defence experts: that the effect of the tool could be to weaken the encryption mechanisms such that in each instance the encryption key would be known to the authorities so that they could capture traffic in transit between handsets.

70 The defence tool is called VDL and the NCA tool RS.

Defence attempts at getting the Encro evidence excluded by asking judges to use their discretion under s 78 PACE 1984 were largely unsuccessful: the evidence was not so unreliable that a jury should be denied an opportunity to consider it; s 78 requires a very high threshold.

To repeat, each trial was, and is, different. Prosecutors sought to overcome the problems of the incompleteness and unreliability of the Encro evidence by showing support for the overall case they wished to make by pointing to additional corroborating material. This included cellsite findings, ANPR vehicle movement records, the results of conventional surveillance and the contents of messages and photos. Most but not all contested prosecutions have been successful.

Appendix III: CrimPD 19.4

19.4. Where rule 19.3(3) applies, an expert's report must—

(a) give details of the expert's qualifications, relevant experience and accreditation;

(b) give details of any literature or other information which the expert has relied on in making the report;

(c) contain a statement setting out the substance of all facts given to the expert which are material to the opinions expressed in the report, or upon which those opinions are based;

(d) make clear which of the facts stated in the report are within the expert's own knowledge;

(e) where the expert has based an opinion or inference on a representation of fact or opinion made by another person for the purposes of criminal proceedings (for example, as to the outcome of an examination, measurement, test or experiment)—

(i) identify the person who made that representation to the expert,

(ii) give the qualifications, relevant experience and any accreditation of that person, and

(iii) certify that that person had personal knowledge of the matters stated in that representation;

(f) where there is a range of opinion on the matters dealt with in the report—

(i) summarise the range of opinion, and

(ii) give reasons for the expert's own opinion;

(g) if the expert is not able to give an opinion without qualification, state the qualification;

(h include such information as the court may need to decide whether the expert's opinion is sufficiently reliable to be admissible as evidence;

(i) contain a summary of the conclusions reached;

(j contain a statement that the expert understands an expert's duty to the court, and has complied and will continue to comply with that duty; and

(k) contain the same declaration of truth as a witness statement