Digital Footprints: Assessing Computer Evidence

Peter Sommer
Computer Security Research Centre,
London School of Economics and Political Science

Summary: *This article describes some of the more common of the new forms of computer evidence and the new techniques of evidence acquisition, preservation and analysis. It shows how inferences are being drawn from computer-derived materials that would not usually be viewed by the ordinary computer user. It attempts to indicate some of the practical problems of assessing reliability. As will be seen, even if as widely expected section 69 disappears, a number of other issues of admissibility will arise. Finally it makes some provisional policy suggestions.*

Computer evidence used to mean one of two things. Its most typical form was regular print-out from a corporate computer. The alternative form was a reading from any single-purpose measuring or counting device which can be regarded as a mute witness free from human intervention, such as an intoximeter, a telephone call meter or a weighing machine. Overwhelmingly journal articles and legal text-books have concentrated on issues of admissibility. In the case of regular computer print-out, the problems have been of the scope and circumstances of certification of proper working and notions of "document" and "statement" - what may be referred to in short-hand as "section 69 issues"[1]. In the case of the simple measuring devices the problem has been the limits of this area of interpretation of "real evidence".

When the Law Commission produced its Consultation Paper "Evidence in Criminal Proceedings: Hearsay and Related Topics"[2] in May 1995 and then its Report published in June 1997[3] significant consideration was given to the problems of computer evidence both as "real evidence"[4] and as statements which required certification[5]. The main relevant recommendations of the Report are as follows:

> "3. that, where a representation of any fact is made otherwise than by a person, but depends for its accuracy on information supplied by a person, it should not be admissible as evidence of the fact unless it is proved that the information was accurate...

---

[1] In reality, as well as s.69, see Criminal Justice Act 1988, ss.23, 24 and the schedules thereto and, for interpretation, Civil Evidence Act 1995 s.13.
[2] Law Commission, Consultation Paper No 138 *Evidence in Criminal Proceedings: Hearsay and Related Topics*
[3] Law Commission, Report Law Com No 245 *Evidence in Criminal Proceedings: Hearsay and Related Topics*
[4] Consultation Paper No 138, paras 2.14-2.19, 7.42-7.50 and Recommendation 3 of Law Com No 245.
[5] Consultation Paper No 138, Parts XIV; Part XIII and Recommendation 50 of Law Com No 245.

16. that statements falling within the business documents exception should be automatically admissible, but that the court should have power to direct that a statement is not admissible as a business document if it is satisfied that the statement's reliability is doubtful...
50.the repeal of section 69 of PACE."

But over the last decade the huge changes in the physical forms computers take, the range of applications, patterns of ownership, the ways in which they are used and the extent to which they can be interlinked across businesses and across the world have produced many new forms of computer-derived evidence. Many of the assumptions in the earlier articles and in the precedents to which they refer are no longer true. For example a computer is not necessarily "just like" a filing cabinet and as a result computer "documents" may not be "just like" the paper equivalent. Again, it is not necessarily the case that computer errors are nearly always manifest in that the result is either no read-out or print-out of any kind or gross nonsense.[6] Depending on circumstances, a computer print-out can look plausibly correct but nevertheless be misleading or be misinterpreted. Increasingly too, the courts are being presented with configuration, logging and other system files which would not normally be viewed by the ordinary computer user - indeed such a user may not even know of their existence - but which investigators and prosecutors are tendering as evidence of an accused's activities or intentions.

In both the Consultation Paper and the Report, the Commissioners showed concern about some of the practical problems of assessing the reliability of computers and computer output, though their focus was on section 69 of the Police and Criminal Evidence Act ("PACE"). They gave the following main reasons for regarding that section as unsatisfactory:[7] that it fails to address the major causes of inaccuracy in computer evidence; that advances in computer technology make it increasingly difficult to comply with section 69; that it is becoming "increasingly impractical to examine (and therefore certify) all the intricacies of computer operation";[8] that the recipient of computer evidence may be in no position to satisfy the court about the operation of the computer; that it is illogical that section 69 applies where the document is tendered in evidence, but not where it is used by an expert in arriving at his conclusions, nor where a witness uses it to refresh his or her memory.[9] In the Consultation Paper the Commissioners quote Kelman and Sizer[10] with approval: "with a large and complex computer system, it is doubtful whether...a manager could have sufficient knowledge [to issue a section 69 certificate]… the computer malfunction or an act of unauthorised tampering might be almost impossible

---

[6] As suggested by Professor Colin Tapper in "Discovery in Modern Times" (1991) 67 *Chicago-Kent Law Review* 217, 248 and in *Computer Law* (4th ed., Longman, London, 1989 Chapter 9, *passim*

[7] Law Com No 245, paras 13.6-13.22.

[8] Citing Castell, S., "Evidence and Authorisation: is EDI [Electronic Data Interchange] 'legally reliable'?" (1990) 6(5) *Computer Law and Security Report* 2.

[9] *Golizadeh* [1995] *Crim LR* 232, *Sophocleous v Ringer* [1988] *RTR* 52.

[10] Consultation Paper No 138, para 14.15 citing Kelman, A., and Sizer, R., *The Computer in Court* (Gower Publishing, London, 1982) p 19

to detect by all but experts in the field." A little later, the Commissioners go on to remark:[11]

"…. comments from judges to the effect that determined defence lawyers can and do examine the prosecution's computer expert at great length. The complexity of modern systems makes it relatively easy to establish a reasonable doubt in a juror's mind as to whether the computer was operating properly. We are concerned about smoke-screens being raised by cross-examination…"

The Commissioners' conclusion was that it is not possible to legislate protectively with regard to computer evidence and that where there are specific reasons to doubt the reliability of a particular document generated by a computer these doubts should go to weight and not to admissibility.

In effect, the Commissioners are throwing all the burden of assessment on to the trier of fact, which for more serious offences, will be a lay jury. If we agree that it is mistake to "legislate protectively" given all the potential problems of rigidity in interpretation, are there any broad tests for "reliability" we can offer? Should we consider Codes of Practice which might guide law enforcement officers and the Courts? Would these be enough? Many of the expressed worries about the use of lay juries in trials of complex fraud[12] transfer very easily to situations where there are complex computer systems. Again, many of the problems of assessing novel scientific evidence, most recently considered in connection with DNA evidence [13] re-appear with renewed vigour.

The Growth of Computer Forensics

A few brief paragraphs of historical context-setting may be helpful in understanding how and why the techniques came into existence. Three or four key trends have distinguished the history of computing over the last fifteen and particularly the last ten years; the main trends have in turn spawned many lesser ones and all have interacted with, and reinforced, each other. They are: the growth in use and power of personal computers; the move in the design of corporate computer systems away from the centralised monolithic mainframe towards a multiplicity of smaller but powerful machines which inter-work and inter-connect in a form usually called distributed processing; and the growth of networks, both private and, in the form of the Internet, globally public. All of these changes have had an impact not only on what computers can deliver to their owners but also in the types of evidence that may be found within them.

---

[11] Consultation Paper No 138, para 14.20.

[12] For example in the Roskill Report, *Fraud Trials Committee Report* (HMSO, 1986) Chapter 8 *passim*; Home Office, *Juries in Serious Fraud Trials* (London, 1998).

[13] Steventon, B., *The Ability to Challenge DNA Evidence*, (Royal Commission on Criminal Justice Research Study No 9, HMS0, 1993); Alldridge, P., "Recognising Novel Scientific Techniques: DNA as a test case" [1992] *Crim. L.R.* 687 at pp 689-691; Redmayne, M., "The DNA database" [1998] *Crim. L.R.* 437.

Personal Computers: PCs have been used for non-recreational purposes for almost 20 years, and today the sub-£1000 PC is more powerful than many business mainframes of 20 years ago. Unlike physically larger computers, they can be easily taken away in their entirety during the execution of a search warrant. As they are personal to an individual in addition to formal business documents, they are much more likely to hold informal material which could, for example, indicate intentions or hidden activity. As a result of the increasing complexity of PC operating systems and applications, PCs create many non-obvious files which improve system performance and allow recovery in the event of disaster; on examination these can be interpreted to show how the computer has been used recently. PCs are also the primary means through which the Internet is used for sending global e-mail and viewing information on the world wide web. The programs that provide these facilities also create substantial logging and other files on the PCs hard-disk which can subsequently be examined.

Distributed processing: Distributed processing is way of designing systems which, in contrast to the use of a single very powerful central computer which both holds and processes all organizational information, is easier to design, faster, cheaper and more resilient. A number of smaller computers are linked together so that they feed one another with information and resources; some of the smaller computers may be quite specialized in nature - indeed they can include automatic teller machines, warehouse and manufacturing robots, and bar-code readers. Distributed processing has been common in larger organizations for at least 15 years. From an evidential perspective, one consequence is that many computer documents are "assembled" only on demand and from many different sources. PCs are often used within distributed processing systems as the primary way in which executives see how the business is performing. Such PCs hold programs which interrogate the main system for information but display the results on the individual executive's PC in a way that the executive has personally devised. What appears on a screen or a print-out in these circumstances depends on the actions of the individual executive as well as the quality of the central pool of corporate information. The problem then is what someone seeking to rely on such a document must do to seize and produce it - and then be in a position to show it to be reliable for the purposes of "weight". Can one rely on a single print-out produced on one PC or should the entire corporate database be seized? Computer systems using distributed processing generate many intermediate and logging files; in addition, if care has been taken in introducing security measures, there may be yet other audit and logging files. Again a skilled computer analyst may be able to interpret these to provide assurance of consistency to a court or alternatively demonstrate a critical inconsistency.

Networking: In networks, where several computers are linked together, there are similar problems of discovering where a document is held and how much needs to be seized in order to provide sufficient "weight". There are a number of ways of designing networks: the simplest variety simply provides individual PCs with the capacity to communicate with each other and, depending on how the security is set, access part of each others' hard-disks. A more complex design would include one or more servers, larger computers which hold programs and data. The programs might include internal e-mail and the data

may include back-ups of key business records. Servers are an important source of computer evidence. Distributed processing systems rely heavily on complex networks. In the largest of organizations, part of the network may be beyond local jurisdiction. Private networks also exist at an industry level and first-generation EDIs (Electronic Data Interchanges) depend on them.

Internet: The Internet is the largest public network. Although its history goes back to the early 1980s, its real growth for commercial companies and private individuals only began in 1994. The combination of the availability of powerful PCs with large hard-disks, cheap high-speed modems, the development of inventive software, changes in Internet regulation which enabled private investment in Internet infrastructure and other forms of private enterprise have fuelled the Internet's growth. But these same factors have also encouraged new forms of traditional crimes: for example, the exchanging of paedophile material on the Internet has only become substantial because customers for this material have PCs that can hold and display large numbers of such detailed photographs and because data transfer times are now very quick. Combined with cryptography, Internet e-mail provides a secure means of communicating messages for a criminal purpose. At the same time, there are many opportunities for a skilled investigator to track evidence of Internet activity, but the problem is how to give it weight. In many cases investigating officers seek to strengthen the story told by one strand of computer-derived evidence by corroborating it with one or more others from separate independent sources, or indeed by evidence which has nothing to do with computers at all.

As well as these changes in technology, a further reason for the growth of computer forensics has been the introduction of criminal offences the investigation of which necessarily involves law enforcement officers and the courts to consider internal computer processes.[14]

In response, the new techniques in computer forensics have appeared at astonishing speed: whereas the history of DNA profiling goes back to work at Leicester University in 1984 and has since seen a steady refinement in procedures and technique within the disciplines of traditional forensic science,[15] computer forensics involves many different techniques to cope with a variety of computer hardware and software situations, and with many different potential outcomes and levels of reasonable expectation of reliability. Many advances in computer forensics have come though the initiative of individual law enforcement officers and private sector computer technicians, and the involvement of the established forensic science laboratories has tended to trail behind.

---

[14] Especially the Computer Misuse Act, 1990 where "unauthorised access" and "unauthorised data modification" must be proved.

[15] See n.13 supra and also Houlder, V., "Fingerprints of the Future: Technology DNA Testing", *Financial Times*, 14 May 1998, "Proof' under Suspicion: Forensic DNA Testing", *Financial Times*, 26 May 1998

In 1992 Paul Collier and Barry Spaul produced a series of arguments in favour of a discipline to be called "Computer Forensics".[16] The courts had been dealing with computer-derived evidence for many years before that, and the term was already in informal use,[17] but this was probably the first article in an academic journal. At the beginning of the 1990s some individuals within the UK law enforcement agencies - investigators and technical support operatives - the small number of specialists to whom they turned for advice and the even smaller number of computer experts who were available for defence work began to realize that in computer forensics, as in other similar fields, "standard" techniques, protocols and procedures needed to be evolved. Conferences initially convened by the Serious Fraud Office, Inland Revenue and Customs and Excise took place at the Police Staff College at Bramshill in 1994 and 1995; subsequent meetings had to move to larger premises at Warwick University. An inter-agency working party has been in existence since then. The National Criminal Intelligence Service have carried out research under the heading Project Trawler,[18] and ACPO have established a Computer Crime Committee. Early in 1997, Edward Wilding had a bold, if premature, attempt at the subject in his *Computer Evidence: a Forensic Investigations Handbook*,[19] but the techniques described in detail are almost exclusively limited to stand-alone DOS-based PCs, making it already obsolete.[20] In 1998, David Davies, a Detective Inspector at West Midlands Police,[21] who had become interested in computer investigations after involvement in a lengthy paedophile case, produced a guide for police officers . It is not generally available to the public and is principally a guide to the Internet rather than to investigations on the Internet.

Common Computer Forensic Techniques

Seizure of Computer Hardware: This is probably the best established of the techniques, and the one closest to traditional scene of crime activity. The protocols issued to the police describe a variety of investigative procedures, including:[22] carrying out a pre-raid

---

[16] Collier, P.A. and Spaul, B.J., " A Forensic Methodology for Countering Computer Crime" (1992) 32(1) *Journal of Forensic Science* 27.

[17] See, for example: Sommer, P., *Computer Forensics: an introduction* in *Proceedings of Compsec International, 1992*, (Elsevier Advanced Technology, Oxford, 1992) pp 89-96.

[18] A conference was held by NCIS in London on May 28 1997

[19] Wilding, E, *Computer Evidence: a Forensic Investigations Handbook*, (Sweet & Maxwell, London, 1997).

[20] Other books include:, Icove, D., Seger, K., & VonStorch, W., *Computer Crime: a Crimefighter's Handbook*, (O'Reilly & Associates, Inc, Sebastopol, Ca, 1995) and Clark, F., and Diliberto, K., *Investigating Computer Crime*¸ (CRC Press, Baco Raton Fa, 1996)

[21] Davies, D. *Internet Detective: an investigator's guide*, (Police Research Group, Home Office, London, 1998).

[22] For example *Federal Guidelines for Searching and Seizing Computers*, US Department of Justice, at <http://usdoj.gov/criminal/cybercrime/search_docs/> *passim*; Icove at al. *op cit*, p391 ff. UK Customs & Excise have similar though unpublished procedures which use ISO9001 Quality Controls. During 1998 the Computer Crime Group of ACPO issued its own guidelines, *Good Practice Guide for Computer-based Evidence*, but has not sanctioned general publication. Guidelines from Scotland Yard's Computer Crime Unit are available at http://www.csfi.demon.co.uk/scotlandyard/index.htm. In the absence of anything

intelligence review to assess what types of hardware may be expected, what sorts of software, identifying what sorts of back-up might be held and how these might relate to potential evidence; defining the scope of warrants - this is not a forensic procedure as such but is essential if there is to be conformity with admissibility rules; photographing the computer(s) *in situ*, particularly any cabling of peripherals and ancillaries; careful identification and labelling of all items, including cables, peripherals, external data storage such as disks and tapes; careful dismantling, to include preventative measures to avoid inadvertent damage or contamination, and bagging; appropriate record-keeping; precautions to prevent the data being destroyed by hostile individuals immediately prior to the raid; the handling of computers that are running at the time of the raid; procedures for safe shutting down; the noting of the time on the computer's internal clock - which is used among other things, to provide date and time stamps on computer files; and the making of an exact sector-by-sector copy of every hard-disk.

This last item needs some explanation. A particular problem of evidence from hard-disks attached to computers is that the very process of turning on a computer and/or seeking to copy its contents can alter the contents to such an extent that they become contaminated. In order to avoid this most UK law enforcement agencies use a process sometimes called "legal imaging"[23] which, with a combination of special hardware and software and appropriate procedures, is intended to overcome the hazards of contamination[24]. The procedure should take place as soon as possible after a computer has been seized; subsequent examination is then carried out on the copies of the hard-disk.[25] The method consists of starting (or "booting") the computer not from the first hard-disk as would be normal but from the floppy or "A" drive. The computer is booted with a minimal operating system as opposed to a complex one like Windows 95. The operating system contains additional features or "drivers" which make the computer recognise an external data storage device such as a removable hard-disk. Still operating from the floppy drive, software is run which will make an "image" of the hard-disk (or hard-disks if there is more than one) onto the external device. The image is an exact copy (sometimes referred to as a "bit copy" or "sector by sector copy" of the original. It includes not only the visible files on the original disk but others which would normally not be seen, the parts of the disk that contain the information from which the directory details are obtained (file names, sizes, date and time stamp) and also certain other forensic fragments from previously deleted files can sometimes be recovered. The "image" file itself cannot easily be viewed, but by reversing the imaging process onto a second computer similar in specification to the original, an exact clone of the original disk,

---

more specific, non-consensual searches could be conducted under PACE s.9 and sched.1, to which Code of Practice B applies.

[23] The use of the word "image" is a little confusing as people also refer to files containing pictures as images.

[24] Products to achieve this include DIBS - Digital Image Backup System - and Vogon/Authentec FlightServer, both of which are aimed at professional forensic users but the essential facilities are available within PowerQuest's much cheaper utility, DriveImage 2.0.

[25] *R v City of London Magistrates' Court and the SFO, ex p.Greene* [1998] *Crim LR* 54-56 records a dispute over the adequacy of the word "download" used in an injunction to describe what happens in these circumstances

including all the “hidden” information is created. This process is sometimes called “extraction”. The procedures used have certain controls in-built: the original computer remains available for inspection; often two image copies are made, one to act as a control in a manner similar to that used where police-station interviews are taped. In addition, the images and the “extracted” files are recorded to CD-ROM, which is a Write Once, Read Many medium which cannot be altered. CD-ROMs made in these circumstances are usually disclosed to the defence. A further feature of the procedures as used by some law enforcement agencies is that, where ever possible, there is a separation between technicians who operate on the raw computer evidence and investigating officers involved in analysing the results. Essentially these protocols address the issue of *freezing the scene*. Witness statements and interview records[26] are needed in support and to provide *continuity of evidence*.

Followed properly, hard-disk imaging is uncontroversial. From an admissibility perspective, the computer and its hard-disk are "real evidence"; all subsequent images, copies, print-outs etc are "documents" and at the moment appear to need section 69 certification. Problems arise from the types of material produced from the hard-disk and the inferences that may be made, for example:

- *simple data files* - word-processed documents, database and accounts records, pictures,[27] copies of faxes - produced from regular applications present little difficulty. The date-and-time stamp which can be displayed in the computer's directory is of last modification rather than original creation. Some applications generate records of first creation and also list modifications, but most do not. PCs do not normally create formal audit or logging records
- *e-mail messages and faxes*, sent and received, may have been retained by the computer owner; but the owner may also have selectively deleted some of them
- sophisticated *extended use of directory information* can help build up chronologies of events within a computer, but the data available may be incomplete or imperfect and significant amounts of interpretation may be needed. The basic tool is to request a list of all files in all directories on all disks sorted in date/time order. The chronologies may show, among other things: when an operating system was installed, reinstalled or upgraded; when an application was installed, re-installed or upgraded; when new hardware was installed or reinstalled; sessions during which files were being created or modified; sessions in which files were viewed without necessarily being modified; dates when faxes were sent and received; sessions online to the Internet and other external services; times when diagnostic packages were run because of some suspected system fault;
- *deleted files*, particularly if the deletion is recent, can be recovered using facilities built into modern operating systems to provide resilience against accident. This is possible because initially unwanted files are only marked for deletion so that they do not appear in a disk directory though the content remains until the specific disk space

[26] For example under PACE Code of Practice C.
[27] *R v Fellows and Arnold* [1997] 1 *Cr.App.R.* 244, C.A.

occupied is re-used by newer files. This type of undeleting is uncontroversial, but technicians can also sometimes recover fragments direct from disk sectors; here a greater element of interpretation may be needed. Careful examination of certain application files, for example documents created in Microsoft Word, may include fragments which the creator believes has been discarded. The danger here is that a computer technician, in making a reconstruction of a document, becomes influenced by other aspects of the investigation.[28]

- *swap files* are temporary files created on hard-disk by operating systems when there is insufficient random access memory (RAM) for a specific activity, for example when several programs run simultaneously, or a large document or picture is being edited. Here again a technician may uncover evidence of recent activities, including alterations and deletions to files, or the transmission of passwords. Here too one technician's interpretation may be challenged by another.

If an individual PC is handled properly at and after seizure and if it was within the sole control of a suspect, a great deal of important evidence about the suspect's activities is potentially available. However some of the conclusions offered by prosecution experts may depend on interpretation rather than uncontestable fact-finding, and the extent of this may not be obvious.

Larger Corporate Systems: The larger the computer system, the greater the difficulties of transporting it anywhere, particularly if the system is extensively networked and consists of a number of disparate computers, linked together by networks for some purposes and not for others. The larger the computer system, on the whole the greater the potential that its seizure will cause collateral damage to wholly innocent individuals and organisations; once a computer is seized the business that owned it is likely to come to a sharp halt, affecting employees, customers and creditors. In these circumstances there are no clear guidelines.[29] Investigators then have to make a decision to leave the hardware *in situ*, hope to locate an employee of the raided firm who is technically competent but not under suspicion or other person, and supervise that person while copies of operating systems, logs, software and data are made. Section 19(4) of PACE permits a constable to "require any information which is contained in a computer and accessible from the premises [referred to in the warrant] to be produced in a form in which it can be taken away and in which it is visible and legible". The reference to "accessible from" seems to suggest that provided a warrant referred to a single relevant site, the whole of a corporate network, where ever its components were located, would be included. In practice a selection may have to be made on grounds of cost and bulk. Investigators also need to acquire a

[28] Deleted files can be recovered from mainframes and pocket computers as well. As long ago as 1986 drug smuggler Paul Dye was convicted on the basis of files, apparently deleted but recovered from a Psion personal organiser: Channel 4 News, 27 November 1986; *DataLink*, 1 December 1986; *The Guardian* 7 March 1988. A more celebrated example was that of the recovered White House e-mail records of former National Security Advisor, John Poindexter, during the Iran-Contra Affair (*United States v Poindexter*, Crim No 88-0080-1)

[29] PACE s.16(8) states "A search under warrant may only be a search to the extent required for the purpose for which the warrant was issued."

detailed hardware and software inventory of the computer system, plus any reports prepared by EDP auditors and the like. If the computer system belongs to an international company, there may be different components in different jurisdictions and time-zones.

Once the raw evidence has been acquired, the problem is to show that it can be relied on. Again some of the tests developed in the section 69 cases can be extended to other aspects of probative value. Thus, in the appeal in *R v Cochrane*[30] which concerned print-out from an automated teller machine (ATM) connected to a complex banking / building society system, Waterhouse, J observed: " It is with some surprise that we record that none of the witnesses who gave evidence in the court below knew even the name of the town in which the mainframe computer was located." He concluded:

> "In the end, however, it is clear that, whether or not the judge's view was that section 69 of the 1984 Act applied or that at least some of the entries in the till rolls relied upon by the prosecution were real evidence in the sense that they were direct evidence of the transactions carried out, it was necessary for evidence to be adduced on behalf of the prosecution to explain how each of the relevant pieces of information on the till roll came into existence. In particular, it was necessary that appropriate authoritative evidence should be called to describe the function and operation of the mainframe computer, including the extent to which it brought to bear information stored within it in order to validate a transaction and to enable an appropriate record to be made on the till roll."

He went on: "It is necessary to add that the problem of proving transactions of this kind must now arise frequently and it should be possible for the Crown Prosecution Service to devise a standard form of evidence to deal with it." While one sympathises with the judge, there are formidable difficulties in envisioning a "standard form of evidence". Indeed since 1989 when the events in *Cochrane* took place, computer systems have become much more complex and now include personal computers. We will return to this matter later.

Evidence from the Internet: There are two principal situations to be considered: where the offence is concentrated on an individual's use of the Internet and where a remote site holds evidence of an offence. Typical examples of the former include the downloading of paedophiliac material and unauthorised access; a great deal of evidence may exist on the accused's own computer. Examples of the latter include: evidence of fraudulent promises to deliver goods,[31] evidence of fraudulent offers to provide services,[32] evidence of fraudulent or non-compliant investment offers,[33] infringed copyright materials offered in the course of a business,[34] holding or offering pornographic files and pictures,[35] and incitements to racial hatred, terrorism and other offences,[36] and conspiracies.[37]

---

[30] [1993] *Crim LR* 48
[31] Under Theft Act, 1968 ss 15(1) and 16.
[32] Under Theft Act, 1978 s.1.
[33] See, for example, Drinkhall, J., "Internet Fraud", (1997) 4(3) *Journal of Financial Crime* 258.
[34] For example, under Copyright Designs and Patents Act 1988 s 107.

To understand where evidence of Internet-related offences maybe located we need to recall how Internet connections are made and the forms they may take. Typically an individual uses his computer to connect to the Internet via an Internet Service Provider (ISP); home users dial in via a telephone network. There are thus four points at which evidence of various sorts may exist: on an individual's own computer, in his telephone bill, at the ISP and on remote sites. For law enforcement there is also the possibility of eavesdropping on Internet traffic in transit using a technique called "sniffing".

Considering, first, material held on a suspect's own computer, in addition to the material already referred to, PCs are likely hold the following Internet-specific logging files:

- e-mails sent and received are usually saved to hard-disk during routine use; however, most users regularly delete unwanted material to free up disk space;
- newsgroups subscribed to are also usually saved to hard-disk during routine use; however again, most users regularly delete unwanted material to free up disk space;
- Internet Relay Chat (IRC) sessions are real-time discussions rather like CB radio; logging files which record what all participants have said are optional. There are also commercial and improved versions of IRC like Microsoft Netmeeting and other products which provide Internet telephony and viewphones; again logging may exist;
- browser cache files are a specific sort of temporary file which is used to store data that the computer has recently used and may want again in the very near future. Although caching is used throughout computing, one of the most significant uses is within Internet browsers, the software used to visit sites on the world wide web. Here the cache stores copies of each web page as it is visited. Users often need revisit previously seen pages, particularly if they containing an index to other pages. The browser software can swiftly retrieve such a page from its cache rather than going back to the original source site (which would result in greater delay to the user and also add to the overall traffic on the Internet's main connections). In most browsers cache files are kept after individual sessions, often for weeks and months afterwards; some browsers and some specialist software can be used to view cache files and also associated "history" files which retain some date-and-time information. Thus it is possible to determine what the users of a specific computer have been viewing and, to a limited extent and after careful interpretation, when. There has been at least one attempt by prosecutors to assert that material saved in a web-browser cache but not otherwise intentionally retained constitutes "possession" for the purposes of section 160, Criminal Justice Act, 1988[38].

---

[35] An extensive review of US and English law appears in Akdeniz, Y., "Computer Pornography; a Comparative Study of the US and English Obscenity Laws and Child Pornography Laws in Relation to the Internet" (1996) 10(2) *International Review of Law, Computers and Technology* 235.

[36] Racial hatred offences include Public Order Act 1986 ss 18,19,21 and 23; terrorism is defined in the Prevention of Terrorism (Temporary Provisions) Act 1989 s.20. Simple incitement of another to commit an offence is a common law misdemeanor. Blasphemy also remains a common law misdemeanor - *Whitehouse v Gay News Ltd and Lemon* [1979] *A.C.* 617.

[37] Criminal Law Act 1977 s 1(1).

[38] Hamilton, A., "Caught Looking", *Computers & Law* August/September 1998, Vol 9 Issue 3, pp 9-10

It is sometimes possible to recover deleted logging files. However the completeness of any of these files, previously deleted or otherwise, and the extent to which date-and-time stamps are accurate is a matter that a person producing such forms of evidence must expect to be asked to demonstrate.

As regards telephone logs, private customers of ISPs usually dial-in via telephone - so, the logs provided by telephone companies showing numbers called, time and duration often give powerful corroboration to other types of evidence[39]. Until relatively recently phone companies collected this type of information from specialist external devices attached to a subscriber's line: from an admissibility perspective it is possible to argue that the output of such call loggers or monitors is real evidence. More recently exhibits have been produced direct from the telephone company's regular billing computer. Although there are so far no recorded cases on the point, it could be argued that in these circumstances a proper section 69 PACE certificate is needed as well as support to show that the exhibit is a "business etc document" for the purposes of section 24 of the Criminal Justice Act, 1988. If law enforcement wish to capture data traffic on a telephone line between an ISP and its customer, the Interception of Communications Act, 1985 (ICOA) applies.[40]

The material held by an ISP may also provide evidence. The ISP may be a commercial entity specifically in business for the purpose or may be an existing body such as a university institution. Business customers may have a permanent link, a leased line, to the ISP. In addition to providing the necessary connections to the Internet, ISPs maintain their own computers to log in subscribers and to hold e-mail and Usenet messages against the time when subscribers wish to collect material. The computers holding e-mail and Usenet messages are known respectively as mail-servers and news-servers. Potentially mail-servers and news-servers can provide evidence of message content. The current law enforcement procedure appears to be as follows:[41] applications to ISPs to disclose the identity of their customers are made on forms under the Data Protection Act, section 28(3). The position of message content held on ISP computers is more complex: ACPO believe they should use the Special Procedure within PACE[42] to obtain warrants. So far there are no test cases to determine whether an ISP's news server and mail server computers are part of a public telecommunications service, in which case ICOA might

[39] Law enforcement officers obtain this information in respect of phone lines owned by private individuals by supplying the telephone company with a form referring to Data Protection Act, 1984, s. 28(3). How far that Act extends to business lines will depend on the likelihood that the business is dealing in personal information. In any event, s.28(3) merely authorises a data user to make a disclosure to the police but does not obligate them to do so; it is therefore distinguishable from the duty imposed by a production order or warrant.

[40] In practice, it would seem that the s.28(3) procedure is preferred - the police search the records and data stored on the ISP servers rather than intercept traffic.

[41] Letter from the Chairman of the ACPO Computer Crime Committee to the *Sunday Telegraph*, 28 September 1998.

[42] Defined in ss. 9 and 14 and detailed in Schedule I.

apply.[43] ISPs can of course volunteer to help the police without insisting on a warrant but then may later face claims from their subscribers under the Data Protection Act or for breach of confidence. Although the police could also be sued for breach of confidence,[44] the main practical penalty they face for failure to use appropriate procedures is that a judge may use his discretion to exclude unfairly acquired material under section 78, PACE.

Next, there may be material relevant to the investigation held on remote sites. If, for ordinary purposes we wish to record the contents of a web-page on a remote computer the simplest way of doing so is to use the appropriate menu command within the browser software and print it out; alternatively it can be saved to disk. This would be wholly inadequate for evidential purposes:

- some of the facilities within the browsers to save WWW pages to disk are imperfect; text may be saved but not associated images; again, with some very complex pages (for example, involving "frames" and "templates"), what is seen on screen and what is saved to disk may be quite different
- the method used to save a file to disk may not carry any individual labelling which shows where and when it was obtained
- such saved files are very easily modified or forged; accidental alteration is also a substantial hazard
- because of the browser cache facility there is no immediate, fool-proof way of telling when a specific page was last acquired. Thus if a whole series of cached pages are examined an entirely false picture could be built up - the pages are almost certainly not contemporaneous. Moreover, during a live session, what is produced on screen could be a mixture of pages immediately acquired from the remote computer and others acquired earlier on.
- caches exist elsewhere. Many Internet Service Providers have facilities known as proxy servers to speed up the delivery of popular pages and limit congestion problems on the network. Thus a customer of such an ISP may not be able to be sure that what he has received on his computer is the latest version from the source computer as opposed to an earlier cached version held by his ISP.
- When the World Wide Web is used as an interface for electronic commerce, further problems appear. The pages of instruction which are converted into the pages the user actually sees have often been created on-the-fly by the remote computer, which itself may be linked to a further conventional "accounts", "catalogue", "sales/invoice" or "retail bank" computer. Thus, no immediate complete record of what the user actually saw may exist at the remote computer either, though presumably for many purposes the owner of that computer would

[43] But the search of recorded data on a server is presumably not an "intercept". Part of such a search may be akin to the searches of call logs under sched.2 of the ICOA but investigation of the content of stored messages arguably falls outside of the ICOA altogether.

[44] But see *R v Chief Constable of North Wales Police ex p.AB* [1998] 3 *W.L.R.* 57.

like to be able convincingly to demonstrate to others the terms and facts of a transaction.

But this is only part of the problem faced by prosecutors: How can they show that the remote computer was behaving reliably at the time? This is important for "weight" even if we discard the need for section 69 certification. Again, how can they show that data has been obtained from a specific computer and nowhere else; website forgery is not uncommon [45]. Can prosecutors link the material from the remote computer to the person accused? Given the volatility of computer files, acquisition also usually needs to be linked to a specific day and time. This level of authentication cannot be done within a purely technological / computer context but will require other forms of evidence such as witness statements, exhibits indicating ownership of or access to the computer and/or data media, or the possibility of inference from the nature of the content of the files. Can the producing witness give a full and believable explanation of the processes by which the file was acquired from the remote computer to the user's machine to show that the result is accurate, free from contamination and complete? How was the evidence frozen and rendered tamper-proof? [46]

A further problem arises if a complainant needs to demonstrate the existence of a computer-mediated contract, possibly fraudulent, to show that an offer was made and accepted and that authority was given for a payment[47]. Current advice to web-designers suggests that each stage is marked by some positive act by the purchaser, a "click" or "enter" in an on-screen-form. What evidence does a purchaser/victim acquire in these circumstances?

In effect the only plausible route to acquiring evidence from a remote Internet site is to seize the remote computer itself. That in turn depends on its being within the jurisdiction of the courts to which investigating officers have access.

The final possible source of evidence is eavesdropped Internet Traffic. The principles of Internet eavesdropping are well known to technicians: Internet traffic is despatched as a series of "packets", each of which contain information about originator and destination as well as the actual content. Packets are also numbered so that they can be correctly re-assembled if they arrive out of order. An eavesdropping computer anywhere between the originator and destination can capture a transmission and re-construct it. The practical problems are that at certain points along the path there will be vast amounts of regular Internet traffic to be sifted in order to find the material being sought and in any event it is basic to the design of the Internet that, even within the transmission of a simple e-mail message, constituent packets may use radically different

[45] For example, the Labour Party website (<http://www.poptel.org.uk/labour-party/>) was "spoofed" in 1996: *The Guardian* 10 December 1996. The weakness that is exploited arises from the fact that most websites are updated remotely: the pages are created on computers other than the one hosting the site and are FTP'd over the Internet. Packet sniffing enables hackers to identify packets carrying FTP requests destined for the website and which carry sequences associated with log-ons and passwords.

[46] For a more extended discussion, see Sommer, P., "Evidence from Cyberspace: Downloads, Logs and Captures" (1997) 5(2) *Journal of Financial Crime* 138.

[47] See Gringras, C., *The Laws of the Internet* (Butterworths, London, 1997) Chapter 2 *passim.*

routes, thus creating the possibility that not all of the relevant traffic has been captured. The most effective forms of eavesdropping take place very close - in terms of the topography of the network - to an originator or recipient[48]. For law enforcement wishing to rely on such evidence there is a further problem: the defence will seek disclosure of the precise tool used for eavesdropping and its network location, arguing that without such information the reliability and completeness of the evidence cannot be assessed. A judge asked to consider an application for Public Interest Immunity may also simultaneously be asked to exclude the evidence all together for unfairness.

A number of examples of Internet-eavesdropped evidence were produced by USAF officers in the form of keystroke monitoring in *R v Pryce and R v Bevan*, where two young men were accused of unauthorised access into large numbers of computers owned, *inter alia*, by the United States Air Force and the defence company Lockheed.[49] The decision of Pryce to plead guilty on reduced charges and the abandonment of charges against Bevan stopped any court-room examination of the evidence.

In practice most Internet and online crime appears to be prosecuted on the basis of evidence found close to the suspect - the computer hard-disk, other data, media and artefacts found on premises associated with the accused, as well as telephone logs[50]. Thus, both in *R v N*[51], N's defence that a business rival had planted paedophiliac pictures and text on disks found in his possession and in *R v W*[52], W's assertion that similar material had been planted on his computer by a lodger, failed to persuade in the face of a detailed analysis of time-stamped logging files on their computers corroborated by telephone logs. On the other hand, in *R v G*[53], G was charged with incitement to commit offences under the Computer Misuse Act, 1990, on the basis of a file containing very detailed instructions available for download by visitors to a bulletin board system (BBS) he was running. His defence was that the BBS had been set up for legitimate purposes but that he had been persuaded to add libraries of many more files in order to increase the number of visitors, that he had acquired these further files in bulk had not examined them for content and thus lacked the necessary *mens rea* for incitement. An examination of the computer, the BBS software and the file time-stamps provided strong corroboration for this defence as a result of which the CPS dropped the charge. Poor handling of hard-disk evidence by investigators employed by an industry-funded software anti-piracy enforcement body in *R v Y*[54], another bulletin board case, this time involving charges under section 107 of the

---

[48] See Sommer, P., "Intrusion Detection Systems as Evidence", Proceedings of RAID98, Louvain-la-Neuve, 1998

[49] The events took place in 1994, and the monitoring tools were called Stethoscope, Network Security Monitor and Pathfinder. The cases finally came before the UK courts in 1997 (Bow Street Magistrates' Court); the author acted as defence expert. The (US) General Accounting Office Report GAO/AIMD-96-84 Defense Information Security and the Testimony of Jim Christy, Air Force Investigator, Senate Governmental Affairs Committee Permanent Investigations Sub-Committee, “Security in Cyberspace”, June 5 1996, provide a description and give an idea of how the US authorities viewed the case.

[50] So far there do not appear to have been any relevant surveys; this commentary is based on case and newspaper reports, the author's own experiences and anecdotes from prosecution and defence experts.

[51] Bristol Crown Court, January 1998

[52] Bicester Magistrates' Court, July 1998

[53] Bow Street Magistrates' Court, January 1998

[54] Watford Crown Court, June 1996

Copyright Designs and Patents Act, 1988, forced prosecutors to abandon this form of evidence in seeking a conviction. Examinations had been carried out on the hard-disk found at the accused's home rather than a copy; the circumventing of security measures and the explorations of various consultants, not all of them properly recorded in witness statements, were clearly visible to the defence expert.

Most successful prosecutions rely on more than one stream of computer-derived evidence. What is needed is a multiplicity of independent streams of evidence, both computer- and non-computer-derived, which corroborate each other. Any single stream may fail either because of intrinsic inadequacy or because the courts find it too difficult to understand.

Are there any general principles for evaluating computer evidence?

Computer-derived evidence is not intrinsically different from other types of evidence produced in criminal proceedings. Rather the problems arise from the fragility and transience of many of the forms of computer evidence, the fact that provenance may be difficult to understand and the speed with which computer technology, and hence the evidence potentially available, changes.

There are few easy solutions. As we have seen, Waterhouse, J hoped for "a standard form of evidence",[55] but English law is hostile to the idea of giving scientific or forensic evidence a juridical quality. In *R v Doheny*,[56] DNA statistical evidence was produced in a rape and buggery case. The conviction was overturned on appeal on the basis that the expert had overstepped his role, restricting the role of the jury. A move to the US procedure of expecting judges to act as the gatekeeper for novel scientific evidence, most recently considered in the 1993 US case of *Daubert v Merrell Dow*,[57] is not promising either. Even if the English courts accepted the principle, it is doubtful whether some computer forensic evidence currently being tendered would meet the tests of (1) whether the theory or technique can be (and has been) tested; (2) the error rate associated with the method; (3) publication in a peer-reviewed journal; and (4) whether the technique has gained widespread acceptance. The Royal Commission on Criminal Justice chaired by Lord Runciman[58] devoted Chapter 9 to a consideration of Forensic Science and Expert Evidence proposed *inter alia* the setting up a Forensic Science Council,[59] but how well equipped would it be to assess skills in computer forensics? Similar concerns must apply to the notion of court-appointed experts - how would they be selected? Many of these proposals would have the effect of denying the criminal justice system the benefits of the new techniques. And yet nearly all the arguments about

[55] Waterhouse, J in *R v Cochrane* [1993] *Crim LR* 48,
[56] *R v Doheny, R v Adams* [1997] *Crim LR* 669.
[57] (1993) 509 U.S. 579.
[58] Cm2263, HMSO, London.
[59] Chapter 9.33, recommendation 262. See further Forensic Science Working Group, *Report* (Royal Society of Chemistry, London, 1997), described in Walker, C., and Stockdale, R., "Forensic evidence" in Walker, C., and Starmer, K., *Miscarriages of Justice* (Blackstone Press, London, 1998, forthcoming) chap.6. See also Erzinçlioglu, Z., "British forensic science in the dock" *Nature* 392, 859-860 (1998)

the safe acquisition and preservation of computers and hard-disks and forms of listing computer-derived materials in search registers. It would provide guidance for those issuing warrants. It would add to the existing framework for the maintenance of adequate safeguards and records. It would provide fair rules and procedures for the rapid post seizure return of computer hardware and data so that the activities and privacy of companies and individuals are not unduly penalised but without the need for constant recourse to the Police (Property) Act 1897. It would give guidance for judges in assessing the process by which a computer-derived exhibit has arrived in court and/or in assisting. It would provide greater fairness to the defence, including procedures for delivery of exhibits and access to specialist software necessary to review the validity of prosecution claims. It would lead to fewer "form" protests by the defence in court or for irresponsible questioning of crown experts as feared by the Law Commission in its Consultative Paper in 1995. It would reduce the costs of trials involving computer-related evidence by the avoidance of the delivery of unnecessarily bulky prosecution bundles of print-out and by allowing prosecution and defence experts access to electronic evidence which can then be analysed with computers. It would provide a framework for specific training of law enforcement officers, leading to greater efficiencies and higher chances of success, while ensuring that fewer poor quality cases are presented to the courts. Finally, it would provide the Legal Aid Board with guidance in assessing the requests for funding by defence interests.