

UNIVERSITY OF SOUTHAMPTON.

**TECHNOLOGY AND ITS EFFECT, UPON THE INVESTIGATION OF,
AND PRESENTATION OF EVIDENCE IN, SERIOUS FRAUD CASES.**

by

Arthur Philip Whittick.
Detective Superintendent
of the Metropolitan Police
Company Fraud Department.

Thesis submitted to the University of Southampton
in fulfilment of the requirements for the degree of

Master of Philosophy

1989.



I dedicate this thesis to my family.

TECHNOLOGY AND ITS EFFECT, UPON THE INVESTIGATION OF,
AND PRESENTATION OF EVIDENCE IN, SERIOUS FRAUD CASES.

CONTENTS.

	<u>Page No.</u>
Abstract.	i
Acknowledgements.	ii
Table of cases cited.	iv
Table of statutes.	v
List of tables and table of figures.	vi

CHAPTER.

ONE. TECHNOLOGY AND THE FRAUD INVESTIGATOR.

A.	Introduction.	1
1.1.	The impact of technology upon the investigation of fraud.	2
1.2.	Technology and its human interface.	7
1.3.	The technology environment of fraud investigators.	10
1.4.	Visual display technologies.	15
1.5.	Teleconferencing and computer links.	20
1.6.	Expert systems.	25
B.	Conclusions.	27

TWO. ADMISSIBILITY OF COMPUTER RECORDS.

A.	Introduction.	28
2.1.	Authentication of evidence.	29
2.2.	Real evidence.	33
2.3.	Judicial notice and presumptions.	38
2.4.	Admissibility of computer records by statute.	41
2.5.	Police and Criminal Evidence Act 1984.	44
2.6.	Criminal Justice Act 1988.	48
2.7.	Miscellaneous other statutes.	52
B.	Conclusions.	55

CHAPTER.

**THREE. COMPUTER FRAUD INVESTIGATION AND ADDUCTION
OF COMPUTER RECORDS.**

	<u>Page No.</u>
A. Introduction.	56
3.1. An interpretation of computer fraud.	57
3.2. Guarding against computer crime.	60
3.3. Investigation of computer crime.	63
3.4. Pre-trial adduction of computer records.	70
3.5. Preparatory hearings.	75
3.6. Trial.	80
B. Conclusions.	83

FOUR. PROSECUTING SERIOUS FRAUD WITH TECHNOLOGY.

A. Introduction.	84
4.1. The Serious Fraud Office.	85
4.2. Presenting complex information to juries.	88
4.3. Courtroom technology.	93
4.4. Technology on trial.	98
4.5. Televised evidence.	105
B. Conclusions.	108

FIVE. RESEARCH RESULTS AND CONCLUSIONS.

A. Introduction.	109
5.1. Resources.	111
5.2. Developments in technology.	116
5.3. Career prospects and training.	120
5.4. Reform and initiatives.	124
5.5. Regulating computer generated evidence.	126
5.6. Summation of questionnaire findings.	128
B. Final conclusions and recommendations.	131

ADDENDUM, APPENDICES AND BIBLIOGRAPHY.

138

onwards

UNIVERSITY OF SOUTHAMPTON.

ABSTRACT.

FACULTY OF LAW.

PHILOSOPHY.

MASTER OF PHILOSOPHY.

TECHNOLOGY AND ITS EFFECT, UPON THE INVESTIGATION OF, AND
PRESENTATION OF EVIDENCE IN, SERIOUS FRAUD CASES.

by Arthur Philip Whittick.

Technology has much to offer those whose duty it is to investigate and prosecute allegations of serious fraud. However, many people who were educated in the pre-microchip era, often appear to regard devices such as the computer, as an unwelcome medusa to their workplace. But it is not only psychological barriers that have added an aura of mystique to these modern technologies, as there have also been legal uncertainties over their application in both the civil law and the criminal law. Here, constant and sometimes Procrustean incursions, have affected the rules of evidence linked to documents which are derived from computers and other electronic media.

This thesis examines the admissibility of electronically produced documents including computer records, which encompasses an area of law that has been affected by considerable statutory regulation. The most significant of these statutes determine the criteria for the admissibility of computer generated evidence, and the manner in which information technology is perceived, as a presentational aid to long-suffering juries in fraud trials. The research undertaken during this study, also considers the McMillenesque wind of change now evident in the corridors of fraud policing in this country, due to an increase in the use of information technology. This progress being synonymous with a number of recommendations made by the Fraud Trials Committee, in their 1986 Report.

In the final part of this thesis, recommendations are proposed, which, in the view of the researcher, would help to establish a structured and nationally coordinated approach, to future IT objectives in fraud policing. These recommendations whilst taking into account the paucity of police resources allocated to the campaign against fraud, also propose that there is a need to consider guidelines for certain forms of evidence of a documentary nature, which, when derived from the medium of electronic devices, may be subjected to unnecessary risk of challenge through failure to follow prudent precautions.

ACKNOWLEDGEMENTS.

I am indebted to the many people who have helped me in preparing this research. Heading my list of preferential creditors, are: Commander Malcolm Campbell and former Detective Chief Superintendent Michael John, of the Metropolitan and City Police Company Fraud Department. Their valued support at the outset, gave me the boost of confidence that I needed, and their tentacles of influence which spread beyond the Police Service into the world of commerce, enabled important areas of my work to gain momentum elsewhere. I am also grateful to Mr Campbell for agreeing to act as the police nominated supervisor of this research project, and for the active support that he gave me in that capacity.

Detective Sergeant Peter Bennett must also be given credit for his part in furthering the aims of this research. Particularly for his enthusiastic assistance in pioneering the use of technology in fraud trials, at a time when its advent was regarded with uncertainty, and sometimes even suspicion, by those who were unfamiliar with these new techniques. His subsequent development of this work has earned the respect and admiration of many policemen and members of the legal profession.

An important clue as to the overall size of my debt, is evinced in the revelation, that some of my affairs were investigated by senior members of the Institute of Chartered Accountants in England and Wales. Due to the public spiritedness of those such as Douglas Llambias, Michael Groom and Trevor D'Cruz, and several other volunteers, the enquiry centred around the future IT needs in fraud policing. This exercise proved to be an excellent example of voluntary public service and inter-agency

cooperation and was completed with efficiency, and, fortunately, without damage to my own personal wealth.

This citation of preferred creditors would not be complete without an expression of appreciation to the trustees of the Bramshill Fellowship Award scheme and my own employers, who funded this research. The Commandant and others of the Police Staff College at Bramshill, also provided generous facilities which enabled me to extend my research into other important areas of this work.

Finally, but in terms of chronology only, is the debt of gratitude that I owe to the Faculty of Law at Southampton University, where the majority of this research was carried out. Particular thanks are due to, my academic supervisor Stephen Saxby, for his sharp thinking which cut across academic red-tape with surprising dexterity, thus allowing this research to commence at the earliest opportunity, and in tandem with the many legal reforms and technological developments that are currently taking place. Indeed, had it not been for his early recognition of this research potential, important initiatives might well have been lost. I would like to thank Andrew Rutherford for his supporting supervisory role and for his sound advice, which enabled me to prune down this thesis into a manageable size. The advice afforded me by Doctor Ralph Beddard at times of need, is also much appreciated.

Due to reasons of brevity, there are many non-priority creditors who must sadly remain anonymous, but whose collective input has nevertheless added to the solvency of this research.

Table of Cases Cited.

- Anton Piller K.G., v. Manufacturing Processes Ltd. (1976)
Ch. 55, CA.
- Barber J. and sons v. Lloyds Underwriters (1986) 2 All ER
845 QB.
- Barker v. Wilson (1980) 2 All ER 81. QBD.
- Booker McConnell PLC v. Plascow (1985) RPC 425 CA.
- Castle v. Cross (1985) 1 All ER 87 QBD.
- Flight v. Robinson (1844) 8 Beav 22.
- Gates v. Swift (1981) FSR 57, Ch (order only). (1982) RPC
339, Ch (also including headnote and argument of
counsel).
- Humphrey v. Dale (1857) 7 E & B 266.
- Kajala v. Noble (1982) 75 Cr App R 117, CA.
- Myers v. DPP (1965) AC 1001, HL.
- People v. Superior Court of Santa Clara County, 104 Cal,
3rd 1001. 163 Cal. Rptr. 906 (1980).
- R. v. Adelaja and others (1988) unreported. CCC.
- R. v. Ewing (1983) QB. 1039.
- R. v. Hall. The Times, 10th February, 1987.
- R. v. Gardner and others (1987) unreported. CCC.
- R. v. Gold and another.
- R. v. Maqsd Ali (1966) QB 688, CCA.
- R. v. Patel (1981) 73 Cr App R. 117, CA.
- R. v. Pettigrew (1980) 71 Cr App R. 39, Ca.
- R. v. Relton and others (1988) unreported CCC.
- R. v. Robson and Harris (1972) 2 All ER 699, CCA.
- R. v. Shone (1982) 76 Cr App R. 72, CA.
- R. v. Stevenson (1971) 1 All ER 678, Ass.
- R. v. Wayte (1982) 76 Cr App R. 110, CA.
- R. v. Wiles (1982) Crim. L. R. 699.
- R. v. Wood (1982) 76 Cr App R. 23, CA.
- R. v. Wood Green Crown Court ex parte P. (1982) 4 FLR 206,
Fam D.
- Sophocleous v. Ringer. Times Newspaper 10th February,
1987.
- The Statue of Liberty (1968) 2 All ER 195, PDA. (Cal.
Super Ct 1972).
- Ward v. Superior Court. See 3 Computer L. Serv. Rep. 206.

Table of Statutes.

Bankers' Books Evidence Act 1879.

Banking Act 1979.

Civil Evidence Act 1938.

Civil Evidence Act 1968.

Civil Evidence Act 1972.

Companies Act 1985.

Criminal Evidence Act 1965.

Criminal Justice Act 1987.

Criminal Justice Act 1988.

Data Protection Act 1984.

Drugs Trafficking Offences Act 1986.

Forgery and Counterfeiting Act 1981.

Police and Criminal Evidence Act 1984.

Solicitors Act 1974.

List of Tables and Table of Figures.

List of Tables.

<u>Table No.</u>	<u>Description.</u>	<u>Page No.</u>
1.	Availability of facsimile equipment to fraud squads.	14
2.	Reported increases to fraud squad manning levels.	112
3.	Reported decreases to fraud squad manning levels.	112
4.	Distribution of computers to fraud squads.	113
5.	Distribution of specialist trained fraud squad officers.	121

Table of Figures.

<u>Figure No.</u>	<u>Description.</u>	<u>Page No.</u>
1.	Example of a franking machine crime prevention slogan.	19
2.	Investigating computer crime.	68
3.	Technology in court.	94
4.	Spreadsheet illustration.	99
5.	Non-electronic document retrieval system (diagram).	102
6.	Example of computer graphics used in fraud trial.	104

CHAPTER ONE.

TECHNOLOGY AND THE FRAUD INVESTIGATOR.

A. Introduction.

The police service, in common with society in general, is struggling to familiarise itself with the glut of technology that is now becoming widely available. Whilst derivatives of microchip technologies such as computers, hold centre stage in terms of recent rapid growth, there are also many other devices and techniques that are making incursions into the field of fraud policing.

Not all of these devices are necessarily sophisticated, and some may even be described as ancient, as for example when overhead projectors are used to present complex information to fraud trial juries. Developments in the way that technologies are converging with the multi-disciplinary skills of those such as the artist, graphic designer and many others,¹ is yet a further example of how the phenomena of technology is permeating the ionosphere of modern fraud policing.

This chapter therefore considers the apparent upsurge in the recent use of technology by fraud squads nationally, with particular relevance to the progress made since the Fraud Trials Committee's Report was published in January, 1986. As much of the fraud investigator's work is conducted behind the scenes in an office environment, it is hardly suprising that several of the technologies now to be discussed, have broad similarities with automated office systems commonly used in the world of commerce.

1. For a brief discussion on how these skills are converging, see page 6, below.

1.1. THE IMPACT OF TECHNOLOGY ON FRAUD INVESTIGATION.

Despite the fact that the working environment of fraud squad officers has been allowed to keep pace with developments in reprographic and other forms of modern office technology, the incursion of the computer as an investigative tool has been slow to evolve. There are a number of reasons that may be advanced for this vacuum in progress. One causal factor proposed by Levi. M., (1987 at p.138) draws attention to the low priority that fraud often receives from senior officers in the police service, which is reflected in the inadequate resources that are allocated towards investigating this category of crime.

There is also a case for arguing that since society in general lacks an awareness of the phenomena resulting from the technological revolution as described by Sherman. B., (1985 at p.29) that, this lethargy has in turn affected the attitudes of fraud investigators in recent years. Sherman (ibid. p.29) comments on the paradox that exists in noting, that irrespective of the fact that 'computers are the ubiquitous technology affecting the citizens of an industrialised society from pre-cradle to the grave, it is a wonder that so few people know anything about them'.

Others who comment on the inadequacy of police resources in terms of fraud investigation are the Fraud Trials Committee in their Report (1986a at para. 2.71). Whilst the Committee's Report alludes mainly to manpower shortages, research conducted for this thesis reveals that only one of the forty-three fraud squads in England and Wales who responded to the survey, could lay claim to having its own computer at the time that the Committee's Report was released for publication.

The position that currently exists, however, is a much healthier one. Responses from those 35 fraud squad representatives who replied to this thesis survey regarding computer support, indicate that computer systems are now available to over 48% (i.e. 17) of the fraud squads which responded. Despite the sharp upsurge in the computer support availability that is reflected in the 1988 statistics, by comparison with the 1986 figure, there is, however, little room for complacency when taking into account the realisation that as many as 51.43% (i.e. 18) of the fraud squads that submitted a response, are still without their own computer support facilities.

It is also evident that computer operator training facilities are not sufficiently available to over 29% of fraud squads that said they had their own computer support systems, and furthermore, the national approach to fraud squad computerisation is a piece-meal attempt. This means that developments are often being pioneered in isolation of other fraud squad achievements, thus lacking in the coordination necessary to establish uniformity in standards. This detracts from the other significant advances that have been made in the main-stream of policing, such as the development of the HOLMES (Home Office Large Major Enquiry System), and CRIS (Crime Report Information System), and many others.

The value of computers and other relevant forms of technology, have recently emerged as an important medium for presenting complex information to juries in fraud trials, owing to the attention which has been drawn to the benefits of their use by the Fraud Trials Committee in their Report (ibid. recommendations 55-57 and 102-103). The Criminal Justice Act 1987 now paves the way for 'preparatory hearings', under sub-section 7 (1) of the Act, by virtue of which, the trial judge may now order the

prosecution to prepare explanatory materials to assist the comprehension of juries in cases of sufficient seriousness and complexity. More recent legislative reform has witnessed the enactment of the Criminal Justice Act 1988, which now provides for the furnishing of evidence in any form to help juries to understand complicated issues of fact, notwithstanding the existence of admissible evidence from which the evidence was derived.¹ Further provisions under the Act,² also enables the evidence of certain categories of witnesses to be given via the medium of live televised links.

Technology in the context of fraud investigation, can range from the most complex and sophisticated systems known to man, such as the modern day derivatives of the DENDRAL project, which as noted by Susskind (1987 at p.10) was pioneered by Feigenbaum in the development of artificial intelligence and expert systems. Home Office forensic science laboratories also use various forms of computer assisted devices such as the SEM (Scanning Electron Microscope), whilst at the lower end of the scale, the technologies used in the manufacture of highlighter pen products, may in the opinion of this author, acquire an equally practical status for the presentation of complex information. Since the application of even this basic technique can be used to create a visual 'zoom' effect in order to isolate a singularly important word from amongst many others on a particularly significant document.

1. By virtue of section 31.

2. I.e. under section 32.

Because of the relatively recent emergence of modern information technology systems in the courts, few counsel or even judges, can be said to be totally familiar with these techniques of presentation. Certain forms of technology, such as overhead projectors, whilst modest by comparison with their latter day competitors, are still considered by some exponents of these techniques such as Baldwin. D.,¹ to have an equally important role to play in helping juries to understand complicated issues of fact.

The awareness created by the Fraud Trials Committee in their Report, regarding the need to present fraud cases more effectively, has provoked a number of positive responses by prosecutors in recent fraud trials.² The use of modern forms of technology has not only extended the vocabulary of fraud squads officers, who now refer to electronically prepared schedules as 'spreadsheets', and whose hand-drawn diagrams have been replaced by computer graphics, but it has also added to the content of some job descriptions. An example of this change in title is when computer workstations are manned by police officers during a trial, and they are now referred to as 'electronic exhibit officers',³ to mark the expansion of their work experience in technology.

The effect that technology is now having in other areas of fraud policing relates to familiarity with systems that previously, were unfamiliar to fraud investigators. In

1. Ibid. Fraud in a Good Light. The Police Review, dated 9th August, 1985. At p.1622.

2. For examples of these responses, see pp.93 to 103, below.

3. For a review on the recent use of computer workstations, see Saxby. S., ed., Conference Review. Presentation of Evidence in the Court Room - How IT can help. Vol.4, iss. 1, The Computer Law and Security Report, 1988, at p.12.

terms of police support services, technology is conjoining the disciplines, skills and techniques that are concerned with the reproduction of graphics (consisting of drawings, photographs, illustrations, artwork and text), into the context of a single purpose. This transformation is aptly described by Painter. D., (1988 at p.28) as 'the convergence of skills not previously thought of as a single discipline'.

To attempt a definition of technology in terms of its impact on fraud investigators, would be as inhibiting as trying to define a computer¹, particularly as computers are merely one branch of the technology tree. However, in view of the growing value of technology, both as an investigative tool and as a medium for presenting information to juries, it would seem proper for the purposes of this chapter at least, to consider that the term technology includes,

'Any device or technique that may be used, to aid the comprehension of complex information, at any stage of criminal proceedings.'

1. For a discussion on the futility of defining computers, see generally, Tapper. C., Computer Evidence (1988).

1.2. TECHNOLOGY AND ITS HUMAN INTERFACE.

Technology, in whatever sophisticated form it appears, is simply another tool of mankind. Whilst mankind may rely heavily on the ability of computers to handle large amounts of data with speed and precision, the fact that man has been involved in the manufacturing process of these devices, as well as the subsequent operation and maintenance of them, is not to be overlooked. An appropriate definition of technology in terms of its interface with mankind, and indeed, its relationship with influences outside the infrastructure of a single organisation, is supplied by Naughton. J., (1981 at p.30) to students of the Open University, in this way,

'Technology is the application of scientific and other organised knowledge to practical tasks by hierarchically ordered systems, that involve people and machines.'

An example of a hierarchically ordered system as suggested by the author of this thesis in terms of fraud policing, would be to set standards to enable easy interface to take place between compatible computer operating systems. This would ensure that individual data records could be held in structured fields to enable cross-sectional searching and rapid exchange of data.

The interface of technology, vis-a-vis mankind, encompasses the convergence of the traditional skills of man and his links with developments in technology. An example of this would be the use of transparent materials, such as perspex to build a model of a ship. This technique which required both artisan as well as machine skills, was used to produce a miniature replica of the stricken cargo

ferry the Herald of Free Enterprise, to a court which was enquiring into the Zeebrugge incident. This model having been prepared for the purpose of assisting witnesses in the recall of their testimony.

A more lateral, although extreme example, of man's interface with technology, relates to his exploits with the modules of the American Apollo moon program in the 1960s, regarded by Naughton. J.,¹ as a remarkable achievement even more than a quarter of century later, due to the need of man's involvement in the undertaking by the employment of 40,000 or so scientists, engineers, technicians and computer experts who invested their individual specialised knowledge to provide for the common task.

The skills associated with the development of technology in the police service are no less varied, requiring the joint skills of scientists and artisans to process systems, install, operate and maintain them. Whilst the role of the forensic scientist is vital in investigating, and then illustrating, the results of his computerised analyses, his work would be severely hindered, if those responsible for maintaining the equipment failed to provide a satisfactory service. To this end, the Metropolitan Police, to give but one example, have established an entire department consisting of computer support staff to address the issues of purchasing, installation and administrative aspects of computer support.

1. Ibid. (1981 at p.26).

To summarise at this juncture, it is impossible to consider the diverse implications of technology without also taking into account, the involvement of man, the practicalities of task motivation, as well as the hierarchy of the environment under which fraud investigators operate. Galbraith. J.K.,¹ describes how these sub-divided tasks finally culminate in the finished product as a whole, due to the combined efforts of all involved along the line. The same argument could well be applied to the work of the fraud investigator, and the complex link of multi-disciplinary skills that range from the reprographer to the scientist, throughout the entire process of a complex investigation.

1. The New Industrial State, 2nd edn, Deutsch, 1972, pp. 12-13; Penguin edn, 1974, pp. 31-32.

1.3. THE TECHNOLOGY ENVIRONMENT OF FRAUD INVESTIGATORS.

Apart from the domestic technologies that a fraud investigator may encounter during his leisure pursuits, his working environment is now also awash with a catalogue of new devices. However, as noted by the Fraud Trials Committee, in their Report (ibid. 1986 at para. 2.8), despite the amalgamation of police forces in England and Wales in 1974, it is still the larger forces who are better equipped with expertise and experience. Although the senior management of policing have a general responsibility for all forms of police training, fraud policing and the skills needed for its effectiveness, appear to have no central pivot of coordination. In other areas of specialisation this is not the case, as for example with Regional Crime Squads, who have a National Coordinator to further its aims. Nevertheless, the Metropolitan and City Police Company Fraud Department operate an intelligence service¹ which is also available to provincial fraud squads seeking details of fraudsters and their modus operandi.

Due to the fact that the main workbase of a fraud investigator is his office environment, it follows that many of the modern systems used in offices in the world of commerce will also become available to fraud squads according to the level of their financial resources. In terms of routine information gathering about the world of finance from such traditional sources as libraries, this can be time-consuming and might involve delays that could put crucial decisions at risk. This may in turn affect the progress of important initiatives. In this sense, technology has in many respects come to the rescue.

1. As noted by the Fraud Trials Committee Report (ibid. 1986 at para. 2.8).

Gaukroger. J., (1988 at p.86) summarises the position by describing how 'on-line' database systems are of value in this area of research gathering. 'Gateway' facilities (ibid. p.86) also enable host organisations to provide a computer linking service to personnel working away from the office with portable computers, making it possible for officers to key-in to the fraud squad office computer, details of any information necessary to update the system.

As fraud investigation involves the preparation of precise case-reports for the information of the prosecuting authorities, the value of word-processors is also seen by the last commentator (ibid. p.xiii) as capable of enabling high quality text to be produced to a standard which is commensurate with the image of a well-administered, professional organisation.

Newcomers to the developing world of office technology may be educated about the likely benefits that are to be gained from new systems, based on the experience of organisations employing advanced office systems. One example of such an organisation is given by Gaukroger (ibid. p.xv) as the Department of Trade and Industry's Office Automation Pilot Project.

Developments in the field of communications allow electronic mail systems to provide the speedier and guaranteed delivery of documents against a background of uncertainties in the postal system, whilst centralised computer information provides easy accessibility to computerised management information, in addition to the other benefits.

The Fraud Trials Committee in their Report (ibid 1986a at p.231) note the manning levels of all the fraud squads in England and Wales. The highest recorded establishment of

manpower being that apportioned to the Metropolitan Police, which at the time their data was published stood at 147 personnel.¹ The lowest recorded level of only 2 fraud squad personnel was shared by Dyfed-Powys² and Surrey. Such a variation in manning levels nationally, will affect the technology and computer user requirements of these group sizes. Thus, the larger fraud squads will be attracted to the 'mainframe' systems which are in the larger corporate range of computers, or the 'minicomputers', which enable a limited number of users to process data simultaneously. Conversely, the smaller fraud squads will be drawn towards the less powerful, but more appropriately sized, microcomputers (or personal computers). The use of portable (or laptop) computers have potential benefits for fraud squads of whatever size, in terms of manpower.

The development of OCR (Optical Character Recognition) technology alleviates the duplication of effort that would otherwise be involved in converting previously typed documents (of the type prepared on a conventional typewriter), into another form of 'keying-in' system of the word-processor variety. An optical character recognition device attached to a word-processor can scan a page of typed work and input the characters directly onto the VDU. However, as noted by Gaukroger. J., (ibid. p.16) OCR has a low adoption rate at this time, due to the expense of this equipment, rate of error, and the limited ability of some systems to accept a wider range of font or typestyles.

-
1. It should be noted however that this figure has declined to 138 officers, due to other priorities in operational policing.
 2. Dyfed-Powys now lay claim to a slight increase in the establishment of their fraud squad.

Amongst the pot-pourri of modern office technologies available to the fraud investigator, should also be included CAD (Computer Aided Design), which although mainly used in industry to assist professionals in the creation and modification of technical designs of cars, aeroplanes and building plans, could also be used to assist in the case management of some of the more complex frauds. Its potential use as a medium for electronic charting and information flow systems is considerable.

Desktop publishing systems too, have benefits to offer the fraud investigator who seeks to perfect the quality of his case-file preparation. These devices enable the user to combine the tasks of inputting texts, pasting in diagrams and photographs at appropriate points, and final printing into a single process. However, as argued by Gaukroger (ibid. p.99) the cost of these systems currently places them beyond the financial reach of casual users. It is of interest to note, that the same commentator (ibid. p.99) predicts that the multi-functional capacity of desktop publishing systems are likely to become an integral function of a new generation of word-processing packages (particularly with the more widespread use of laser printers), to vary typestyles and sizes, and to incorporate external documents and diagrams into text, thus usurping some of the prime advantages of desktop publishing systems.

With the rising cost of staff salaries, the desirability of installing mechanical security systems in some of the larger fraud squad establishments, is self-evident. Data entry systems, operated by the insertion of PIN cards (Personal Identifier Number), will ensure that entry to buildings and/or parts of buildings, is restricted to those individuals whose access levels are appropriate.

Future product developments include integrated management workstations and will incorporate a selection of features, which Gaukroger (ibid. p.113) describes in detail, but the same commentator concludes on a rather gloomy note by inferring that such workstations will inevitably contribute to fraud squad managers becoming even more deskbound, if they are implemented.

In terms of more recent developments, however, results of a survey conducted by the author of this thesis, indicates that fraud squads are now increasing their use of facsimile devices to ensure a faster despatch/receipt rate of documentation and thereby assist in reducing the amount of time spent conducting investigations. Table 1 below, reveals the position that currently exists, in relation to fraud squads and the availability to them of facsimile equipment.

Table 1.

The availability of facsimile equipment to fraud squads.

	Number of fraud squads	in percentage terms.
Fraud squads having sole use of their own equipment.	7	20%
Those required to share equipment of others but but with easy access.	26	74.28%
Those with no easy access to facsimile equipment.	2	5.72%
Total.	35	

(based on data given by those who answered this question).

Few people reflect on the skills and artistic disciplines employed in the manufacture of the maps of the London Underground Rail network, and yet, a closer examination than that applied by the casual observer seeking his destination, will reveal its true artistry as a medium for communicating visual information of a public nature. Whether or not it is viewed in either the pocket-sized or wall mounted version, the data it contains relates to over 280 underground destinations, spanning a complex of 17 rail networks. In order to achieve that standard of presentation in public information, there are a number of rules relating to brevity and clarity, that must be taken into account.¹

As an organisation which is also required to communicate with the public, and sometimes by the medium of text, the police service has also become associated with legendary public notices. Crime prevention posters which warn that there is a thief about, are classical examples of this type. However, not all of the visual displays used by the police are prepared for the benefit of the general public, and even fewer of those that are produced for internal reasons are professionally manufactured. This is due not only to reasons of cost, but also arises from the need for expediency. As such, the police service has developed its own methods for producing cottage industry displays.

The police plan drawer was for many years the innovator of ad hoc visual displays, but in forces such as the Metropolitan Police, this function has been contracted out

1. See generally, Jaffe and Spierer, Misused Statistics (1987) for a good discussion on the guidelines relating to information presented in this way.

to the Ordnance Survey Office, as part of the force goal to increase the police presence in the community. Nevertheless, many of the traditional methods still exist. An example of this are the white melamine magnetic boards, which provide an immediate 'tell-at-a-glance' information guide, regarding the state of current action in major incidents of one form or another. There are many advantages associated with even these basics forms of information technology, including their ability to provide a focus for attention to centralised pieces of information that might otherwise require a search at fragmented points of reference ¹ such as files, indices, manuals containing police policy, and similar records.

Other non-technical forms of visual displays, are slot index systems, of the type which incorporate the insertion of 'T' cards for the purposes of estimating the availability of personnel, vehicles and other resources. There is still a place for even these crude methods of monitoring, particularly at a time when the resources being allocated to the investigation of fraud are in some instances declining.²

The more sophisticated forms of visual displays used in policing apposite to fraud investigation, include the use of technological briefing aids, of which pre-recorded video-taped films, are one example. Popularised by the Sir Kenneth Newman, former Commissioner of the Metropolitan Police to disseminate his force planning strategies, such a method would be entirely appropriate in cases of complex fraud enquiries, in helping to explain the intricacies of

-
1. See Ponsford. K., Visual Displays (1970), Report No. 17/70. An unpublished research monograph held at the Police Staff College library, at Bramshill.
 2. See for example, results of research at pp. 111-115 below.

a particular case, to personnel in need of familiarisation with the current status of an investigation.

Results from part of the survey carried out in respect of this thesis, reveal that the Ministry of Defence Police fraud squad now possess an electronic briefing board. This equipment enables the operator to choose from any one of the seven rotating screens that are available to him, via the medium of button manipulation. Once details of the briefing have been finalised, and perhaps even improved upon following discourse resulting from such briefing, miniaturised versions of the screened data may then be replicated through xerographic reproduction and handed to the participants, as a form of aide-memoire.

The use of laminated cue-cards containing step-by-step instructions of detailed procedures, is also proving beneficial to fraud investigators who are required to operate tape-recording devices during interviews with suspected perpetrators of fraud.

A miscellany of technology exists that could adapted for visual information displays, which might improve the quality of life and the flow of information to fraud squad personnel occupying several floors of accommodation, such as in the case of the Metropolitan fraud squad, based at Richbell Place, Holborn. The choice of equipment may range from the purely audio methods of the type used for transmitting remote public address messages (a form of modern day Tannoy system), to those which favour the visual mode, of which textlights and videotext provide but two examples.

Charting techniques occupy a position of considerable importance in the modern police approach to case management of serious fraud enquiries. Despite the note of

caution exercised by Appleby. R.C., (1972 at p.56) relative to the changing circumstances which quickly outdate the effect of charts, in addition to other shortfalls, there is now an upsurge in the use of ANACAPA charting facilities, due to a commitment by the Police Service towards increasing its professional analysis of information by visual methods.

As ascertained from course material relevant to the subject of ANACAPA techniques¹ this scheme, which was imported from America, is based on the analytical investigative methods used there in dealing with drugs trafficking, complex criminal activity and other forms of organised crime. The term ANACAPA is now synonymous with a variety of sophisticated charting techniques used by the Metropolitan and other police forces in England and Wales, following the purchase of the scheme's franchise from the American company of the same name.

Other concepts in crime analysis charting currently in use, are broadly similar in outline to the principles of ANACAPA. One example of this is VIA (Visual Investigative Analysis) charting, which Morris. J., (1983 at pp. 12-14) describes as having evolved out of a general need for more organisation in case analysis, and agency activity planning. However, both ANACAPA and VIA charting, are either wholly or in part, based on the principles of two earlier charting sciences.²

The first of these is described in the publication Crime Analysis Charting (ibid. Morris. J., 1983 at p. 14) as CPM (Critical Path Method), being used primarily for scheduling, planning and controlling projects with

1. Source, undated course literature, 1979.

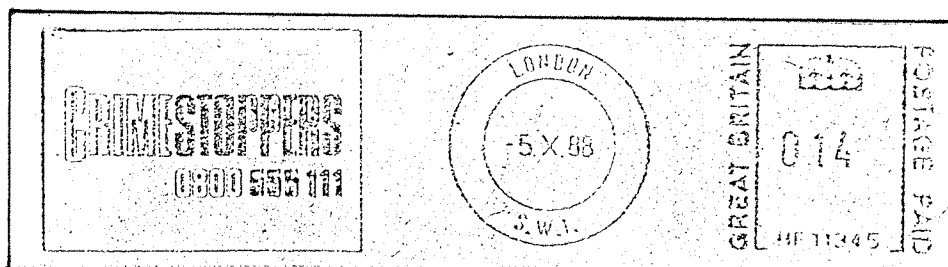
2. See also Levin. R.I., and Kirkpatrick. C.A., (1966).

deadlines to be faced in the construction of buildings and ships. By allowing its users to decide which path in a network was likely to take the most critical path. With the second concept, that of PERT (Program Evaluation and Review Technique), the principle behind this, as explained by Morris. J. (ibid. 1983 at p. 13) is to enable managers to monitor the progress of projects.

As a result of advice and other cooperation afforded by members of the Metropolitan and City Police Company Fraud Department to the Securities and Investments Board, it was possible to develop the concept of visual displays towards a fraud prevention campaign, by participating in the preparation of advice booklets¹ to small-time investors during the prelude to deregulation of investment business in the United Kingdom and the drafting of the Financial Services Act 1986. The warning slogan in the booklet foretold, that in the climate of 'Big-Bang', ill-chosen investments 'can damage your wealth'.

Other visual displays that may be considered in fraud prevention campaigns, are those derived from mail franking devices and which carry appropriate slogans, such as the one demonstrated in Fig. 1. below, for example.

Figure. 1.



1. See under Securities and Investments Board (1986).

1.5. TELECONFERENCING AND COMPUTER LINKS.

There are two matters that require consideration before embarking upon the subject of teleconferencing. The first is, that written forms of communication such as mail and facsimile equipment are ideal for sending information in one direction, but the originator must then wait for an indefinite period of time for a reply to any query that he might have raised. In terms of immediacy and particularly where expert advice is sought quickly, a two-way exchange of information is often essential. The second consideration is that traditionally, meetings involving senior police managers have always played an important part in determining policy, in a spontaneous and informal atmosphere. However, as noted by Gaukroger. J., (1988 at p. 100) such meetings may not always be necessary, nor in the light of modern technology, convenient. The reasons for this may be due to the amount of travelling that is sometimes involved in order to attend these meetings, coupled with the expense involved in obtaining overnight accommodation in certain cases. There is also the question of time lost elsewhere within the organisation when meetings are being routinely attended, rather than for reasons of necessity.

To obviate the need to be physically present at a meeting, there are two concepts that will enable groups of people situated at different locations to become linked by means of telecommunications, which are known as teleconferencing. Sometimes also referred to as 'electronic meetings', Gaukroger (ibid p. 101) describes how this method of communication attracts arguments which go both in favour as well as against the concept. In arguing a case for the advantages offered by the improved productivity in executive manpower as a result of less time being spent away from the workplace, Gaukroger (ibid

p. 102) also notes the neutralising effects that these electronic meetings have on social conviviality, due to the remoteness of participants. The same commentator (ibid. p. 100) also draws attention to reductions in job-satisfaction levels that are sometimes caused by electronic meetings, due to lost opportunities for travel, for example.

Teleconferencing may be conducted by the mainly audio mode of meeting known as 'audioconferencing', or conversely, another branch of teleconferencing which favours the visual approach that is called 'videoconferencing'. With audioconferencing, two or more people may be linked to the same voiced telephone conversation, and when two groups of people are involved, loudspeakers and microphone systems may be introduced. Audiographics may be added to some of the newer systems. Audiographics are capable of producing graphical information in addition to the voice communication facility by means of an electronic blackboard or telewriter tablet.

Although audioconferencing is a relatively cheap form of teleconferencing which can be installed fairly easily, Gaukroger (ibid. p. 102) argues that variations may sometimes occur in the quality of sound and that the difficulties in identifying the voices of the relevant speakers add to other disadvantages of this method of communication. However, purpose-built audioconferencing systems of the type Conference 2000 and Confertel, which are used by British Telecom, include control buttons to allow interception of speakers by a nominated chairman, enabling the meetings to be conducted in a more structured fashion, whereby impromptu interruptions by dominant speakers may be controlled.

Videoconferencing enables electronic meetings to be conducted via the medium of linked television screens and sound facilities. In organisations which are prosperous enough to own equipment of this type, their executives have merely to enter the company's videoconferencing room in order to engage in the businesses of meetings which involve other participants who could be situated long distances away. This type of equipment is also available at a number of centres which are operated by British Telecom's Confravision service.

Despite the fact that videoconferencing widens the scope of meetings that can be undertaken by comparison with audioconferencing methods, Gaukroger (*ibid.* p. 103) draws attention to the high cost of these systems, the fact that they are currently restricted for use between two locations only and the inconvenience that some users may experience in having to travel to public videoconferencing centres, such as those operated by British Telecom.

The British Telecom Confravision system provides a videoconferencing service to the public, from London and other major UK cities. It also provides worldwide links to designated countries. Costs, which are charged at hourly or part hourly rates between UK centres, vary from between £190 and £290 per hour. The user of an hour's Confravision time between London and New York, however, could expect to pay £1400 to £1500. Private systems are also available, although system costs currently inhibit their wider use.

In the context of fraud policing, investigators could become involved in teleconferencing, if called upon to investigate the activities of personnel employed by organisations which operate these systems. An example of such an instance, would be where allegations are received from British Telecom involving widespread and organised

fraud perpetrated to their detriment, in a number of major cities where their Confravision service is in operation, and in the interests of expediency, it becomes necessary to discuss tactics with representatives from each of the given areas.

Although the costs of teleconferencing currently inhibits its routine and short-term use by fraud investigators, Gaukroger (ibid. p. 103) predicts that this problem will be reduced when the full development of ISDN (Integrated Services Digital Network) is achieved in the 1990s, to allow for the transmission of video. When they eventually become financially viable propositions, teleconferencing systems have much potential as an investigative tool, in dealing with international fraudsters or as an alternative method of communicating on a face-to-face basis, with foreign law enforcement agencies regarding fraud trends.

But before UK fraud squads should even begin to consider the practical advantages of technology with overseas agencies, there is still much left to be achieved in terms of computer systems and the implications of their national compatibility. Computers are now an essential part of the equipment of modern fraud squads, and investigators increasingly require access to a variety of different systems to enable them to perform their duties efficiently. Lessons that were learned from the case of R. v. Sutcliffe,¹ revealed the practical necessity for individual forces to pool information during times of serious (and series) crimes, and by the provision of these cross-border links it was possible to ensure that a wider interpretation of the evidence could be achieved.

1. [1981], i.e. The Yorkshire Ripper enquiry.

The requirement to link machines together is not unique to the police service, as there are worldwide moves towards the standardisation of such devices, which as noted by the Police Requirements Support Unit,¹ is the Seven Layer Model, known as OSI (Open Systems Interconnection). In terms of computer systems which are used as aids during the investigation of crime, the police service response to the Sutcliffe incident, has led to the implementation of HOLMES² (Home Office Large Major Enquiry System).

-
1. Ibid. Open Systems Interconnection - An Overview. Information Desk Bulletin No. 26, June 1987 at para. 3.
 2. The Police Requirements Support Unit (ibid. Bulletin No. 29 at p.33), reported in March 1988, that due to the fact that operators representing the vast majority of forces are now trained in the use of HOLMES, it has no longer become necessary to provide training on a nationwide basis. If this example were to be mirrored in terms of fraud policing needs, a giant step forward will have been achieved.

1.6.

EXPERT SYSTEMS.

Expert systems in the context of fraud policing, are particularly relevant at this time. As noted by the Home Office sponsored Police Requirements Support Unit Bulletin, two of the successful applicants for a monetary award were officers from the Metropolitan fraud squad for their development of the project SAFES (Self-Analysing Fraud Expert System).¹

The police service however, were not the first body to suggest the use of an expert system in terms of fraud case information. The Fraud Trials Committee in their accompanying Report which deals with four research studies undertaken into the presentation of information,² also took note of the potential use of microcomputers, which when fitted with suitable word-processing software packages, could conceivably be used to prepare a glossary of the technical, legal and financial terms that a jury might encounter during trial proceedings (ibid. p.7). The intention being, that once a comprehensive glossary had been prepared and stored on disk, those with particular relevance to certain trials could be extracted by means of the computer's electronic searching facilities.

Despite Gaukroger's oversimplified definition of an expert system (ibid. p.93), she nevertheless perceives the fundamental basis of this technological phenomenon, as systems which are concerned with capturing the knowledge held by experts into a computerised system, which can be interrogated by the non-expert. The aim being to produce as good a decision, or an even better one, than is given by the expert in person.

1. Ibid. Bulletin No. 29 at p.4.

2. Ibid. 1986b.

The same author (ibid. p.93) gives examples of experts as being people who are consultants, barristers and solicitors, as well as accountants and other professionals. Based on this commentator's philosophy, the definition of an expert could be extended to include those who have acquired expertise in the investigation of fraud.

As noted above,¹ expert systems include derivatives of Feigenbaum's DENDRAL project and also encompass other forms of AI (Artificial Intelligence), such as the techniques used in CAI (Computer Aided Instruction) by many police training establishments and other educational centres. This type of training is also used by the American judicial system to enable judges to become familiar with jurisprudential techniques, as further discussed below.² An explanation of the wider use of expert systems in Britain has been sponsored by the Department of Trade and Industry.³

Susskind (1987) discusses the various types of expert systems that are currently being developed in the United Kingdom, with particular emphasis on those which have application to the law, including database systems of the Lexis type (ibid. p.4) which may be interrogated by users when seeking case-law and others forms of information. The Lexis handbook (1981 pp. 24 and 12) provides further details of its capabilities. Susskind (ibid. p. 12) also defines the meaning of a shell or skeletal system, which based on the work undertaken by those involved in the Oxford Project prototype relating to the divorce law productions in Scotland, would provide the basis for a

1. At page 4.

2. At page 97.

3. Expert Systems in Britain, by Ovum Ltd. Which is obtainable upon request from the Department of Trade and Industry.

shell for expert systems in law, in other legal domains. In drawing attention to the contention that is attributed by such information theorists as Dretske, Mehl and Niblett, regarding their interpretations of information and meaning, Susskind (ibid. p.13), concludes that few, if any, of the expert systems that currently purport to be so, fall within the proper definition of expert systems in the truly purist sense. However, Niblett¹ argues that Susskind gives the role of jurisprudence in the design of legal expert systems, a greater significance than it deserves.

B. Conclusions.

This part of the research indicates that modern technology, in the context of fraud policing, is often being developed by individual fraud squads in isolation of others.² There is, however, a considerable increase in the reported use of computer systems, which supports the theory that fraud investigators are now making a conscious effort to understand and to use methods that not only serve to reduce human effort, but which also produce high quality case-work documentation and other forms of printed text. These higher standards of presentation, are synonymous with the professional image that courts have always expected from fraud investigators, and since it is the courts who are to determine the admissibility or otherwise of such evidence, it can be argued with much justification, that whilst the present rate of progress is encouraging, these new aids to fraud policing, should be developed centrally, and with the priority consideration of senior police managers.

1. See under book review of Expert Systems in Law. 56 Computers and Law. June 1988 at pp. 32-33.
2. As noted at p. 3, above.

CHAPTER TWO.

ADMISSIBILITY OF COMPUTER RECORDS.

A. Introduction.

Although constituting a mere branch of the technology tree, computers emerge as the prima donnas of police information management systems. However, the laws of evidence, which govern the admissibility of evidence emanating from these devices, owe their origins to legal decisions which can be traced back into the last century.¹ This chapter considers the implications arising from the use of 'techno-evidence', and its development through the passage of time. The methodology used to assess this progress, has been to review the extensive research of Tapper. C., whose specialised knowledge in this field, has proved invaluable during the preparation of this thesis.

Tapper,² notes that documents have now acquired an enhanced status, in being allowed to 'speak for themselves', as opposed to the traditional reliance that was placed on the human witness. However, where documents are derived from computerised devices, it is essential that proponents and opponents are able to establish that such systems were operating properly at the time that the relevant documents were produced. Where the police and other parties fall short in meeting the standards that have been set for authenticating this type of evidence, valuable material may be rendered inadmissible by the courts, and juries will in turn be deprived of pertinent issues upon which a proper verdict depends.

1. See footnote 1, on page 29 for example.

2. Ibid. (1988). Computer Evidence. at p. 4.

2.1.

AUTHENTICATION OF EVIDENCE.

Proving facts during the process of a trial, is regulated by the laws of evidence which are administered by the judiciary in the Higher courts. Throughout time, judges have tended to be palliative towards change, which is exemplified in the dictum expressed by Lord Campbell C.J., in contemplating the case of Humphrey v. Dale,¹ thus;

'It is the business of the courts reasonably so to shape their rules of evidence as to make them suitable to the habits of mankind.'

One fundamental principle of the common law, is that rule which applies itself to the exclusion of hearsay evidence. The definition of hearsay as suggested by Tapper. C., (1988 at p.9) may be summarised as 'an assertion other than one made by a person whilst giving oral evidence in the proceedings, when tendered as evidence of any fact so asserted'.

Tapper (ibid p.9) notes that when evidence has been derived from a computer, it is necessary to ensure that it is authenticated so that it may qualify either as 'direct' or 'circumstantial' evidence, but adds, that in terms of 'real' evidence, separate considerations must apply to evidence which is derived in this way.² The principle of authentication as legally interpreted, relates to the concept that, since a document is incapable of self-

1. Ibid. (1857) 7 E & B 266 at 277, 8.

2. Tapper (ibid. p.14), explains that; 'evidence which is derived from a computer, constitutes real evidence when it is used circumstantially rather than testimonially, that is to say that the fact that it takes one form rather than another is what makes it relevant, rather than the truth of some assertion which it contains.'

testimony, a person must satisfy the court as to its identity and relevance.

The law treats evidence of this nature with a jaundiced eye, when it is produced from the custody of someone who is actually a party to the proceedings. Particularly if there has been an opportunity to tamper with the text or any other data, upon which documents such as print-outs are based. In such circumstances it will be the validity of the print-out itself that is in issue, and any doubt will relate to tracing the point at which any likely alteration has occurred within the mechanism of the computer, due to the flexibility of these devices and the ease with which they can be manipulated.

There appears to be an absence of English test cases dealing with the problems of authentication of evidence which has been derived from computers. There are, however, other cases that have been tested regarding technological devices. The use of tape-recordings in proceedings provides a rich source of analogous material upon which comparisons can be made. One case in point is R. v. Maqsd Ali,¹ although, in this extreme example there were further complications because the language used in the taped-conversations was of an obscure Punjabi dialect.

In considering everyday tape-recordings of conversations, which have been conducted in the English language and which are then transcribed into a written form, it could be argued that the transcription acquires a status which is similar to that of a computer print-out. The reasoning for this is due to the fact that in both the computer print-out example and the transcription of the tape-recording, the compilers are both relying on their own

1. (1966) Q.B. 688, C.C.A.

interpretation of the information which is available to them. In the computer example, the information is in text and other forms of data, whilst in the case of tape-recordings, the information is conveyed by the medium of speech. To argue that both the print-out and the transcription are reduced to secondary forms of evidence, is to over-simplify the position. Whilst the claim might be true in both examples, in the case of computers it is somewhat different, as the form in which its text and other information appears on the screen of the VDU as human-readable material is based upon the machine's interpretation of the magnetic codings on the disks which specify spacing, lineation, pagination, etc. This means that text in its human-readable appearance, represents an even earlier form of secondary evidence, than the print-out.

Thus, judging from the case of R. v. Maqsud, it is evident that the Court of Appeal is generally supportive to evidence which is derived from modern forms of technology and there is no reason to suppose that evidence which is derived from computers would be less favourably treated. Despite the fact that the case in question dealt with the broader issues of voice identification, the outcome of the case nevertheless gives an indication of the willingness on the part of the courts not to deny to the law of evidence those advantages that are to be gained by the use of new devices and techniques.

Although the last case to be discussed was not concerned with that aspect of integrity vis-a-vis the risks arising from tampering with the original tape-recordings, when possession changes hands, this was certainly the position in R. v. Stevenson¹ where such evidence was disallowed.

1. (1971) 1 All ER 678, Ass.

This decision was taken partly as a warning that, in future cases, sufficient care must be taken by those obtaining the original evidence in the first instance. This aspect affecting the authentication of evidence would have close relevance to records held on a computer.

Similar issues arose in the case of R. v. Robson and R.v. Harris¹ after expert evidence had been introduced to discredit the authenticity of tape-recordings, and also in rebuttal to support their credibility, but which evidence was nevertheless admitted on the balance of probabilities, that the defence claim was inappropriate. In this case, Shaw. J., took the view that the proper course was for the trial judge, to determine whether a prima facie case had been established in favour of such authenticity, and in terms of the continuity of the evidence from the time of their recording and production at court. Once satisfied on the grounds of authenticity, the trial judge may then consider that the issues are capable of being aired before the jury, as in all other cases of fact.

A similar test may be expected regarding evidence derived from computers, particularly with regard to the integrity of the procedures used for collecting the data, input into the computer, manipulation, checking and storing until presentation of such evidence at court. Tapper (ibid. p.14) summarises the position in relation to documents produced by computers which are to be proved by use of a microfilmed copy. In such circumstances, the court is given unrestricted discretion to approve any method of authentication.²

1. (1972) 2 All ER 699, CCC.

2. Police and Criminal Evidence Act 1984, section 71.

2.2.

REAL EVIDENCE.

As noted above,¹ evidence which is derived from a computer constitutes real evidence when it is used circumstantially rather than testimonially. Tapper (1988 at p.14) comments on the interaction of this rule with the hearsay rule, which he observes not only bars the testimonial use of an assertion, but also its circumstantial use. The reason for this safeguard is to preserve the rule from becoming too readily undermined.

Adopting Tapper's line of reasoning for this view (ibid. p.14) it is argued that in the same way an employer's statement would be inadmissible against an employee whom he had initially accused of theft but had then subsequently refused to testify against, any other assertion relating to the same accusation would become equally inadmissible. As for example, under circumstances whereby that assertion had been entered into a computerised database which had been regularly checked for the accuracy of the statements contained in it by efficient and impartial third parties. Thus, a printout from such a device containing the statement that a particular employee is a thief, is not even circumstantial evidence of that fact.

Where assertive statements originate from the functions of a machine, further complications arise. An example of this was experienced in The Statue of Liberty² where a collision involving two vessels in the Thames estuary had occurred, at a time when the estuary was being continuously monitored by radar and the radar traces had been automatically recorded by means of a cinematograph device. Had the incident been witnessed by humans who

1. At p. 29.

2. (1968) 2 All ER 195, PDA.

dictated their observations into a tape-recorder, the recording would amount to hearsay and would be rendered inadmissible, in the event that no exception to the hearsay rule could be invoked.

Simon. P., wisely rejected the contention that the film was susceptible to a similar objection on the basis that it constituted real evidence, and not hearsay, thus placing the quality of this form of evidence on a par with direct oral testimony. The courts therefore support the view, that where machines have replaced human beings it makes no sense to insist upon rules devised to cater for human beings, but rather as Simon. P. said (supra footnote 2, above, *ibid.* p. 196), 'The law is bound these days to take cognisance of the fact that mechanical means replace human effort'.

This useful distinction appears to have been overlooked in the case of R. v. Pettigrew¹ where the prosecution sought to introduce evidence relating to the numerical sequence of stolen banknotes. The system of numbering these banknotes was a hybrid one, which partly involved human effort at various stages of the manufacturing process, as well as the automatic operation of the machinery. Counsel for the prosecution unwisely argued on the basis that the printout on which his case relied was a business record under the terms of section 1 (1) (a) of the Criminal Evidence Act 1965, but the Court of Appeal ruled against this submission on the basis that the operator had no personal knowledge of banknotes that had been rejected during the manufacturing process, due to their automatic compilation by a computer.

1. (1980) 71 Cr App R. 39, CA. See also R. v. Wiles [1982], Crim LR 669, Kingston Cr Ct, where Pettigrew was applied to the reading calculated automatically by the meter on a petrol pump.

Although the court's conclusion had mirrored the correct interpretation of the hearsay rule as it applied to the discussion, the print-out's value as real evidence, had been ignored. If the entire manufacturing process of the banknotes had been compiled automatically by the computer, the analysis relating to the cinematograph film in The Statute of Liberty would have taken effect, as seems now to have been accepted as a matter of common law.¹

In the case of R. v. Wood² the chemical composition of metal ingots was analysed respectively by an x-ray spectrometer and a neutron transmission monitor as an alternative to the extensive and laborious human effort of mathematical calculation that would otherwise have been involved. The prosecution successfully countered the defence contention that the results amounted to hearsay evidence, and were supported by the court which found that the computer was being used merely as a calculator, and did not support any human assertion which had been entered into it. As such, this evidence was just as admissible, and with as little reference to the hearsay rule, as any calculation performed by a witness for the purposes of giving evidence, as for example using a slide-rule or weighing machine. So far as the output of a computer when tendered as real evidence, the court indicated that it was immaterial that more than one person might have been involved in setting up the system within which it was used.³

The court recognised that the dividing line between admissibility as real evidence at common law, and inadmissibility as hearsay would not always be so easy to draw,⁴ adding that no two cases are the same.

1. As also argued by Tapper (ibid. p.58).

2. (1982) 76 Cr App Rep 23, CA.

3. At p.27.

4. At p.28.

Similar conclusions were also reached in Castle v. Cross,¹ where the document in question was the printout of a breath machine.

In terms of best evidence, the relevant rule has its origins in the eighteenth century in requiring that a party should adduce the best evidence that the nature of the case allowed. The effect of its subsequent interpretation is echoed by Tapper (*ibid.* p.22) as amounting to a requirement that no evidence, which on its face indicated the existence of better evidence should be admitted, at least until a satisfactory explanation of that better evidence had been given. As further observed by the same commentator (*ibid.* p.22) this rule has sometimes been used to question the admissibility of evidence that has been derived from computers, although these contentions have occurred more often in other jurisdictions than in England.

Courts are now tending to regard this rule as obsolete, as was the case in Kajala v. Noble² which impinged upon the prosecution's reliance of a video-film produced by the BBC. The producers were unwilling to release the original film and therefore only a copy of it was available when the case was presented. There was also an added complication in that the cameramen who had made the recording were abroad, and not available to give evidence in support of the copy. In deciding on all the issues of the appeal, the Divisional Court rejected the somewhat tenuous grounds put forward by the defence. It should also be noted that no challenge had been made at the time of the original hearing at Southall Magistrates' Court, nor did the defendant give any evidence on his own behalf.

-
1. (1985) 1 All ER 87 QBD.
 2. (1982) 75 Cr App Rep 149.

The findings of Tapper (ibid. pp. 223-228) in relation to evidence which is derived from computers, may be summarised in this way. The most common objection to the admissibility of evidence which is derived from these devices, is that which amounts to hearsay. The rule which as noted above (at p. 33) operates to exclude assertions made by persons other than the witness who is testifying as evidence of the truth of that which is asserted. Thus, if a system for recording the numbers of various components of a motor car is maintained on a computer, the print-out will amount to hearsay if it is produced to prove that combination of numbered parts in a given car.¹

In comparing the examples of Myers, (supra footnote 1, below), R. v. Patel² and R. v. Shone,³ Tapper (ibid. pp. 24-25) concludes that the restrictive effect of the common law necessitated the development of a number of exceptions to the hearsay rule. Some of these changes have affected the admissibility status of evidence derived from computers. In terms of of civil cases, the common law aspects have been supplanted by the statutory regime. In criminal cases however, the common law exceptions may still apply in addition to the new exceptions that are contained under the Police and Criminal Evidence Act 1984. Tapper (ibid. pp. 27-28) who also discusses those common law provisions which generally relate to admissions binding a party to proceedings, and the computerisation of Society record books, also observes (ibid. p.27) that no new common law exceptions can now be created, following the House of Lords ruling in the Myers case.

-
1. Cp. Myers v. D.P.P [1965] AC 1001, HL where in fact the records were held on microfilm, but as noted by Tapper (ibid. p. 176) it would have made no difference had they been held in a computer.
 2. (1981) 73 Cr App R 117, CA.
 3. (1982) 76 Cr App R 72, CA.

2.3. JUDICIAL NOTICE AND PRESUMPTIONS.

As noted by Mitchell., ed. (1982 at pp. 336-337) judicial notice is where a court finds that a fact exists (or directs the jury to find that a fact exists), although its existence has not been established by evidence. However, in relation to modern technology, Tapper (1988 at p.28) notes that most forms of new technology are too recent and indeed too sophisticated to qualify for exclusion under this doctrine. One area which has been tested, however, involves the record which forms the output of breath-testing devices, because of frequent challenges surrounding their operation. Another area is in relation to the social practice of using computers for record-keeping purposes, as in the business world, when such issues are challenged in evidence.

The presumption that machines are deemed to be operating in working order, unless proved to the contrary, is enshrined in the doctrine 'omnia praesumentur rite esse acta'. Despite the complexities of technology and the problems that are sometimes associated with the operation of computers, the courts tend to support this presumption with some conviction.¹ One of the methods used to apply this test is that the machine should be one of a kind, of which it is common knowledge, is more often than not in working order.

Despite the findings in Castle v. Cross, however, general evidence relating to a computerised system of record-keeping was not accepted by the Divisional Court in the case of R v. Hall,² regarding the despatch of girocheques from the Department of Health and Social Security, when it

1. E.g. see Castle v. Cross: (1985) 1 All ER 87 QBD.

2. As reported in The Times, January 8th 1987, QBD, and which case Tapper (*ibid.* p. 29) discusses fully.

was alleged during the evidence of the prosecution that the accused had received the cheques. As argued by Tapper (ibid p.30), the need to show that regular checks were made on the current operation of the computer should be sufficient in order to establish this presumption and thereby transfer the onus during rebuttal; to the side raising the issue of challenge.

The peculiar method of processing information through computers, signifies the lateral approach that must be applied in understanding the admissibility of documents derived in this way. If a document derived from a computer were produced in its original form, it would consist of computer coded data and would therefore be entirely unintelligible to juries. The courts allow for the admission of secondary evidence, which precedes the print-out phase. The admission of the print-out under such circumstances is explained by the law not distinguishing between degrees of secondary evidence,¹ despite the suspicion that is traditionally shown by the courts, regarding documents other than those that are in their original form.

The changing attitude towards the use of secondary evidence is further demonstrated by the introduction of explicit statutory provision for the admissibility in criminal proceedings of a microfilmed copy.² Specific amendment has been necessary to statutory provisions to facilitate the use of computer-based systems and these include a number of exceptions to the rule that original documents should normally be produced. Privilege, which is one such exception, is considered next.

-
1. As for example in the case of R. v. Wayte (1982) 76 Cr App R 110, 116, CA.
 2. Police and Criminal Evidence Act 1984 section 71.

Privilege not to disclose evidence may be conferred where the adducer might otherwise be incriminated, i.e. as in the case of a police informant, or under circumstances amounting to legal professional privilege or in disputes to settle a claim where such evidence is deemed to be 'without prejudice' in the course of negotiations to settle a dispute. As noted by Tapper (ibid. p.31) the fact that documents may have been produced by a computer will not affect their status of privilege, unless specifically stated under statutory provision.

Many sensitive government records are now held on computers and where their admissibility would be against the efficient and secure business of government and/or the public interest, these are excluded on the basis of these overriding exclusionary rules, in the same way that records held in any other form would also be.

2.4. ADMISSIBILITY OF COMPUTER RECORDS BY STATUTE.

The admissibility of computer records encompasses an area of law which has been affected by considerable statutory regulation: of which the most significant statutes determine, (a) the criteria for the admissibility of computer generated evidence, and (b) those which seek to bypass the hearsay rule of evidence at common law. There are some statutes which stretch provision for documentary records to systems which are based upon the use of computers, whilst others regulate the weight to be attached to records which are produced by means of such advances in technology. The piecemeal statutory reform of the hearsay rule has created a highly undesirable situation, which Tapper (1988 at pp.33-34) expands upon.

The first statute to essay a general exception to the hearsay rule to allow for the admission of documentary records, was the Evidence Act 1938. This Act admitted documents only under rather strict conditions, the effect of which was to limit its usefulness.¹ Although its main provisions were replaced by the Civil Evidence Act 1968, the 1938 Act continues to apply to civil proceedings in Magistrates' Courts² by virtue of the recommendations which were made by the Law Reform Committee. Tapper (ibid. p.35) who exemplifies the restrictive nature of the 1938 Act with relevance to the admissibility of statements in documents, notes the principle obstacles to the application of this legislation in the computer context, where under section 6 (1), the definition of a document includes, 'books, maps, plans, drawings and photographs'. Tapper concludes his assessment on the Civil Evidence Act

-
1. See Law Reform Committee 13th Report Hearsay Evidence in Civil Proceedings, Cmnd. 2964 (1966) para 11.
 2. R. v. Wood Green Crown Court ex parte P. (1982), 4 FLR 206, Fam D.

1938, by observing that the Act can only be applied to evidence derived from computers with the greatest difficulty, since its terminology was phrased at a time which predates the use of computers and, as such, was not designed to cater for this type of device. It appears fortunate that in the restricted range of proceedings to which the Act still applies, they are those in which such evidence is least likely to be required.¹

Due mainly to the defectiveness of the law of evidence in its application to modern business records, the Law Reform Committee met to consider the provisions that should be made in modifying the evidentiary rules. Hearsay evidence within the field of evidence, was its topic. Although this Committee explicitly extended its recommendations to include mechanically recorded statements, providing there was a duty to record them,² it did not deal separately with evidence derived from computers. Instead, it intended its general proposals to cater for such evidence. This activity culminated in the enactment of the Civil Evidence Act 1968, the intricacies of this legislation in relation to evidence derived from computers produced in civil proceedings, is particularised by Tapper (ibid. pp.38-47), who also deals briefly with the anomalous effect on expert opinion when attempts were later made to improve the law of evidence with regard to hearsay, in the Civil Evidence Act 1972.

The Criminal Evidence Act 1965, was the prompt legislative response from the House of Lords in Myers v. D.P.P.,³ to reform the law of hearsay in its application to modern business records. Tapper (ibid. p.48) notes that this was the first general statutory reform of the hearsay rule to

1. See Law Reform Committee 13th report, para. 51.

2. Para. 19.

3. [1965] AC 1001, HL.

be essayed in England in the computer age. However, this legislation has since been repealed by the Police and Criminal Evidence Act 1984, but it has been influential in the development of some of the basic concepts that have been introduced into succeeding legislation.

2.5. POLICE AND CRIMINAL EVIDENCE ACT 1984.

Further reform to the law of evidence in relation to the hearsay rule saw not only changes that arose from the draft provisions proposed by the Criminal Law Revision Committee in 1973,¹ but also those which had been contained in the government bill which lapsed when Parliament was prematurely dissolved for the purposes of a general election in 1983. The scheme of this Act differs from that of the Criminal Evidence Act 1968, or that proposed by the Criminal Law Revision Committee. The broad terms of Part VII of the Police and Criminal Evidence Act 1984, are, that it admits documentary records which have been made in furtherance of a duty if the maker is either unavailable or not worth calling, and in the case of computer records subject to proof of the proper operation of the computer.

One important difference between the 1984 Act and the Criminal Evidence Act 1965, is that there is no limitation with regard to business records in the latest legislation. The Act applies to all statements in documents compiled by a person acting under a duty from information supplied by someone who had, or could reasonably be supposed to have had, personal knowledge of the matters dealt with in it. Tapper (1988 at p.51) notes that the most important difference is the special requirements for computer records which are superimposed upon the general provision. This means that in the case of a document derived from a computer it will be admissible only if it satisfies the requirements of both section 68 and section 69 of the Act.

In comparing the provisions of both the Civil Evidence Act 1968 and the Criminal Evidence Act 1965, Tapper (ibid.

1. See Part II of the draft bill, clauses 30-41.

1988 p.52) observes that section 68 of the Police and Criminal Evidence Act 1984 replaces the relevant provisions of the 1965 Act, appropriate to documents derived from computers. In commenting on the anomalies that apply to evidence which is derived from computers generally, the same commentator (ibid. p.53) is of the opinion that such anomalies are more unfortunate in the criminal law rather than the civil law. He supports this theory on the basis, that incidents have occurred when even purely technical points have been allowed in the interests of the defence of a person accused of crime, but Tapper nevertheless concedes that this approach is the better one and, that under such circumstances, amounts to the more generous view.

The scheme of the Police and Criminal Evidence Act 1984, is that it preserves the effect of the Criminal Evidence Act 1965 in applying the restricted concept to statements in documents, derived from computers. It also provides a minor improvement in the conditions for dispensing with the attendance of the supplier of information with the substitution of the more justifiable phrase 'outside the United Kingdom' for 'beyond the seas' which occurs in the Criminal Evidence Act 1965, the Civil Evidence Act 1968, and the rules made under the latter.¹

However, Tapper (ibid. p.54) draws attention to the restrictive nature of the phraseology of sub-section 69 (2) (a) (iii) of the Police and Criminal Evidence Act 1984, relative to one who 'cannot reasonably be expected (having regard to the time which has elapsed since he supplied or acquired the information and to all the circumstances) to have any recollection of the matters dealt with in that information', which owes its origin to

1. Order 38 rule 25.

the wording in the 1965 Act. The same commentator (ibid p.55) suggests that the preferred option would have been to adopt the phraseology of sub-section 8 (2) (b) of the Civil Evidence Act 1968 which specifies the subject of rules to be made under the legislation by referring to one who 'cannot reasonably be expected (having regard to the time which has elapsed since he supplied or acquired the information and to all the circumstances) to have recollection of matters relevant to the accuracy or otherwise of the statement'.

Section 69 of the Police and Criminal Evidence Act 1984 has the effect of adding further conditions to the admissibility of records which are derived from computers, and whilst its provisions do not conform to the original plan of the Law Reform Committee to treat all documents alike, whatever their provenance, this part of the Act is a vast improvement upon the intricate wording of section 5 of the Civil Evidence Act 1968. Section 69 of the 1984 Act applies to any statement contained in a document produced by computers and specifies three requirements, namely;

- '(a) that there are no reasonable grounds for believing that the statement is inaccurate because of the improper use of the computer;
- (b) that at all the material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and
- (c) that any relevant conditions specified in rules of court under sub-section (2) below are satisfied'

One recent and important finding apposite to the use of a computer which has been used to facilitate analysis, is

that of Sophocleus v. Ringer,¹ which alludes to the decision reached by the Divisional Court that the conditions imposed by section 69 do not apply. Tapper (ibid. p.57) who bases his opinion on the vestigially reported newspaper report (supra footnote 1, below) concludes that this interpretation 'appears to fly in the face' of the wording of section 69, which purports to apply to a 'statement contained in a document produced by a computer', as well as the interpretation that is also suggested by Schedule 3 Part II of the Police and Criminal Evidence Act 1984, itself. The same commentator nevertheless concedes (ibid p.58) that it is possible to take a fairly relaxed view of this question since the conditions which would be required to be satisfied at common law for the output of a scientific device² are not very different from those imposed by section 69.

1. Times Newspaper 10 February 1987.

2. As in the case of The Statue of Liberty, discussed at p. 33, above.

2.6.

CRIMINAL JUSTICE ACT 1988.

Prior to the enactment of the Police and Criminal Evidence Act 1984, the government had referred the whole question of criminal proceedings in cases of fraud to an independent committee which had as its chairman, Lord Roskill. This committee found that in terms of the adequacy of criminal procedure there was widespread concern, with particular emphasis on the law of evidence regarding the successful prosecution of fraud. The Committee, devoted an entire chapter of its report to suggestions for the reform of the law of evidence, and concluded that the acceptance of its proposals were necessary if the reform was to be carried out effectively. Adding, that some of its proposals might be advantageous to reforms in other areas of criminal proceedings, and should not therefore, be strictly limited to cases of serious fraud.

The government concurred with the findings that fraud ought not to be isolated from the rest of the criminal law, and thus was set in train, a further radical change in the admissibility of evidence derived from computers in criminal proceedings. The broad aims of this Act being to expand the exclusionary rules relative to the admissibility of hearsay evidence which appear in Part II of the Criminal Justice Act 1988.

Tapper (1988. p.60) in considering the uncertainties created by some of the phraseology in the Act, comments on the status of sections 68 and 69 of the Police and Criminal Evidence Act 1984, as to what extent they remain effective in the light of the new legislation, since they do not appear to have been repealed. His discussion does

1. Fraud Trials Committee Report, para. 5.32.

however, conclude on the optimistic note that any anomaly that the new legislation may have created is slight, and that treating the conditions imposed by Part II of the 1988 Act serves as sufficient guarantee for ensuring the admissibility of documents falling within its provisions.

The effect of Part II of the Criminal Justice Act 1988, is that it now provides for the general admissibility of all first hand documentary hearsay:¹ of more remote documentary hearsay if contained in a business record:² but subject to general exclusionary discretion if its admission is considered inimical to the interests of justice:³ and to a more specific exclusionary rule if prepared for the purposes of the proceedings in which it is tendered, although this in turn is affected by an inclusionary discretion for any such statements when admission is considered to promote the interests of justice.⁴ There is also specific provision for the admissibility of hearsay expert reports,⁵ and for a number of minor improvements in the form in which documentary evidence may be presented to the court.

Tapper (ibid. p.62) who compares the relationship of the 1988 Act with various aspects of the Criminal Evidence Act 1965, the Civil Evidence Act 1968, and the Police and Criminal Evidence Act 1984, comments on how the effect of the earlier legislation has helped to mould the development of the new Act with regard to the improvements to the admissibility of business records.

In considering other aspects of the Act, there is an attempt to reduce the risks from the fabrication of false documents, since section 26 specifically excludes those

1. Section 23.
2. Section 24.
3. Section 25 (1).

4. Section 26.
5. Section 30.

statements in documents prepared for the purposes of contemplated proceedings or criminal investigations¹ although logically, there are two very significant qualifications to the generality of this exclusionary rule. The effect of these exclusions, would be to exclude documents of the sort tendered in the case of R. v. Wood,² showing the analysis of metal ingots for the purpose of demonstrating in court the identity of two samples.³ However, this exclusion would be negated in cases of such evidence having been prepared by experts since their statements fall within the ambit of section 30 of the Criminal Justice Act 1988, which enables their inclusion as 'expert reports'. On this issue, Tapper (ibid. p.66), comments on the admissibility aspect of expert reports in relation to evidence which is derived from a computer, and submits, that despite the uncertainty of the status of section 69 of the Police and Criminal Evidence Act 1984, in terms of supercedence by the 1988 Act, the conditions of section 69 should be proved to have been complied with, in relation to the proper use and operation of computers used to prepare documents relied upon by the expert.

One important aspect of section 26 of the 1988 Act, relevant to exclusions/inclusions, is that it does specifically allow for the admissibility of '(a) the

-
1. As noted by Tapper (ibid p.180) the extension to criminal investigations has no precedent even in the broadly similar provision in the draft bill appended to the 11th Report of the Criminal Law Revision Committee, Cmnd. 4991 (1972) cl. 32 (3).
 2. (1982) 76 Cr. App. Rep. 23, CA.
 3. Tapper (ibid. p.181) also notes that another example would be the computer analysis of the control group of documents used for the purpose of comparison with the disputed statements as described in Niblett and Boreham Cluster Analysis in Court, [1976] Crim. L.R. 175.

furnishing of evidence in any form, notwithstanding the existence of admissible material from which the evidence to be given in that form would be derived; and (b) as to the furnishing of glossaries for such purposes as may be specified', when prepared for the purpose of helping juries to understand complicated issues of fact or technical terms. In such instances, Crown Court rules may make provision to enable a court to give leave for, or require, that evidence or a glossary is so furnished. The effect of this section is to regularise the position in cases where investigators rely on the use of computers and other forms of technology, to assist in the presentation of evidence in complex trials. The previous lack of legislative coverage, gave rise to a system of custom and practice regarding admissibility, as there were no precise guidelines laid down to cater for schedules and other materials which had been prepared by non-experts, for the purposes of criminal proceedings.

Thus, the 1988 Act liberalises a number of restrictive rules relating to means of tendering different types of evidence, and additionally provides that a copy of a document is as admissible as an original, notwithstanding the existence of the original, and no matter how many removes there are between the original and the copy¹ and that documents and copies can be authenticated in any manner approved by the court.

As noted below,² the effect of section 32 of the Act, relative to a person (other than the accused) giving evidence through a live television link in a trial on indictment or an appeal to the Criminal division of the Court of Appeal, is dealt with separately.

1. Section 27.
2. At pp. 105-108.

2.7.

MISCELLANEOUS OTHER STATUTES.

In addition to the general statutes discussed in the previous part of this chapter, a number of special cases have been identified, where as noted by Tapper (1988 at p.68) some special addition to, or modification of, the common law was felt to be required. An early example of this process is the Bankers' Books Evidence Act 1879, which was one of the first statutes to make inroads into the exclusionary rules of evidence in favour of the smooth operation of commercial practice. The primary purpose of this Act being, to ensure that the business of banking was not disrupted by the need to produce the bank's original records in court.

In permitting the use of copies, this Act began to make incursions into the hearsay rule in providing¹ for the entry to amount to prima facie evidence of the matters recorded in it. Although the definition in the original legislation referred exclusively to 'books' of various descriptions,² a robust interpretation has since been applied with regard to its modern day relevance.³

Schedule 6 of the Banking Act 1979, provides for a new section 9 (2),⁴ which has been expanded to take into

1. Section 3.

2. Section 9.

3. Barker v. Wilson [1980] 2 All ER 81 at 83, QBD, per L.J, thus; 'The Bankers' Books Evidence Act 1879 was enacted with the practice of bankers in 1879 in mind. It must be construed in 1980 in relation to the practice of bankers as we now understand it. So construing the phrase 'an entry in a banker's book', it seems to me that clearly that both phrases are apt to include any form of permanent record kept by the bank of transactions relating to the bank's business, made by any of the methods which modern technology makes available, including, in particular, microfilm.'

account the banks use of modern technology for the purposes of catering for its administrative functions. The phraseology of the new sub-section 9 (2), leaves little room for doubt that it will also apply to optical storage techniques and other forms of developing technology.

Tapper (ibid. p.71) notes that in order to be admissible, the record must be one made in the ordinary course of the business of the bank, that it must also have been under the bank's control,¹ and it must be further proved that the copy adduced in court has been examined against the original entry and is correct.² However, the same commentator (ibid p.71) observes that whilst it is uncertain how these provisions will be applied in the case of computers, they appear to have caused no difficulty in the case of R. v. Ewing, and anticipates that their satisfaction will only be challenged rarely.

The Data Protection Act 1984, imposes duties on data handlers and confers rights upon data subjects. The provisions of the Act may have an adverse impact on some commercial enterprises, and are designed to provide redress for grievances harboured by data subjects in relation to information which is processed automatically, and which is invariably in a computer. The Act, which provides for an elaborate scheme of registration, accordingly sets up a special tribunal to deal with appeals against the determinations of the registrar, and allows access to the ordinary courts for the redress of grievances which, for example, may be in order to secure compensation where damage has been caused by the use of inaccurate data.

-
1. Section 4.
 2. Section 9.
 3. [1983] QB 1039.

Tapper (ibid. p.72) observes that the Act contains no provisions which relate to the admissibility of evidence derived from computers, which in view of its purpose, might well have been designed to cover this eventuality. Instead, as noted by Tapper (ibid. p.72) the Act seems to assume that the ordinary rules can cope with such evidence without difficulty. In that connection, in the guidelines set out for establishing rules of procedure to be followed by the Tribunal for hearing appeals, reference is made to securing 'data material' as well as documents, inferring their admissibility in evidence but making no explicit provision for such admissibility.¹

Section 723 of the Companies Act 1985, is one example of the sort of provision which may be adopted to facilitate the use of modern business methods, particularly those which relate to provisions that institutions soliciting funds should keep adequate records as a check against fraud, which records are increasingly being held on computers, requiring explicit authorisation. By virtue of section 723 of the Act, power is bestowed, to keep such records 'otherwise than in legible form', but on the condition that, 'the recording is capable of being reproduced in a legible form', and the Act then simply transfers access provisions the legible form.

The samples of legislation which have been dealt with so far in this part of the chapter, are by no means a complete inventory. Tapper (ibid. p.73) particularises

1. In noting that despite the explicit mention that is made of such mundane matters as the summoning of witnesses and the administration of oaths, Tapper (ibid p.181) observes the contrast between the much more specific provision made for the consideration of computer records in the Insolvency Practitioners Tribunal (Conduct of Investigations) Rules 1986 SI 1986 No. 952 s. 7 (b).

details of more itinerant enactments which although too numerous to detail here, are mainly of the type infrequently encountered by those whose duty it is to investigate allegations of fraud. One example of the obscure nature of those cited by Tapper, appertains to the lists and registers which are explicitly authorised to be maintained by computer (in addition to those already mentioned under section 723 of the Companies Act 1985), is that of the Roll of solicitors which must be maintained by virtue of section 6 (2) of the Solcitors Act 1974. The practising status of a solicitor would have particular relevance in cases where they become criminally implicated with their clients. An example of this would be in cases involving mortgage frauds, as was recently encountered during one Old Bailey trial.¹

B. Conclusions.

Given that the police and other bodies who engage in the investigation of serious fraud, prudently observe the rules which govern the furnishing of 'techno-evidence', there seems no reason to suppose that such materials when derived from these media, cannot have as beneficial an effect upon the process of a complex investigation and the business of the courts, as they are already having upon the business of the modern world.

1. In the case R. v. Adelaja and others, (1988) unreported, the connivance of solicitors is alleged to have enabled the fraudulent transaction to have taken place.

CHAPTER THREE.

COMPUTER FRAUD INVESTIGATION AND THE ADDUCTION OF COMPUTER RECORDS

A. Introduction.

There is a great deal of controversy regarding the extent to which the incidence of computer frauds has become a special problem in modern society.¹ Ironically, the ease with which devices such as computers relieve the tedium of human involvement in complex tasks also provides something of a safe haven for those who perpetrate fraud via this electronic medium.

This chapter therefore considers the social definition of computer fraud, and the statutory reforms, which, although palliative towards the use of technology in the management of information, have yet to provide approaches that will enable 'techno-fraudsters' to be charged with offences that stand up in court.

New concepts in legal procedures such as preparatory hearings, are also discussed in this chapter, and the effect of decisions made during these hearings upon the subsequent conduct of the trial itself. In the final section, further consideration is given to the manner in which evidence such as spreadsheets and computer graphics should be authenticated, when prepared by fraud investigators for presentation to juries during the trial phase.

-
1. For a discussion on this controversy, see Levi. M., (1987).
 2. See for example; R. v. Gold, pp. 63-64, below.

3.1. AN INTERPRETATION OF COMPUTER FRAUD.

There have been numerous attempts to define computer fraud and its broader concepts in terms of computer crime generally. Soma (1986 at p.265) in noting the observations of Bequai, expresses the views from one school of thought which believes that there is no widely accepted definition of computer crime, but includes a concise inventory of matters which might be considered appropriate to those which are paradigmatic of this category. Soma's interpretation of computer fraud (ibid. p.264) is that it is merely one branch from the tree of computer crime, covering a number of different kinds of occurrences, in, around and through a computer that can be classified, if not necessarily prosecuted, as illegal acts.

Offences which may fall under the classification of computer fraud/crime, range widely to incorporate such aspects as: misappropriation of computer time; theft of: software, computer data, services, trade secrets, or finances, by means of its use. Intentional damage to: computer hardware, or its processing facilities, and even industrial or commercial espionage. These crimes may vary according to the degree of inspiration used during the modus operandi by their perpetrators, and may attract such jargon as 'data diddling', as well as many others.¹

Concern in some quarters where there is a belief that computer frauds had become a special problem in the last decade,² tend not to receive the authoritative support of

1. A brief but by no means comprehensive overview of some of these terms; are 'a trojan horse, the salami technique, superzapping, trap doors, logic bombs, data leakage, wire tapping, simulation and modelling, piggybacking, impersonation and scavenging. Source, Soma (ibid. p.264).

2. As observed by Levi (1987 at p.8).

those such as the Audit Commission which, as noted by Levi (ibid. p.7) must be treated with scepticism. The Metropolitan fraud squad, whose views on computer fraud are contained in the 1987 Annual Report of the Commissioner of Police for the Metropolis, observes that whilst incidents of computer fraud had increased, 'there was still a strong suspicion that this type of crime is often unreported', thus echoing the unease that is nevertheless, often felt in many circles in relation to the 'techno-crime' phenomena. Part of the difficulty of recognising computer fraud, is expressed by the Institute of Chartered Accountants (1987a at p.9) who in drawing attention to the special risks that computers present, also add that many misunderstandings still exist about the nature of computer systems in relation to their impact on the possibility or likelihood of fraud.

Levi (ibid. p.37) expounds his own theory, that the social definition of computer fraud is one of a growing number of 'new' technocrimes which is accompanied by those such as the media, who have an obsession about 'hacking' into computer systems and obtaining information or manipulating data, either for money or for amusement. Levi (ibid. p.37) further expresses the view, that press reports, which from time to time draw attention to computer frauds that have been perpetrated by schoolchildren, highlights what amounts to a temporary phenomena. This being the result of a generation gap between the 'have-nots' who were educated in a pre-computer era and the 'haves' who are being educated today. Such a syndrome observes Levi (ibid. p.38) reveals a 'kind of Chaplinesque morality', where computer frauds are perpetrated by little men who humiliate and triumph over those in authority.

Despite Levi's somewhat flippant approach to the subject of computer fraud in general, and his comparison (ibid. p.41) that, as with some of the official views of the mafia, 'computer fraud is a commercial bogeyman whose psychological significance is enhanced, rather than diminished by lack of evidence', the police approach to computer fraud is to regard it as a crime which should be treated seriously, and with the same degree of professional respect that is attributed to all other forms of complex crime. As to guarding against computer fraud and other forms of computer crime, that is to be considered in the next part of this chapter.

3.2.

GUARDING AGAINST COMPUTER CRIME.

However careful the perpetrators of computer fraud may endeavour to be in conducting their clandestine operations, there is always the likelihood of some unexpected event to uncover their plot. This was certainly the position in the case of Ward v. Superior Court¹ when the only clue that led to the discovery of the crime was the coincidental dumping of punched cards that occurred concurrently with the telephone intrusion of the system. The brief circumstances of which incident involved alleged attempts by an employee of a computer company known as UCC, to gain the competitive edge over a rival company called ISD, by transmitting the program in ISD's computer system; to which access had been previously gained via the pirate company's data phone.

The ability to detect computer crime outside of accidental discovery, however, is reliant on the degree of formal investigation and auditing techniques that a particular organisation sees fit to employ. The preferred course for implementing this aspect of business practice, is seen by one commentator² as assigning the responsibilities to a single individual or a department against adherence to a computer security plan. The concept of adequate internal controls is also supported by the Institute of Chartered Accountants in England and Wales (1987a at p. 32) who base their opinion on two investigations which were commissioned in 1985 (ibid. p. 32).

The role of the auditor also has some significance, although, due to the expansion in the size of companies over the past 130 years, their task is now considered by

1. See 3 Comp. L. Serv. Rep. 206. (Cal. Super Ct. 1972).

2. Fausse, Computer Security. What can we do? 4 Equity 1, (May 1985).

some, to be 'watchdogs' and not 'bloodhounds' (ibid. p.31) in defending the truth and fairness of financial statements; and whether they have been properly prepared in accordance with the Companies Act 1985.

Auditors who experience a conflict between their traditional duty of confidentiality to their clients, and their consciences, when fraud involving their clients is revealed, may consult the guidelines issued by the Auditing Practices Committee, which is entitled 'Fraud and other Irregularities',¹ or seek guidance on problems of an ethical nature from the Professional Conduct Directorate of the Institute of Chartered Accountants in England and Wales (ibid. p.33).

As noted in another of the Institute's publications,² fraudulent trends resulting from the implementation of new technology, will become significantly affected by the growth in networks and communication facilities that will provide far wider access to data systems and the increased use of on-line data communications within organisations and less use of paper input and records. There will also be far greater inter-connection of systems between organisations to facilitate the sharing and transmission of data. These fraudulent trends will gather momentum as (ibid. 1987b at p.48) 'organisations attempt to reduce paper, speed of communication in business becomes more important, standards for 'electronic invoicing' data transfer emerge, public and administrative organisations such as the Inland Revenue and Customs and Excise promote the concept, and wider acceptance of 'OSI'³ architectures establishes the technical framework within which such systems may operate.

-
1. Institute of Chartered Accountants (1987a at p.32).
 2. Institute of Chartered Accountants (1987b at p.48).
 3. Open Systems Interconnection.

Proper measures for guarding against computer fraud, should, like charity begin at home, or more appropriately, the workplace. Where instances of computer fraud are discovered, the type of action that management are expected to take, should be firmly laid down in a company security policy (ibid 1987b at p.35). Even when the likelihood of loss recovery may be small, a robust approach towards the investigation of suspected fraud is preferable, in order to show the readiness of the company to take appropriate action.

3.3.

INVESTIGATION OF COMPUTER CRIME.

Until the Serious Fraud Office was established, the investigation of computer crime was a specialised area of policing which invariably fell within the ambit of fraud squads for enquiry, in the event that such incidents were reported to the police. However, the Director of the Serious Fraud Office may now invoke his powers under the Criminal Justice Act 1987,¹ to deal with appropriate cases of computer fraud which are of such seriousness or complexity, to warrant his intervention.

The Director of the Serious Fraud Office may also, if he thinks fit, conduct any such investigation in conjunction with the police or with any other person who is, in the opinion of the Director, a proper person to be concerned in it.² However, it is anticipated that the majority of computer frauds will amount to the less serious variety, than that for which the Serious Fraud Office was established, and in view of this the police will not only continue to remain responsible for this area of investigation, but may also find themselves working in tandem with the staff of the Serious Fraud Office during the more serious aspects of these offences.

Although the law has now advanced by increasing the availability of resources for the investigation of fraud, with the formation of the Serious Fraud Office and other recent aspects of legislation,³ it seems to have fallen

-
1. Under section 1 (3).
 2. By virtue of section 1 (4).
 3. Such as the Criminal Justice Act 1987 and Criminal Justice Act 1988 generally, and for example, by virtue of sections 31 and 32 of the Criminal Justice Act 1988, which allows for the admission of information technology as a medium for presenting, as well as communicating evidence.

short in providing adequate legislation to deal with those who perpetrate fraud by means of computer. This was certainly the position in the case of R. v. Gold and another, as reported by Golden. A.,¹ which defendants, who after initially being found guilty of creating a false instrument within the meaning of the Forgery and Counterfeiting Act 1981,² later had their appeal against conviction upheld by the Court of Appeal, which supported the contention that the language of the Act was not intended to cover computer hacking.

The prosecution, despite being granted leave to appeal to the House of Lords, having certified that points of law of general public importance were involved, had their appeal dismissed by Brandon L.J., whose summarised judgement of the House, is further observed in a report by Golden. A.,³ as sharing the view of the Court of Appeal (Criminal Division), it being expressed by Lane L.C.J., 'that there was no reason to regret failure of what had aptly been described as the 'procrustean attempt' to force the facts into the language of an Act not designed to fit them'.

The same difficulties are also shared by law enforcement agencies in other jurisdictions, as echoed by Soma (1986 at p.280) in noting the observations of FBI Director William Webster who when addressing a meeting ASIS (American Society for Industrial Security), stated, 'there is at present no existing effective legislation ... to meet the threat of computer fraud', adding (ibid. p.280) that 'to shoehorn a computer abuse into traditional statutory concepts, is often time-consuming and consequently leads to low conviction rates'.

-
1. Ibid. 57 Computers and Law, September, 1988, at p. 14.
 2. Sub-section 8 (1).
 3. Supra footnote 1, above.

Despite these problems, the need to improve specialised training facilities for fraud squad officers in computer crime investigation techniques,¹ has met with a positive response, and appropriate skills are now gradually being introduced to face the challenge posed by technocrimes. In the present climate of development, however, the complexities of computer-related crime, still present law enforcement officers with unique and serious problems,² one of which is the potential for the complexities of the computer to overwhelm investigators.³

The New Mexico Law Enforcement Academy suggests such a methodology that should be followed during a computer crime investigation, which as noted by Soma (ibid p.277), operates under these seven general categories, of (a) initial investigation, (b) investigation planning, (c) information gathering, (d) interviewing and interrogation, (e) technical data system review, (f) criminalistics and, (g) case presentation.

-
1. Since the publication of the Fraud Trials Committee Report, a four week course is held twice annually at the Police Staff College, Bramshill. This provides the necessary technical training to be undertaken, and since March 1986, when these courses began, 41 officers have been trained. However, the transfer to other duties of some trained personnel, has seen a diminution of this figure.
 2. Bureau of Justice Statistics, US Dept of Justice, Expert Witness Manual: Use of Outside Experts in Computer Related Crime Cases, 1-7 to 1-11 (1980) (detailed list of unique features of computer-related crime and litigation); Swanson and Territo, Computer Crime: Dimensions, Types, Causes & Investigations, 8 J Police Sci & Ad 304, 311 (1980) ('The investigation of computer crime requires special awareness and, as the complexity of schemes increases, definite technical capabilities.')
 3. See generally, Shaw, How can you fight what you don't understand?, L & Or, July 1977, at P.5.

In addition to the senior investigating officer and his investigation and administrative support staff, other personnel used during the course of an investigation, might in appropriate circumstances, include, (a) a computer technician, (b) charting and data analyst, (c) scenes of crime officer, (d) photographer and/or video camera team, (e) forensic scientific officer (which might also include a questioned document examiner¹).

In criminal proceedings, the search and seizure of evidence of computer related crime is a relatively recent phenomena. Due to the difficulties faced in providing accurate descriptions of the nature and object of their search, consultations with experts to assist police in describing to a judge or a magistrate what was stolen or misused, will often be beneficial. This was certainly the position in the American case of Ward v. Superior Court, as observed by Soma (ibid. pp.277-278) who, in describing how a judge was asked to sign a search warrant to authorise the seizure of 'computer memory bank or other data storage devices, magnetically imprinted with ISD (Information Systems Design), remote ploemote plotting programs', wondered when such technical data was shown on search warrant informations, how a judge could be expected to know what the search warrant was designed to find, or if, the local police officers would know where or how to look for the object of the search.

Powers are given to police under the Police and Criminal Evidence Act 1984,² to enable the search for, and seizure of, evidence in the form of information which is contained

-
1. See Crown. D.A., Dr. The Role of the Questioned Document Examiner in Computer Crime Investigations. Computer Security Readings from Security Magazine (1987). At pp. 289-292.
 2. Section 19 (5).

in a computer. This authority is only effective, when the constable 'is lawfully on the premises.'¹ When the information is contained within a computer which is situated on the premises undergoing search, the provisions of the Act enable the constable to require it to be produced 'in a form in which it can be taken away and in which it is visible and legible'.

As in the general scheme of the Police and Criminal Evidence Act 1984, sub-section 19 (5) contains the requirement of reasonableness on the part of police, and accordingly, the constable must have 'reasonable grounds' for believing that '(i) it is evidence in relation to an offence which he is investigating, [or any other offence]; or (ii) it has been obtained in consequence of the commission of an offence.

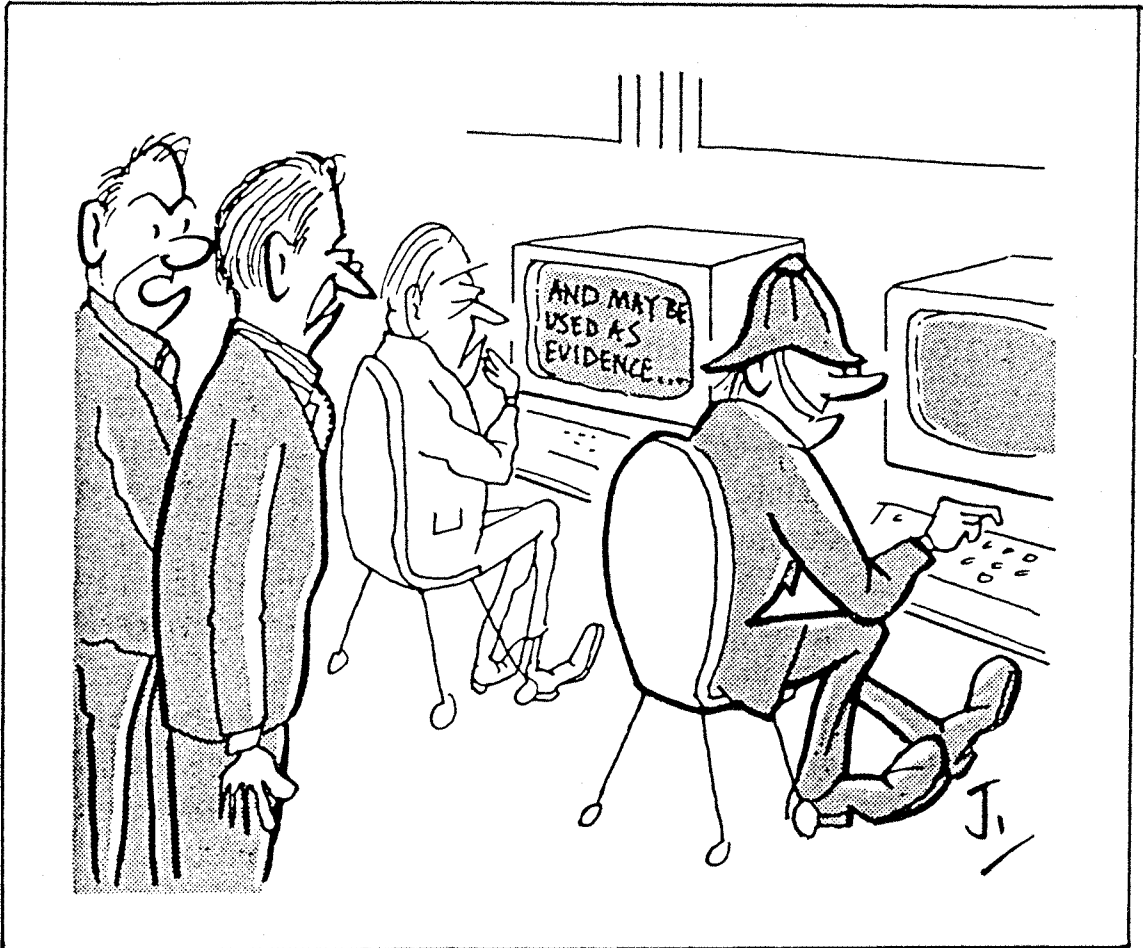
The words 'or any other offence' shown in parenthesis above, would appear to provide police with sufficient latitude to require the production of such information when they are relying on the advice or instructions of someone else. As for example, in a case under investigation by the Serious Fraud Office who are seeking police assistance during search. However, the interpretation of a police officer's 'reasonable grounds' when acting under the guidance of an expert such as a computer technician, has given rise to contrary views in other jurisdictions.

An American case in point, is that of People v. Superior Court of Santa Clara County² where a similar contention resulted in the overturning of the lower court's contrary ruling by the Court of Appeals, whose findings may be

1. E.g. when acting in pursuance of a search warrant.
2. Ibid. 104 Cal. 3rd 1001. 163 Cal Rptr. 906 (1980).

Figure 2.

Investigating computer crime.



'The police are really up to date these days!'

Reproduced by kind permission of the Institute of Chartered Accountants in England and Wales, publishers of Countering Computer Fraud.

summarised as, 'the presence, and participation of the officer in executing the warrant cannot be sensibly be understood to require knowledge which the police officer could not be expected to possess. Consequently, we think that there is no requirement that such experts, prior to stating their conclusions, engage in the futile task of attempting to educate police officers in the rudiments of computer science'.

3.4. PRE-TRIAL ADDUCTION OF COMPUTER RECORDS.

As noted by Tapper, (1988 at p. 75) the common law civil procedure enables parties to proceedings to compel their adversary to 'discover' information in the possession of an adversary through a process of compulsory disclosure, which originated in the courts of Chancery being concisely summarised in Flight v. Robinson.¹

In cases as for example, where there are good grounds for suspecting that the party in possession of the relevant material will destroy or tamper with it as soon as he learns that it has come to the knowledge of his opponent, it is sometimes necessary for a party to act more swiftly and more surreptitiously, than by the normal process of discovery. The first case to be tested by the Court of Appeal, Anton Piller K.G., v. Manufacturing Processes Ltd,² related to the validity of a new extraordinary process to counter this difficulty, which involved the hardware and plans of a computer. The application of this procedure to computer software was later upheld in Gates v. Swift.³

In noting the extraordinary nature of Anton Piller orders Tapper (ibid. p.82) alludes to the example given in the case of Booker McConnell PLC v. Plascow⁴ in observing that 'the courts have always proceeded justifiably, on the basis that the overwhelming majority of people in this

-
1. [1844] 8 Beav. 22, thus, 'The general rule is, that a defendant is bound to discover all the facts within his knowledge, and to produce all documents in his possession, which are material to the case of the plaintiff'.
 2. [1976] Ch 55, CA.
 3. [1981] F.S.R. 57, Ch. (order only). [1982] R.P.C. 339, Ch, (also including headnote and argument of counsel).
 4. [1985] RPC 425, CA.

country will comply with the court's order' and that it is regarded as unnecessary in every case to empower the plaintiff's solicitors to search the defendant's premises, under the provisions of the Anton Piller procedure, which was devised by the High Court.

Evidence which is required to be secured for the purposes of criminal proceedings must be obtained by way of a search warrant. The law relating to the searching of premises and seizure of property, was codified in Part II of the Police and Criminal Evidence Act 1984, and guidelines for its exercise set out in the Code of Practice issued pursuant to section 66 of the Act. However, it should be noted that magistrates may issue search warrants only if on being satisfied that there are reasonable grounds to believe that a serious arrestable offence has been committed, that material valuable to its investigation is to be found on the premises in question, that the material is likely to be relevant evidence, and that unless the warrant is issued the material is unlikely to be forthcoming.¹

The Code of Practice deals specifically with material held in a computer and provides² that an officer 'may require the information to be produced in a form that can be taken away and in which it is visible and legible'. This provision is separate to that which enables an officer to take away a copy in machine readable form under para. 6.4., and which also empowers a police officer to

-
1. Police and Criminal Evidence Act 1984 section 8. The evidence should be admissible in criminal proceedings, and not fall within stated categories of excluded material, that is of a privileged, confidential, or journalistic nature.
 2. Code of Practice for the searching of premises by police officers and the seizure of property found by police officers on persons or premises (1985) para. 6.5.

photograph or copy any document or other article.

The Police and Criminal Evidence Act 1984 is not an 'exclusive and exhaustive' code for search and seizure, and different powers exist under other provisions. An example of this in the context of computers, is the subsequently enacted Financial Services Act 1986, which contains further provisions allowing warrants to be issued in respect of offences of fraud and insider dealing, in relation to evidence involving computers. This legislation¹ bestows similar powers to those named in the search warrant, as are granted to police officers under the Police and Criminal Evidence Act 1984.

Tapper (ibid. p.85) also observes that in addition to these general provisions, specific powers authorise magistrates to issue warrants in intellectual property cases. Included in the examples given by Tapper, are those under section 21 of the Copyright Act 1956, which create certain criminal offences in relation to copyright. These provisions have in turn been amplified by the Copyright (Amendment) Act 1983 and the Copyright (Computer Software) Amendment Act 1985. The former amplified the power to issue search warrants in the case of films and sound recordings, while the latter extended the amplified powers to infringing copies of computer programs whether they consist of 'a disk, tape or chip or any device which embodies signals serving for the importation of the program or part of it.'²

This legislation apes the Anton Piller procedure in permitting the authorisation of other persons to accompany the constable executing the warrant³ but the wording does

1. Section 199 (3).

2. Copyright (Computer Software) Amendment Act 1985 s. 3.

3. Copyright Act 1956 sub-sec. 21 (A) (2) as amended.

not seem apt to permit such persons to participate in the conduct of the search, nor does it seem that it may be his reasonable belief that any material is evidence of the commission of an offence under the Act which justifies its seizure, though, as argued by Tapper (ibid. p.86) there is no reason to suppose that his view might not be influential in assisting the constable to form such a view as is required by legislation.

Under Order 29 rule 3 (1),¹ the court may 'order, authorise or require' any sample to be taken of property which is in issue, or, similarly order observation to be made on such property or any experiment to be tried on or with such property. These powers cover the simulation of devices, of which the most common are those incorporating a computer used to measure or calculate, as in modern breath-testing² or assaying³ devices.

An unusual example of the use of the computer to prepare evidence especially for a criminal trial occurred in 1975,⁴ relating to the veracity of the confession attributed by police to a defendant. The technique was so new and unfamiliar to the court, and in order to support its reliability, the defence were permitted to exhibit the results of the application of the same tests to two other pairs of documents,⁵ similar to a special computer analysis of the disputed document as compared with another of undisputed authorship, tendered by the defence.

-
1. In patent cases Order 104, rule 10, would also be available.
 2. Such as Castle v. Cross [1985] 1 All ER 87, QBD.
 3. Such as in R. v. Wood [1982] 76 Cr App. R. 23 CA.
 4. Described in Niblett and Boreham Cluster Analysis in Court, [1976] Crim. L.R. 175.
 5. Showing that the two confessions were more alike than the novels of Damon Runyon and the Book of Common Prayer, but less alike than the sonnets of Shakespeare and Wordsworth.

Although Tapper (ibid. p. 88) observes that the use of computer simulation techniques has been further developed in the United States than in England, and discusses the implications of legislation in relation to evidence which is held in a computer situated abroad (ibid. p. 90) it is the aspect of evidence which is required for other jurisdictions (ibid. p.93) that reveals an unusual slant. In the context of technology generally, this example relates to the case of J. Barber and Sons v. Lloyds Underwriters,¹ where the request by an American Court for witness interviews to be video-taped, whilst being allowed by the court in principle, was permitted under the proviso that the filming must take place outside of the confines of the court, in order to conform with the provisions of the Contempt of Court Act 1981.

1. [1986] 2 All ER 845 QB.

PREPARATORY HEARINGS.

The value of preparatory hearings in the context of information technology, lies with the opportunities they afford to develop concepts that may have arisen since the case was first committed for trial, owing to the lapse of time, and inevitably people's memory. Thus, in the case of R. v. Gardner and others,¹ in which difficulties had arisen after committal regarding outdated plans of a large government building, the problems were able to be resolved when agreement was reached which enabled the admission of a pre-recorded video-taped film, containing relevant scenes within the building which were pertinent to the matters contained within the indictment.

Preparatory hearings are the subject of nineteen of the recommendations made by the Fraud Trials Committee in their Report (1986a at p.86), upon which the main scheme of the Criminal Justice Act 1987, is based. Such concentration of effort on the concept of preparatory hearings in general, revealed the level of dissatisfaction with the pre-trial procedures that existed before the implementation of the 1987 Act. Under section 7 (1) of the Act, guidelines are laid down for these new provisions, which enable a judge of the Crown Court to hold a preparatory hearing, if he is satisfied that the evidence on an indictment reveals a case of fraud of such seriousness and complexity, that substantial benefits are likely to accrue from such a hearing, namely;

1. [1987] unreported, Central Criminal Court. This was one of the first cases (if not the first), to be listed under the new preparatory hearing scheme. Although this case preceded the enactment of the Criminal Justice Act 1987, which provides for preparatory hearings to be held, the Gardner case amounted to a 'dry run' in terms of testing the machinery of the court to function in this way.

- '(a) identifying the issues which are likely to be material to the verdict of the jury.
- (b) assist their comprehension of any such issues.
- (c) expediting proceedings before the jury, or
- (d) assisting the judge's management of the trial.'

By virtue of section 8 of the Act, a preparatory hearing is now deemed to be an integral part of the trial. The shrewdness of the Fraud Trials Committee in making that particular recommendation, which led to the phraseology of this Part of the Act, lies in providing for the appropriate levels of fees that counsel may now seek for their professional participation and physical appearance at court, rather than relying on junior and less qualified representatives from their chambers, as was previously the case.

Particular advantages that are associated with the new styled preparatory hearings, are those which enable difficulties to be resolved before the jury has been sworn. Under section 9 of the Act, a judge may adjourn a preparatory hearing from time to time, in order to enable problems that have been identified to be resolved,¹ determine applications for dismissal of the charge² and deal with any question as to the admissibility of evidence³ and any other question of law relating to the case.⁴

Under section 9 of the Act, a judge is enabled to order the prosecution to supply to the court and to the defendant(s) a 'case statement'⁵ outlining the principle

1. Sub-sec. 9 (1).
 2. Sub-sec. 9 (3) (a).
 3. Sub-sec. 9 (3) (b).

4. Sub-sec. 9 (3) (c).
 5. Sub-sec. 9 (4) (a) (i).

facts of the prosecution case, with witnesses who will speak of them,¹ the relevant exhibits² and any proposition of law on which the prosecution intend to rely³ which matters are to be reconciled with the counts on the indictment. Further provisions under this section enable the judge to direct the prosecution, to prepare their evidence and other explanatory materials, 'in such a form as appears to him to be likely to aid comprehension by the jury',⁴ to give notice to the court and defendant(s) 'of any documents of which the truth ought in the prosecution's view to be admitted' and other matters which ought to be agreed.⁵

It is only when the prosecution have complied with their obligations to the satisfaction of the court, and the defence,⁶ that the judge may then order the defendant(s) (subject to the conditions under section 10), to comply with any requirements set out under sub-section 9 (5) of the Act, relative to furnishing a general written statement of the defence case, notice of objections to the prosecution's case statement,⁷ relevant points of law⁸ and a notice stating the extent of any areas of agreement with the prosecution's case.⁹

It is not surprising that under the English system of law, the responsibilities of the prosecution must first be

-
1. Sub-sec. 9 (4) (a) (ii).
 2. Sub-sec. 9 (4) (a) (iii).
 3. Sub-sec. 9 (4) (a) (iv).
 4. Sub-sec. 9 (4) (b).
 5. Sub-sec. 9 (4) (c).
 6. Where in consequence of an objection by the defence, the 'case statement' should be amended, provision in favour of such amendment is allowed under sub-sec. 9 (4) (d).
 7. Sub-sec. 9 (5) (i).
 8. Sub-sec. 9 (5) (ii).
 9. Sub-sec. 9 (5) (iii).

met, before the attention of the judge can be directed towards the defence, in imposing any requirements upon them that may be relevant under the circumstances.

Provisions under sub-section 10 (1) of the Act enable the trial judge to make comment if either party departs from the case disclosed at any earlier preparatory hearing, or fails to comply with any requirement that was imposed at such a hearing. In such an instance, a jury is entitled to draw proper inference arising from a trial judge's comments and whether there was justification for doing so.¹

In cases of appeal, this will lie to the Court of Appeal if it arises from any order or ruling of a judge upon the determination of any question as to the admissibility of evidence or any question of law relating to the case, subject to the leave of the judge, or Court of Appeal,² Criminal Division.³ The judge may nevertheless continue a preparatory hearing even if an appeal has been granted although the jury shall not be sworn until after the conclusion of the appeal⁴ and the Court of Appeal has power under this section of the Act to confirm, reverse or vary the decision appealed against.⁵

It could be argued that the decision to allow an appeal, before the case is put to a sworn jury, would add to delay in the process of justice. There can be little doubt, however, that the overall value of a preparatory hearing is eminently more suitable in complex cases. The new framework should enable many issues to be clarified before the juries are sworn and thereby reduce much of the time previously taken up on matters of 'voir dire', which have

1. Sub-sec. 10 (2) (b).

2. Sub-section 9 (11).

3. Sub-sec. 9 (12).

4. Sub-sec. 9 (13).

5. Sub-sec. 9 (14).

excluded juries from the courts and often contributed to their uncertainties.

In terms of aiding the development of technology in the courtroom, preparatory hearings will help all parties to identify the way forward in advance of the trial, enable technicians to familiarise themselves with the layout of the court and plan the siting of appropriate equipment. Above all, however, it should enable society to mete out a better standard of justice to victim and defendant, alike.

3.6.

TRIAL.

The Roskill Committee, concerned about the difficulties experienced by juries in assimilating complicated information in the form in which it had been traditionally presented to them, considered a number of ways in which this could be improved, including the use of computer terminals.¹ This observation appears to be a clear indication of a perceived expansion in the use of computers and other forms of information technology during future trials. The importance, therefore, of evidence derived from computers, will also inevitably increase and greater reliance will undoubtedly be placed upon the provisions made by the Police and Criminal Evidence Act 1984, which under Schedule 3 Part II Paragraph 8, requires that a certificate should be tendered with the statement adduced, pursuant to section 69,² thus;

- '(a) identifying the document containing the statement and describing the manner in which it was produced;
- (b) giving particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;
- (c) dealing with any matters mentioned in sub-sect. (I) of sect. 69 above; and
- (d) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer.'

Under this legislation, the court has power to require oral evidence to be given of any matters capable of being included in such a certificate,³ although it is still a criminal offence to tender a certificate known to be false or not believed to be true.⁴

1. Fraud Trials Committee Report, (1986a) para 9.24.

2. See also pp. 33-37 above, regarding authentication.

3. Schedule 3 Part II para. 9.

4. Paragraph 10.

A document made admissible under these provisions may be proved¹ either by the production of that document or the production of a copy or material part of a copy, authenticated in such manner as the court may approve. It will be noted that the court is here given a discretion as to the means of authentication.

The Act also bestows general rule-making powers² which in the view of one observer, i.e. Tapper (ibid. p. 101) do not yet appear to have been exercised. The Criminal Justice Act 1988 is still less specific, and contents itself by providing in section 27, that 'a document or a copy of a document may be authenticated in such manner as the court may approve, for the use of a statement in it in criminal proceedings'. This section also adds, that 'it is immaterial how many removes there are between a copy and the original.'

Where in criminal proceedings under the Police and Criminal Evidence Act 1984 Schedule 3 Part II paragraph 9, the court may require oral evidence of any matter relating to the adduction of a certificate in evidence, this would have the effect of bringing the relevant manager or operator involved in the transaction of such computer derived evidence, before the court for cross-examination.

In the case of evidence derived from a computer which is admitted in derogation of the hearsay rule, it is necessary to satisfy the provisions of both section 68 and section 69. The general provisions as to weight, appear in Schedule 3 Part I paragraph 7 in relation to section 68, and in Part II paragraph 11 in relation to section 69. These provisions are closely modelled upon those of the

1. Paragraph 11.

2. Sub-section 69 (2) and Schedule 3 Part III para. 15.

Civil Evidence Act 1968, and, as noted by Tapper (ibid. p.109) cover the same ground of contemporaneity and motive to conceal or to misrepresent. The terminology of 'supply' of information is repeated, and paragraph 12 elaborates its meaning in providing¹ that; 'information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment.'

In criminal proceedings the Criminal Justice Act 1988, has made special provision for the furnishing of experts' reports by hearsay, although if the maker is not to be called, it is necessary to enlist the leave of the court. It is worthy of note that this provision, unlike the Civil Evidence Act 1972, makes no attempt to exclude evidence derived from computers. Given the nature of the computer and the general unfamiliarity of the courts with the principles of their operation, it is envisaged as noted by Tapper (ibid. p.110) that it will often be necessary to adduce expert evidence on these matters.

In the context of technology, section 31 of the Act dealing with form of evidence and glossaries and section 32, which provides for the giving of evidence through live television links, may be supplemented due to the powers that have been conferred under these sections to enable Crown Court Rules (and in the case of section 32, also the Criminal Appeal Rules), to be made. Such provision enables the making of rules which appear necessary or expedient for the purposes of both sections. Those responsible for drafting these provisions have been wise to allow sufficient latitude for the courts to develop; as familiarity with technology increases; and so avoid the

1. c.p. Civil Evidence Act 1968 sub-section 5 (5) (a).
2. Sub-section 30 (2).

restrictions imposed by earlier, more inhibiting, legislation.

B. Conclusions.

The inadequacy of statutory concepts to deal appropriately with the prosecution of 'techno-crime', has already been noted.¹ Whilst radical changes to the law now enable case information to be managed and presented to juries more effectively, there is still nevertheless an area of unfinished business, concerning the practical implementation of section 31 of the Criminal Justice Act 1988, relative to the furnishing of glossaries of technical terms.²

However, given the degree of cooperation that currently exists between investigating and prosecuting agencies in the development of their mutual needs,³ there is little doubt that these undelegated tasks can be tackled successfully, by adhering to the concept of the multi-agency approach

1. At page 56, above.

2. For example, one of the proposals of the Fraud Trials Committee in their (1986a) Report, alludes to the input of all known technical, legal and financial terms, likely to be encountered during a complex fraud case, to be entered into a computerised database for selective retrieval, based on their relevance to a particular case. The Report does not however offer any guidance as to whose responsibility this should become.

3. As demonstrated by jointly sponsored events such as the series of one day seminars discussed at pp. 93-94, below.

CHAPTER FOUR.

PROSECUTING SERIOUS FRAUD WITH TECHNOLOGY.

A. Introduction.

This chapter begins by considering the formation of the Serious Fraud Office, whose joint investigative and prosecutive role, will make incursions into territories which were previously considered to be the exclusive domains of the police and other specialised fraud investigating bodies. Some of the psychological and technological issues involved in presenting complex information are then aired, before discourse is given on recent uses of courtroom technology during trials.

The giving of testimony by adult witnesses in fraud trials, is legislatively linked to factors which involve child witnesses in abuse cases, due to the medium of television. Nevertheless, separate provisions do apply to each of these two categories of witness under the Criminal Justice Act 1988, and are only discussed jointly in this chapter, as factors affecting each particular group of witness are likely to have a bearing on the other.

This aspect of this research demonstrates quite distinctively, that the use of technology is beginning to mushroom in the court rooms of the North American continent and in similar establishments in this country. It also supports the theory, that the use of technology, may in certain circumstances, add to the quality of justice that is meted out by the courts.¹

1. See under 'Conclusions', at page 108 below, with reference to measures which reduce instances of reoffending.

4.1.

THE SERIOUS FRAUD OFFICE.

The Criminal Justice Act 1987, which was only part of a larger Bill to be passed before the General Election of that year,¹ represented a positive Government response to the important work of the Fraud Trials Committee, whose Report had drawn attention to;

'The need for a new unified organisation responsible for all the functions of detection, investigation and prosecution of serious fraud cases, should be examined forthwith.'

The Act commanded wide support in Parliament and amongst other achievements, provided for the establishment of a statutory body, the **Serious Fraud Office**,² to be responsible for those functions mentioned in the last paragraph. The provisions of this Act apply to English and Welsh courts as well as those in Northern Ireland.³

Although the Act has not been drafted to include a definition of 'serious fraud', it has been worded with sufficient flexibility to enable the interpretation to be made, that the 'Director of the Serious Fraud Office may investigate any suspected offence which appears to him on reasonable grounds to involve serious or complex fraud'.

The Director of the Serious Fraud Office has extensive investigative powers. These may be delegated to others within or outside the SFO (other than the police) to investigate any person, whereby he may cause a written notice to be served to the person under investigation, or

1. Fraud Trials Committee Report, (1986a). In particular, see recommendation 1, at page 179 in Chapter 11 of the Report.

2. Section 1.

3. Sub-section 1 (1).

anyone believed to have relevant information. This notice may require them to answer questions and/or produce documents. Copies may be taken of documents and explanations sought. The SFO can also apply to a magistrate for a warrant authorising a constable to enter and seize documents. It is a criminal offence to fail to comply with the SFO requirement, to give false or misleading statements, or destroy or conceal relevant material. These offences are punishable by imprisonment or a fine or both.

The Director of the Serious Fraud Office has considerable power to disclose relevant information to other bodies involved in the control of fraud, to disciplinary bodies and to enforcement agencies overseas. However, there are some statutory restraints on disclosure, and it is always necessary for information to be handled with discretion.

The SFO began operations on 6th April, 1988, under the powers granted to it by the Criminal Justice Act 1987, and with specifically declared 'long-term' and 'intermediate' objectives.¹ The more intermediate aims of the SFO, relevant to the use of technology arising from the investigation (and subsequent presentation of evidence during criminal proceedings) are, chronologically speaking, those which link the development of expertise in such specialised areas as, computer (and other) frauds,² and making use of new trial procedures for complex frauds,³ incorporating also the need to consider how⁴

-
1. See Saxby ed., The Serious Fraud Office, 1 Computer Law & Security Report (1988). Vol. 4. at p.6.
 2. University of Southampton Institute of Criminal Justice Conference Paper, 22nd March, 1988. Dealing with Serious Fraud. Lecture notes on the Serious Fraud Office, 'objective (d)'.

 3. Supra note 2, above, objective (e).
 4. supra note 2, above, objective (f).

'to present evidence in such cases in new, more palatable ways, so that the average members of a jury can understand it.'

The machinery for rendering admissible these modern methods of presenting evidence, is contained within section 9 (4) (b) of the Act, which provisions are somewhat limited in that whilst they empower a judge of the Crown Court to order the prosecution to 'prepare their evidence in ways likely to aid jury comprehension', they appear insufficient to enable him to make similar requirements of the defence. In this context the effect of the Act has been somewhat diluted, even when allowing for the tradition of British justice which leans in favour of the defendant, as previously stated above.¹

This legislation is designed to deal with fraud cases which are serious and complex, as specified under section 7 (1) of the Act. This seems to ignore instances whereby serious fraud cases may not necessarily be complex (albeit that that in the majority of cases they are), and vice versa. Neither does the Act entitle a judge to any discretion to order a preparatory hearing in other complicated areas of criminal proceedings, (i.e. complex financial transactions involving drugs profiteering), before the Higher Courts, which appears to fly in the face of one of the more poignant proposals of the Fraud Trials Committee, in which it is thus embodied; ²

'In many instances the reforms we propose, could easily be argued to be of benefit to a wider range of criminal cases.'

1. At page 77.

2. Ibid. Fraud Trials Committee Report, (1986a at p.2).

4.2. PRESENTING COMPLEX INFORMATION TO JURIES

Despite the fact that the law of evidence is not one of the oldest segments of English law since it was largely a response to the distinction of the roles of witnesses and jurors after the period of restoration, Tapper (1988 at p.5) observes, that its foundations nevertheless predate the decline of jury trial in civil actions in the nineteenth century. Furthermore, they also predate the expansion of educational attainment in the last one hundred years. In the opinion of the same commentator (ibid p.5) it was this concentration upon the deliberation of relatively uneducated jurors that led to the stress upon the value of an essentially oral procedure. It was against this background, that witnesses were brought forward to tell what they had seen and heard, so that jurors could then see them exposed to cross-examination. Documents were accepted only grudgingly, and were always regarded as inferior to the recollection of human beings.

Due to society's increased reliance on paper records and less regard for human recollections arising from the expansion of business methods, there has been a change of emphasis regarding the value of documentary evidence. As noted by Tapper (ibid. p.5) this has culminated in the process of divorce between human beings and business records which has generated much of the difficulty in the modern law of evidence in commercial cases.¹ Although society has witnessed considerable recent and radical legislative reform,² the problems associated with developing the skills that are necessary for presenting

1. See also Fraud Trials Committee Report, (1986a at para 5.5.).

2. In the general provisions of both the Criminal Justice Act 1987 and the Criminal Justice Act 1988.

complex information to juries in difficult cases will continue to be a problem for some time to come, as will the uncertainty of whether or not jurors themselves are capable of adequately assimilating the information so presented. In short, it is one thing to provide legislation to implement these methods, but quite another to develop human expertise and understanding by which to operate these new concepts.

It was the belief of the Fraud Trials Committee¹ that many jurors appear to have serious difficulties in assimilating the evidence that was presented to them which, in view of the fact that such evidence often relates to a world wholly outside the experience of laymen, was not an altogether surprising assumption. This situation led the same commentators to draw the conclusion (ibid para. 8.35) that 'many jurors are out of their depth'. Whilst this view is contested by others² who have conducted research into jury trials in America, it could well be that the true value of the jury system lies not in the individual weaknesses of the twelve members which it comprises, but their collective and impressive ability to combine their memories and perspectives, as is suggested by Professors Hastie, Penrod and Pennington.³

The impact of evidence on juries, when it is well supported by charts, photographs and similar techniques prepared by means of modern technology, particularly when produced by such experts as questioned document examiners, can be a daunting prospect to opponents in criminal trials. The disquiet that is often felt by defence counsel

-
1. Ibid. 1986a at para. 8.35.
 2. For an insight into some opposing views, see generally the observations of Myers for example, as observed by Hans and Vidmar (1986 at p. 120).
 3. Ibid. Inside the Jury, (1983). As observed by Hans and Vidmar (1986 at p.120).

in such instances, is expressed by Du Cann. R., (1964 at p.162). However, jury behaviour is complex and the ability to study it is limited, due to the restrictions imposed by the Contempt of Court Act 1981. Attempts by psychologists to research jury behaviour during their deliberations, have been largely unsuccessful. Lloyd-Bostock (1981 at p.1) notes the observations of Greer, in concluding that psychologists tend to work in isolation from others, fail to grasp the important point that 'the truth' is not the only objective of the criminal trial, and that many psychologists therefore tend to oversell the legal implications of their work, and expected their findings to be regarded as virtual saviours of the integrity of the legal system.

In terms of information technology as presentational aids, Hawkins. M.J., ed. (1987) notes that the word 'visual' in relation to its modern meaning, encompasses not only the sense of sight but has also been expanded to become linked to those technologies which have an impact on the use of sight, such as 'visual aid' and 'visual display unit'. The complexities of the human visual system which are regarded by some psychologists as an 'information processor', are seen by such people as Spoehr and Lehmkuhle (1982 at p.ix) as 'the cause of frequent disputes' arising from the origins of various visual phenomena.

In the context of visuality and colour as a combined entity, Varley H., ed. (1980 at p.44) notes that colours can influence mood and feeling, although the same commentator concedes that the psychological basis for this belief is little understood. The relevant views on this matter by Varley (ibid. p.44) may be summarised by saying that the effect of colour on human moods is dependant on lights of different colours entering the eye, which may indirectly affect the hypothalamus and, in turn, the

pituitary gland. This 'master' gland controls the entire endocrine system, including the thyroid and sex glands, and so controls the hormone levels of this system and the moods consequent upon it.

In noting an experiment which was carried out by Goldstein, it is the conclusion of Varley (ibid. p.44) that colour illumination in red light, produces the effect of over-estimating time, and made objects seem larger and heavier, whilst experiments using green or blue light produced results which suggested that time was underestimated, and that objects seemed shorter, smaller and lighter. Thus, in cases where colour is used as a medium for enhancing the presentation of evidence to juries,¹ propriety in the appropriate choice of colours would appear to have ethical connotations.

One of the main areas of concern expressed by the Fraud Trials Committee was whether or not lay juries are capable of achieving a proper understanding of the evidence in complex fraud trials, this culminated in limited research being carried out to obtain an analysis comparing alternative ways of such presentational techniques, by the Applied Psychology Unit of the Medical Research Council at Cambridge.² The four projects contained in the ensuing report and which were later published, considered the effects of glossaries, the presentation of numerical information, the problems of concentration, and the effects of summaries in improving comprehension.

Although the results of the research cannot be conclusive, since individual volunteers were tested and not actual jury members, and in any case they were not required to

1. Such as in computer graphics.

2. Fraud Trials Committee Report, (1986b at p. iii).

participate in any any form of group decision making, the research findings nevertheless help us to assess some of the difficulties that laymen experience in understanding and retaining unfamiliar and complex information. These as Lord Roskill noted,¹ 'provide support for the view that the traditional methods of presenting evidence in court can be significantly improved in several ways'. The findings of the research team were influential in the subsequent recommendations which were made by the Fraud Trials Committee, and appeared as a separate document, published simultaneously with that of the Fraud Trials Committee Report.

The observations so far discussed, assume that the information presented to the court will have been prepared in accordance with the rules of propriety. There is always the danger however, that information may be wrongly interpreted prior to input into computer systems or other technological devices, and that the result as expressed in the acronym GIGO (Garbage In Garbage Out) will ensue. Thus, caution must always be exercised when assessing the output of modern information technology systems to ensure that the sort of misuses of computer statistics and other graphical sins, as considered by researchers such as Jaffe and Spierer (1987), are avoided.

1. Fraud Trials Committee Report, (1986b at p.iii).

4.3.

COURTROOM TECHNOLOGY.

In England and Wales, advances in technology are helping the courts to become automated, particularly in areas of administrative support.¹ In terms of the Crown Court system, Potter R. (1988 at p. 15) observes that by the end of the year 1991, a multi-user system will have been installed to provide the modern office support for all of the Crown Courts in England and Wales, thus reducing the need for staff increases.

On the operational side of the coin, there is also an increasing awareness of the value of information technology as a medium for presenting complex information, in addition to other factors. This is evident from a number of recent events that have been held to promote the concept to representatives from various agencies. This part of the chapter alludes to relevant areas of discourse raised during two recent conferences.

The first of these conferences was held in the appropriate environment of the 'Mock Crown Court' at Hendon Police College, and consisted of a series of one-day seminars, during the period 7-9th March, 1988.² The conference which was jointly sponsored by ITAC (Information Technology And the Courts),³ the Metropolitan and City Police Company

-
1. See for example, Computersation of Court Procedures in Debt Cases, The Claims Registry (1987). Home Office. Hederman. C., undated research monograph. Data Exchange between Magistrates' Courts and Other Agencies. Home Office Research and Planning Group. Potter R., Information Technology and the Court Service, Computers and Law 56. June 1988 at p.14. See also, this Thesis bibliography.
 2. For another review of this conference, see Overend. S., Presentation of Evidence in the Courtroom - How IT Can Help. 56 Computers and Law. At p.12.
 3. A sub-committee of the Society for Computers and Law.

Figure 3.

Technology in court.



Reproduced by kind permission of the Faculty of Law
at The Queen's University of Belfast.

Fraud Department and the Serious Fraud Office, was an unusual event in many ways. Especially as the delegates represented a wide range of callings from Law Lords, lawyers, law enforcement officers and others with kindred interests. The conference featured speakers who had gained recent experience during trials which had witnessed the use of information technology. One such speaker, a detective inspector in charge of the case of R. v. Adelaja and others¹, described the practical advantages of using a computer workstation in the courtroom, as the medium for document retrieval.² The device used in this particular instance was a workstation installed by Channel Communication Services Ltd. The police officers who were responsible for operating the device during the trial, had also to image the original documents onto an optical storage device known as a WORM (Write Once but Read Many times). Such has been the impact of technology on the traditional role of the police exhibits officer, that his job title has now been expanded to include the prefix 'electronic' to mark the additional expertise that he is required to achieve.

During the same conference, vendors displayed and demonstrated devices with graphic packages, electronic document packages and remote conferencing video, the overall value of which is described by Overend. S., (1988a at pp.12-13) and whose observations may be summarised, regarding the success of this type of conference, as whetting the appetites for further discussion on the need

1. Ibid. (1988), unreported.

2. The advantages that are associated with this type of technology relate to the vast amount of information that can quickly and readily be stored on one drive - 200,000 A4 pages on one 5¼" disk, 300,000 pages on a 12½" drive.

for even-handed provision of modern devices as between prosecutor and defence alike, and for the provision of rules of procedure and evidence

The next conference to be considered in this section, is 'The National Conference on Court Technology, held in Denver, Colorado, 24-27 April, 1988'. Overend. S., (1988b at p.20) who reports on the range of technologies discussed, describes how the use of advanced equipment enables urine testing to be carried out on offenders relative to the conditions of their bail, and how these methods of monitoring 'drug in body' defendants influenced a reduction in their rate of re-offending and absconding to levels equivalent to 'non-drug' defendants.¹

Computer aided transcription devices are described by Overend (ibid. p.20) as being capable of producing almost instantaneous hard copies but with the added advantages, brought about by technology, that enable computer word searching facilities in machine readable form. In the Kentucky courts, proceedings are now being recorded by voice-activated 'pan and zoom' video cameras with playback facilities, copies of which are immediately available to courts of appeal in appropriate cases.

1. As noted by Overend. S., (ibid. 1988b at p.21) experiments in the District of Columbia have shown that three out of four persons arrested have been found to have drugs in their body; further, that persons taking drugs are far more likely to commit further offences while on bail, or to abscond. Judges in D.C. now impose conditions of bail that a defendant does not use drugs and that urine samples are submitted once a week, while on bail. If the test is missed or proves negative, a bail offence will be committed. Implementation of this policy (which depends entirely on advanced technology for carrying out the urine samples speedily), has caused the rate of re-offending and absconding of bailed 'drug-in-body' defendants, to fall to that of 'non-drug' defendants.

Technology in the American courts is also used for the arraignment of defendants¹ and judicial training, as noted by Overend (ibid. 1988b at p.23). The latter includes the technique of interactive video which involves playback of pre-recorded video sequences of simulated courtroom proceedings, each of which concludes with an objection by an attorney upon which the judge must reach a decision based on the information that is available to him. Thus technology, in this context, ensures a realistic form of training by improving upon 'paper-feed' exercises.

Based on the reforms to legislation which have now culminated in the enactment of sections 31 and 32 of the Criminal Justice Act 1988, coupled with the developments being made in the American and Canadian² courts, it would appear inevitable, that in future trials in the English courts there will be a substantial increase in the use of computerised devices and video-recording systems, both in the physical presentation of evidence in the courtroom as well as the live transmission of witnesses's evidence via remote video links.

-
1. Overend. S., (ibid. 1988b at p.23) notes that the California Penal Code S.977.2, allows for the initial arraignment in municipal or superior courts of defendants held in any state, county, or local penal facility within the county on felony charges (with certain exceptions), to be conducted by two-way electronic audio-video communication, between the defendant and the courtroom, in lieu of the physical appearance of the defendant in the courtroom.
 2. As outlined in the Conference Notes on Technology in the Canadian courts, (under item 1.22) of the 4th International Congress Sul Tema in Rome, held between 16-21 March 1988, delegates were informed, that: since 1985, the Supreme Court of Canada has been using a nationwide video service to hear leave to appeal and other applications before the court, whereby lawyers and their clients are spared time and the expense of travelling great distances to court on motions which are most often very short in duration.

Despite the recent use of computers to assist in the electronic retrieval of documents in English courts,¹ and the fact that television cameras have acquired access to courts in 43 of the 50 states in America for over 30 years,² not all technology used in the presentation of evidence in complex fraud trials need be as sophisticated as these methods. As noted by Baldwin. D.,³ the use of overhead projector and screen to present fraud evidence, has the advantage of being both cheap and mechanically simple to operate. It is also possible to merge some of the older technologies to blend with the new, an example of which is now discussed.

The case of R. v. Gardner and others,⁴ proved to be a testing ground for a miscellany of technologies. In this instance, computer graphics and spreadsheets had been electronically prepared with the aid of a computer, to show the extent of certain contracts for buildings works which had been allocated by a member of a government department to a contractor, the background of which transaction it is alleged, was set against a combination of both fraudulent and corrupt activities. This case was also used as the experimental platform from which to 'dry

-
1. As for example, in the case of R. v. Adelaja and others, (1988), unreported, which resulted in a trial lasting 6 months and cost 4 million pounds, but no convictions were forthcoming. This case was the subject of criticism by the trial judge, who observed that the use of technology had made document viewing so readily available, that the amount of documents had overwhelmed the jury. This case had also become known as the 'jinx trial', due to the deaths of 6 people involved in it. Source, Daily Telegraph dated 19th May, 1988.
 2. As reported in the magazine Lawyer, vol.2., iss.9., dated 5th May, 1988, at p.14.
 3. Ibid. Fraud in a Good Light, Police Review dated 9th August, 1985, at p.1622.
 4. [1987] Central Criminal Court, unreported.

Figure 4.

Spreadsheet illustration.

SMALL NUMBER	PROJECT/ITEM OFFICER	LOCATION	L.B.H. ORDER NO.	DATE OF ORDER	SUPPLY OF WORKS ORDERED BY ORDER	DATE OF ORDER	SUPPLY OF WORKS ORDERED BY INVOICE	AMOUNT CHARGED	ITEMS VALUATION	PERCENTAGE ABOVE VALUATION	L.B.H. ORDER EXH NO (E) / PAGE NO (P)	MAINTENANCE INSPECTION FORM EXH NO (E) / PAGE NO (P)	COAKLES INVOICE EXH NO (E) / PAGE NO (P)	INVOICE CERT. SLIP EXH NO (E) / PAGE NO (P)	PHOTOCOPY PLAN EXH NO (E) / PAGE NO (P)
1	SMITH	LITTLE STANFORD 1ST & MIDDLE SCHOOL	A21024	01/02/1984	See Official Order	01/05/1984	See Official Order		91.32%		E33/P/28	E21/P/25-24	E22/P/25	E22/P/25	E24/P/27
2	JONES	LITTLE STANFORD MIDDLE SCHOOL	A25701	20/03/1984	See Official Order	03/05/1984	See Official Invoice		44.08%		E25/P/23	E27/P/30-31	E26/P/29	E26/P/29	E28/P/32
3	DAVIS	LITTLE STANFORD 1ST & MIDDLE SCHOOL	A22130	20/04/1984	See Official Order	30/06/1984	See Official Invoice		115.31%		E29/P/15	E31/P/35-36	E30/P/34	E30/P/34	E32/P/33
4	DAVIS	LITTLE STANFORD 1ST & MIDDLE SCHOOL	A28681	09/04/1984	See Official Order	11/03/1984	See Official Invoice		132.90%		E32/P/30	E35/P/40-41	E34/P/33	E34/P/33	E36/P/42
5	SMITH	LITTLE STANFORD 1ST & MIDDLE SCHOOL	A25921	19/06/1984	See Official Order	30/06/1984	See Official Invoice		94.80%		E37/P/43	E39/P/45-47	E38/P/44	E38/P/44	E40/P/46-9
6		NOT USED													
7		NOT USED													
8		NOT USED													
9		NOT USED													
10	SMITH	MORRISBY 1ST & MIDDLE SCHOOL	A11601	23/05/1984	Staff units - remove back panels, disconnect pins and clear restrictions - reassemble smaller units.	30/06/1984	To take down panels, disconnect and clear restrictions to maintain files, reassemble smaller units.		289.58%		E64/P/19	E66/P/181-183	E65/P/180	E65/P/180	E67-92/P/64-6
11	SMITH	MORRISBY 1ST & MIDDLE SCHOOL	A28651	04/04/1984	External divalves - clear one ladder and rails shipped & install in place. Create bill for son.	30/06/1984	To raise one ladder and rails shipped and install hanging files. Complete bill screen.		451.20%		E70/P/187	E89/P/189-191	E71/P/188	E71/P/188	E73-82/P/92-3
12		NOT USED													
13		NOT USED													
14		NOT USED													
15		NOT USED													
16		NOT USED													

P. SMITH & JONES

run' the preparatory hearing procedure. Although the defendant Gardner pleaded guilty to a number of the counts referring to him on the indictment, there were still a number of matters which remained contested by the three defendants that were left. The result being, that the jury copies of the indictments had to be amended almost immediately to ensure that only relevant issues were placed before them. During the ensuing trial, the indictments became the subject of constant amendment as counts were either discarded by the prosecution or otherwise became invalid. In the traditional style of fraud trial where schedules might have been used instead of spreadsheets, it would have been a major task to reconstruct something as complicated as these manually prepared documents during the progress of the trial. In the event, however, the original spreadsheet containing the indictment information, having been quite easily updated on the computer, was soon capable of being xerographically reproduced and with the availability of sufficient copies to enable circulation to all parties in the case, with the minimum of effort.

Copies of the spreadsheet information and graphs, were also used during this trial, and were available as transparencies. The transparencies were produced by placing sheets of acetate in the feed tray of a photocopying machine and operating the 'on' key of the device in the same manner as for normal hard copies. These were then capable of being displayed through the lens of an overhead projector onto a screen in the court

Thus, in the process so far described, we can see that spreadsheets which were initially produced by computerised devices, were printed out and then made into original documents. Copies of the original documents were then obtainable, either as hard copies for distribution to all

individual parties, having been xerographically reproduced, or as transparencies which had passed through a similar electronic process. The final stage in the production line was to adopt the older form of technology for use as overhead projector and screen, through which the transparencies could be displayed onto a screen for courtroom viewing.

The potential value of alternative forms of technology, such as pre-recorded video-films in fraud trials, has already been noted above.¹ There is however, the labour intensiveness of these methods to take into account, as well as the demand on police resources to install the television monitor and ancillary equipment into the courtroom,² by which means the film may be viewed.

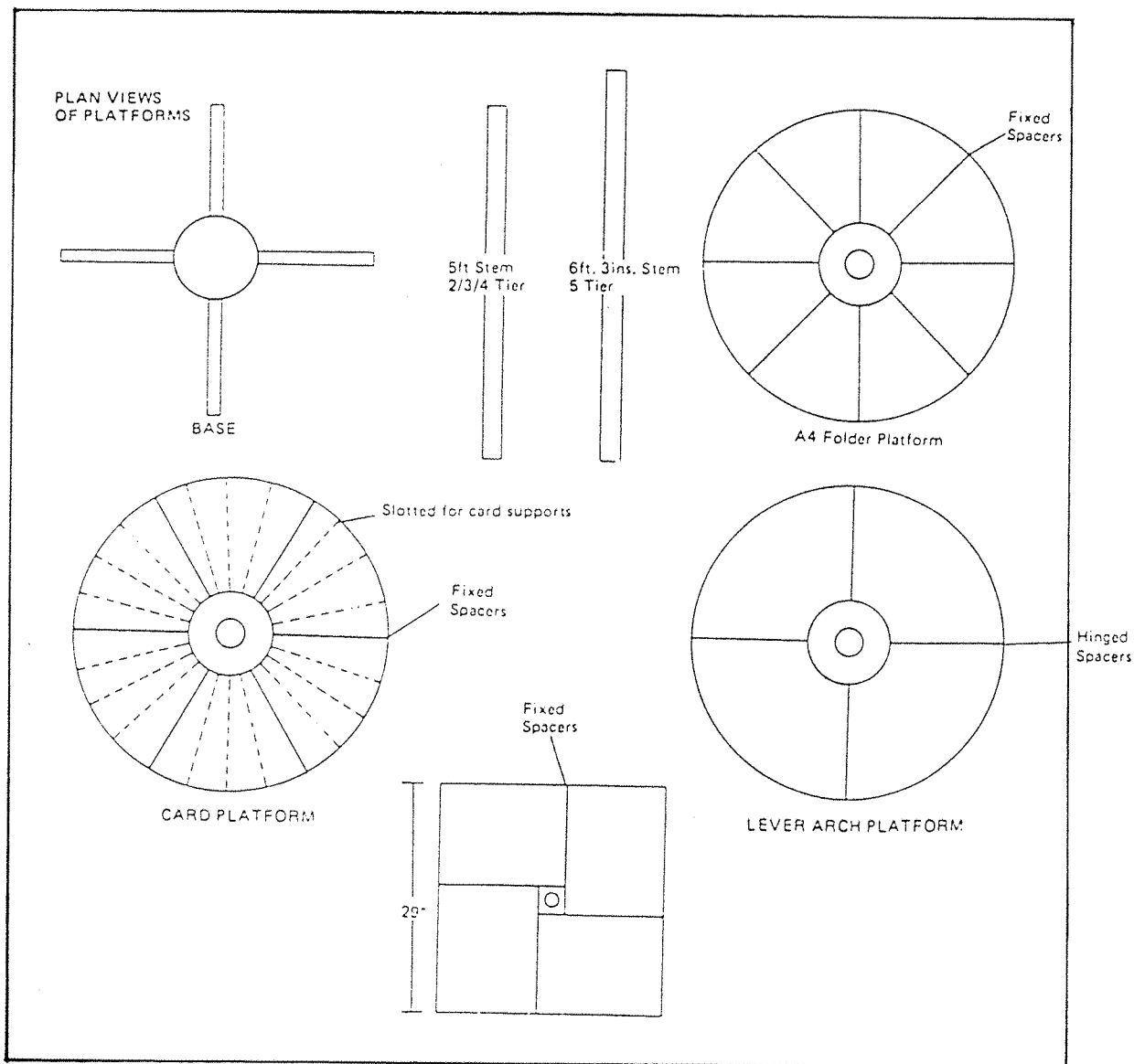
Non-electronic forms of document retrieval systems have also been available for many years and, although designed mainly for office use, have easily been adapted for the case management of voluminous documentary exhibits. An example of how such a system could be implemented, is adopted from the procedure used in the Gardner trial (see Figure 5) where A4 size documentary exhibits were slotted into polythene sleeves, these in turn being inserted in order of sequence into lever arch files, the covers of which were marked with details of their contents to provide a 'tell-at-a-glance' inventory of the documents in use. Finally, the lever arch files were placed onto circular metal shelves which rotated on a pivot, which could be turned by the exhibits officer until the pertinent exhibit could be found, and then retrieved.

1. At p. 75.

2. Despite the fact that the Lord Chancellor's Department manage the administration of Crown Courts, the installation of information technology into the courts, has tended to fall outside their area of accepted responsibility.

Figure 5.

Diagram of non-electronic document retrieval system.

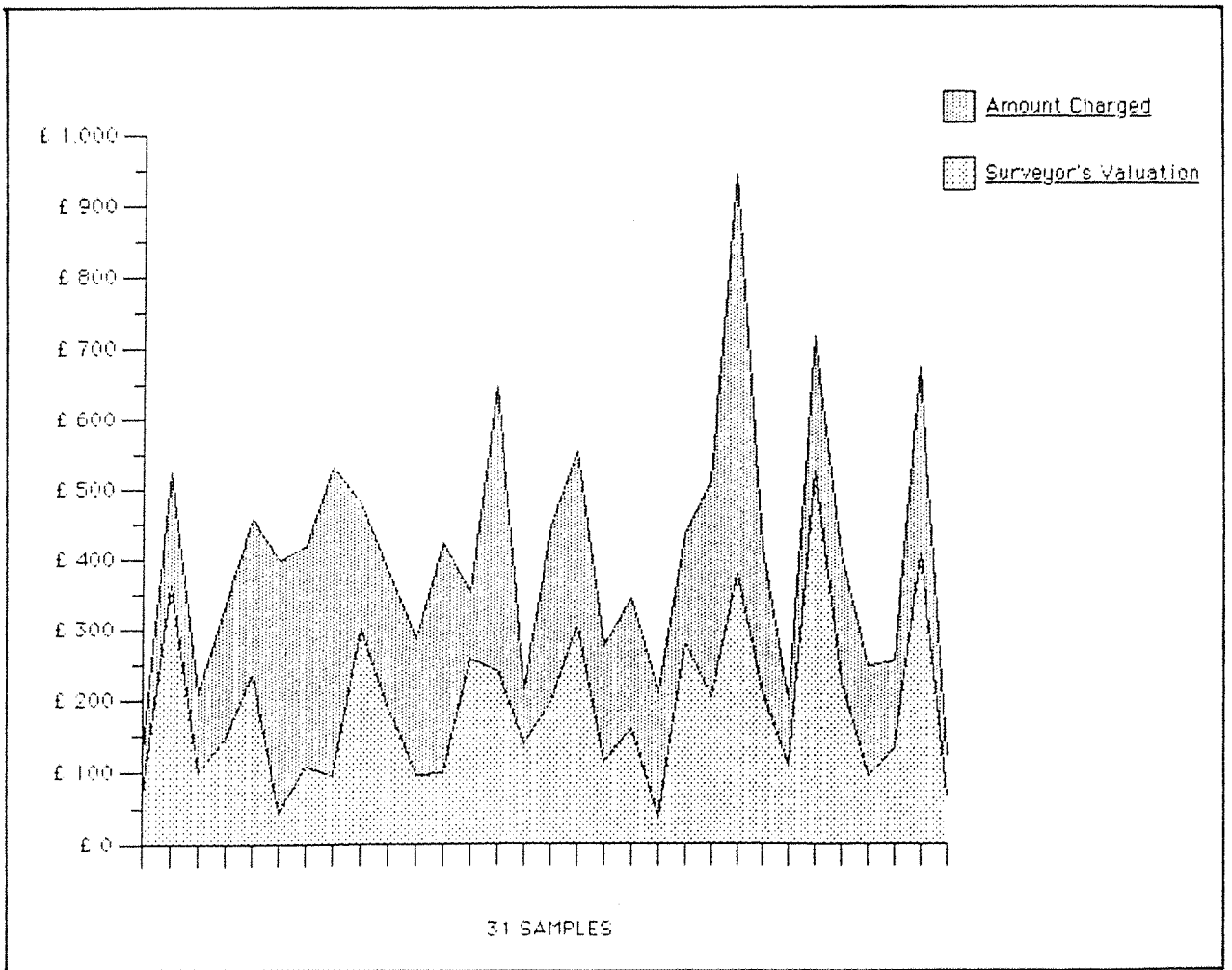


In the case of R. v. Relton,¹ the police officer involved in the preparation of the prosecution case, operated a sophisticated device to present computer graphics to the court. This method was used to overcome some of the difficulties involved in presenting complex information to the trial jury, whereby the computer-produced data was relayed onto television monitors situated around the court. This case provides another sensible example of new technology and older techniques of presentation blending together. To illustrate this point, the bundles of exhibits that were made available to the court and to the individual members of the jury, were inserted into files, each of which had a different coloured cover. The advantage of this method ensured, that when counsel wanted to draw the attention of the jury to a particular bundle of papers, he simply needed to call out the colour of the file to which he was referring, in order to focus everyone's interest in that direction. Thankfully, none of the jurors in this particular case appeared to suffer from colour-blindness, which is an aspect that will undoubtedly be encountered at some future date.

1. [1988], unreported. This case which appeared at the Central Criminal Court, is also known as the 'Brinks Mat' case. For a review of this procedure, see HOLLIDAY. A.H., Computers in the Court - How Computer Graphics were used to present evidence at the Old Bailey, Computers and Law. 57 Sept, 1988. At p.19.

Figure 6.

Example of computer graphics used in fraud trial.



4.5.

TELEVISED EVIDENCE.

The Criminal Justice Act 1988, now paves the way for evidence to be heard from a person (other than the accused), via the medium of live television links, subject to the leave of the court.¹

This legislation has compensated for the concern expressed in the Fraud Trials Committee Report (1986a at p.76) regarding the risk of perjury from a witness giving evidence from abroad, by extending the provisions of section 1 of the Perjury Act 1911, to include instances of perjury committed by witnesses giving their evidence via this medium.² Nevertheless, it is difficult to envisage the practical application of this legislation, in terms of extraditing offenders from jurisdictions outside of this country, to face justice in the UK courts when instances of perjury are discovered, due to considerations of cost, and the legal effort that would be encountered in implementing the relevant extradition requests.³ However, to adopt the argument of the Roskill Committee,⁴ a witness who attended court in person, gave perjured evidence and returned to his country of origin before being found out, would be equally safe from legal retribution.

Section 32 of the Criminal Justice Act 1988 covers two main categories of witness. The first group under sub-section 32 (a) of the Act are assumed to be the adults who, for whatever reason, are prevented from being physically present at the court to give their testimony 'in personam'. The second category under sub-section 32

1. Section 32.

2. Sub-section 32 (3) of the Criminal Justice Act 1988.

3. Under the Extradition Act 1870 or Fugitive Offenders Act 1967.

4. Fraud Trials Committee Report, (1986a at p.76).

(b), are witnesses under the age of 14 years, the qualification for which testimony when given in this way, being, that the offence charged is one relating to some kind of child abuse, as stipulated under sub-section 32 (2) of the Act. The cost considerations of bringing the televised evidence of the two categories of witness, also involve different criteria. The first group who will communicate their evidence via the medium of communication satellites, are dependant on the degree of free air space available. As observed by Zorkoczy, (1982 at p.55) the cost involved in the use of Intelsat 5 satellites and the ground station equipment required to operate them, is expensive, and the quality of transmission is not always satisfactory. Child witnesses on the other hand, will state their evidence live through the medium of closed-circuit television systems which are situated within the confines of the court. The intention of the latter scheme being, to spare children the particular trauma of being confronted by their tormentors.

Subject to certain conditions,¹ section 33 of the Criminal Justice Act 1988, now expands the powers of magistrates by amending the provisions of sub-section 103 (1) (b) of the Magistrates' Courts Act 1980, in relation to the giving of evidence of persons under 14 in committal proceedings for assault, sexual offences etc. The effect of this amendment, is to admit 'any statement made by or taken from a child of which his oral evidence would be admissible'. The phraseology of this section appears to be wide enough to extend to statements made by child witnesses in video-taped interviews. If this is the case,

1. As detailed under sub-section 103 (3) of the Magistrates' Courts Act 1980, as amended by Section 33 of the Criminal Justice Act 1988.

then it is difficult to see how such records of interviews would not also be admissible during the subsequent trials on indictment, to which they relate.

The media has focussed some of its attention on the televising of child witnesses' evidence¹ and there has been much discourse on this subject in general.² Spencer (ibid. p.445) draws attention to the concern felt by some, over the 'loss of immediacy' that televised can introduce. The same commentator (ibid p. 446) does however, balance this view by rightly arguing, 'that far from being an objection, this seems to be a highly desirable consequence', bearing in mind the welfare of the victim. In terms of televised evidence in cases of complex frauds and other crime, it is evident that juries are attracted to information which is presented to them through television monitors, for reasons which include those given by Holliday A.H.,³ when quoting Tantum. M, who observed the frequency and interest with which jurors attention were focussed on the television monitors.

Although cost implications will inhibit the wide-spread use of satellite links to transmit the evidence of witnesses from abroad in the short term, developments in communications resulting in more economic benefits, are

-
1. As for example, the BBC Panorama program, Sept 8, 1986, in which Carman. G., QC, stated, 'It is important the jury be able to observe the demeanour of the child. It is important the defendant is able to give immediate instruction to his counsel as and when the child is giving evidence. And it is equally important that he, himself, is confronted with the child and unhappily, the child is confronted with him.'
 2. See for example, Spencer. J.R., Child Witnesses and Video-Technology - Thoughts for the Home Office. 51 Journal of Criminal Law (pt.4), Nov. 1987.
 3. Ibid. Computers in the Court. How Computer Graphics were used to Present Evidence at the Old Bailey. Computers and Law. No. 57. Sept. 1988, at p.19.

likely to bear witness to an expansion in the use of such equipment in the future. In the case of child witnesses however, there appears to be no legal, financial or technologically based reasons to prevent the immediate and widespread use of televised evidence in our courts.

B. Conclusions.

The effect of technology and its influence in bringing about reforms to the laws of evidence; has been amply illustrated by the recent enactment of the Criminal Justice Acts 1987/1988. Faced with such positive statutory reform, few people can surely doubt the determination of parliament to increase the presence of technology in the courts. Although experiments have, and are continuing to be conducted into the use of these media, they are too novel to have received the attention of the appeal courts, whereby dissent to the use of such methods might be raised as an issue. Nevertheless, it is the experience of some American courts, that technology is helping to reduce incidence of reoffending¹ and where such claims are found to be valid, must be hailed as positive measures towards increasing the quality of justice in society.

Those who participated in the membership of the Fraud Trials Committee can be justifiably pleased with the outcome of the recommendations in their Report, which have now received the seal of legislative approval and support. The experiments discussed in this chapter have been conducted in London courts. However, in order to test the wider application of technological advances by fraud squads in England and Wales, it is necessary to turn to the fifth and final chapter of this thesis.

1. See for example, the comments expressed on page 6 (footnote 1) above, on this issue.

CHAPTER FIVE

RESEARCH RESULTS AND CONCLUSIONS.

A. Introduction.

The methodology used to test individual responses from fraud squads in England and Wales, in relation to the relevant recommendations of the Fraud Trials Committee in their Report (1986a at pp. 179-189), was to conduct a survey by means of prepared questionnaires.¹ These questionnaires were despatched through the postal service with stamped addressed envelopes enclosed, to each of the forty-three Home Office police forces in England and Wales,² and to the Ministry of Defence Police fraud squad.³

There was a high rate of response in that 81.39% (or 35) of the Home Office fraud squads returned completed questionnaires. However, of the eight fraud squads that did not complete questionnaires, only one of these. i.e. Durham, wrote to explain the difficulties which precluded their cooperation. Since no communication was received from the remaining seven fraud squads, viz, Cheshire, Derbyshire, Dorset, Leicestershire, North Yorkshire, Suffolk and West Yorkshire, it is not possible to provide a complete survey report, merely, a large sample.

-
1. A specimen of which is shown at Appendix 'A'.
 2. Please refer to Appendix 'B'.
 3. The Ministry of Defence Police fraud squad has, at its disposal, the most sophisticated technology of all fraud squads in England and Wales. However, the questionnaire results have been confined to the Home Office forces only, for the purposes of this exercise.

This chapter therefore, deals with the analysis of the questionnaire results and concludes with recommendations arising from the salient issues under the following categories.

1. Resources.
2. Developments in technology.
3. Career prospects and training.
4. Reform and initiatives.
5. Regulation of computer generated evidence.

5.1.

RESOURCES.

In order to determine whether or not police resources had been improved since the Fraud Trials Committee made their Report,¹ fraud squad representatives were asked, 'Has there been any variation in the establishment of your police staff since the Roskill Report was published on 10th January, 1986'? Fraud squads representatives who felt that there had been no variation at all to their manning levels, accounted for 60% (or 21) of those responding to this question.

Eight of the remaining replies (i.e. 22.85%) were from people who said that there had been increases to their establishment, although details of the existing levels submitted by two of these respondents, equated with those previously published in the 1986 Fraud Trials Committee Report² and, as such, could not be regarded as valid for the purposes of this exercise. Another of the fraud squads reporting an increase, said they had been given a further 13 officers. However a close scrutiny of the data supplied, revealed that only one of these could be regarded as an increase to the establishment of the fraud squad per se, in accordance with the definition existing in 1986, since the remainder were employed either on cheque fraud duties or as drugs profit confiscation officers.

1. Ibid. (1986a). In para. 2.71, the Committee express concern at the inadequacy of resources devoted to coping with the volume of work involved in the investigation of fraud.

2. Ibid. (1986a) at pp. 231-232.



Table 2 below, reflects the actual variation levels, in respect of those six fraud squads which had reported valid increases to their establishments.

Table 2.

	1985 est.	Current level.	Reported increase.	% inc in manning.
	2	3	1	50%
	19	21	2	10.5%
	12	16	4	33.33%
	16	17	1	6.25%
	3	7	4	133.33%
	2	4	2	100%
Total	54	68	14	

Relevant to decreases in establishments, five fraud squads (i.e. 14.29%) reported an actual decline, although one of these could not be calculated as a decline to establishment for the purposes of this exercise, since the present levels that were supplied, equated with the 1986 figures in the Roskill Report. As will be seen from Table 3 below, the valid decreases in manpower reported by the four fraud squads that were affected, match exactly, the increases that are reflected in Table 2 above. Thus, this research indicates that there have been no overall increases to fraud squad establishments, nationally.

Table 3.

	1985 est.	Current level.	Reported decrease.	% dec. in manpower.
	5	4	1	20%
	12	10	2	16.6%
	147	138	9	6.12%
	11	9	2	18.18%
Total	175	161	14	

A question aimed at assessing the extent of variations to civil staff support, could not properly be quantified owing to the imprecise nature of the data given in the completed questionnaires, vis-a-vis the comparative position between the figures which applied during 1985,

and those which were relevant now. Based on the information supplied, a national increase occurred involving 9 additional civil staff to fraud squad duties in the purist sense,¹ although it was not possible to say how this figure was affected by reported decreases.²

The extent to which computerisation has developed on fraud squads, has already been noted above.³ A breakdown of how the 48.57% (i.e. 17) fraud squads who reported now having their own computer systems, is given in Table 4 below.

Table 4.

Proportion of fraud squads.	Number of computers each.
12	1 (=12)
2	2 (= 4)
2	3 (= 6)
1	6 (= 6)
Total 17	11 (= 30)

It should be noted however, that the relevant questions⁴ had not been worded in a way which sought to ascertain the precise nature of the computers systems that were available to these fraud squads, e.g. word-processors, microcomputers, mini-computers, etc. As such, this data paints only a general picture.

-
1. An allowance was made to ensure that only those employed on fraud squad duties qualified for this purpose. Again, this did not include cheque frauds or drugs profit confiscation duties.
 2. For example, the Metropolitan Police fraud squad reported a decrease in their civil staff establishment, in addition to their police staff. Although no figures were given in respect of the civil staff decreases, a reported decrease in their police staff indicated a reduction of 9 officers. If similar reductions had been made to civil staff, this would again, exactly match, and thus negate, the increases in civil staff employed on fraud squads which had been reported nationally.
 3. At page 3.
 4. Viz; Question Nos. 3-5.

One question¹ attempted to particularise the extent to which computers were available in relation to 'sole use only equipment' and 'shared systems'. This culminated in a surprising reply from one fraud squad in Wales, which reported satisfaction with the availability of their computer support. Reference to other data on the completed questionnaire revealed that the respondent shared the use of equipment owned by the Fraud and Bankruptcy Division of the Crown Prosecution Service, which is in London. Despite the fact that this is an extreme example, the mere fact that any individual would be required to travel from one country to another in order to access computer support, could hardly qualify the degree of availability as immediate.

A summary of the other issues relating to computer development may be made in this way; fraud squads appear to be pioneering the development of technology in isolation and in an uncoordinated and piecemeal fashion.² Financial constraints had contributed to 28.13% (i.e. 9) of the fraud squads being 'badly in need of computers', whilst 34.77% of those responding, who already had a computer system, needed better equipment.³ Almost one-third of the fraud squads who reported having their own computer systems, were dissatisfied with the level of computer operator training that was available to them.

In terms of facsimile equipment, there is evidence of an increase in its availability to fraud squads, as noted above.⁴ The Drugs Trafficking Offences Act 1986, has

1. Please refer to question No. 1, for further details.

2. Question No. 4.

3. Question No. 5.

4. Please refer to Table 1, at p. 14.

contributed to an increase in the work of officers according to the opinion of 53.12% (i.e. 17) of those who responded to this question.

On the issue of resource sharing between fraud squads, respondents were almost unanimous in saying that they frequently gave and received help to and from other fraud squads whenever it was necessary. They also said that reimbursement was either not usually required in cases where help was received and, when help was given, requests for reimbursement were usually avoided. There was only one respondent who stated that help was mostly refused in response to requests from other fraud squads and vice versa; although, even in this isolated example, the question of reimbursement was not an issue. Despite the fact that no details were sought regarding the particular occasions when help was either given or requested, this surprising aspect of the research tends to support the theory that inter-fraud squad cooperation in the sharing of resources, is either (a) no longer a problem area, (b) that respondents to the questionnaire were unwilling to appear uncooperative, or (c) that the position had been misinterpreted by, or misstated to, the Fraud Trials Committee, in the first place.¹

1. Ibid. (1986a at para. 2.71).

5.2.

DEVELOPMENTS IN TECHNOLOGY

This section of the questionnaire relating to developments in technology, began by asking respondents, 'How much importance is attached to the use of computer graphics (i.e, bar charts, etc), by your fraud squad for the presentation of statistical information, and how frequently are they used'? By analysing the replies, it was found that 50% (i.e. 16) of those responding reported that a great deal of importance was attached to the use of computer graphics, and that 25% (i.e. 8) felt that some importance was attached to their use. The remaining 25% felt that very little importance was attached to these methods. However, when other data relating to the dissenters was examined, it was found that over 62.5% (i.e. 5) of these fraud squads had previously said they had no computer of their own. Under those circumstances, the lack of opportunity to experiment with the techniques of producing computer graphics would clearly be a relevant issue. The remaining 37.5% (i.e. 3) of those who said they saw very little value in the use of computer graphics had previously indicated their fraud squads had their own computer. Nevertheless, there was a total of 75% of people who answered this question who felt that the use of computer graphics either had a great deal of value, or value of some kind.

A similar question was put in relation to the use of spreadsheets, and over 90% (i.e. 30) of the respondents reported that they felt there was a great deal of importance attached to their use (i.e.60.60%) or that some importance was attached (i.e. 30.30%). The remaining 9.09% (i.e. 5) felt very little importance was attached to their use. Strangely, one of those from the group of dissenters, represented the views of a fraud squad with its own computer. Since the use of computers to prepare

spreadsheets is seen by many fraud investigators¹ as one of the prime advantages associated with the use of devices of this kind, when compared with the tedium involved in the manual preparation of schedules,² this answer appears to be paradoxical. The basis upon which this dissent is laid is mystifying, unless the term spreadsheet was unfamiliar to respondent, in which case the blame must be attributed to the use of computer jargon during the preparation of the questionnaire, in assuming that its meaning would be understood by all. Nevertheless, the percentage of those dissenting pales into insignificance against the background of of 90% or so who favoured their use, or indicated that they were important. The data, relative to the use of spreadsheets arising from this survey, is strongly weighted in favour of their usefulness.

Responses to a question dealing with the influence of the Roskill Report and any increase in the use of visual aids, resulted in replies being received from 54.54% (i.e. 18) respondents, who said that hardly any increase in their use had taken place. A further 36.36% (i.e. 12) said there had been a moderate increase, and 9% (i.e. 3) said there had been a considerable increase in the use of visual aids. However, these moderate responses are hardly surprising in the light of the novelty of these techniques to some Crown Courts.³

-
1. Over 90% based on the results of this questionnaire alone.
 2. Schedules are one of the most common methods used by fraud investigators to highlight data which is relevant to the matters under investigation. See for example, the case of R. v. Gardner and others, and associated comments at pp. 100-101, above.
 3. For example, during a telephone conversation with one respondent, it was learnt that in the North of England, some Crown Courts are somewhat reluctant to attempt these new methods in fraud trials.

The mere fact that as many as 15 of the fraud squads who were represented felt that the Roskill Report had been instrumental in influencing an increase in the use of visual aids may be argued with some justification, to amount to significant progress, given the apparent dearth in the use of such techniques, prior to 1986.

When respondents were asked the question, **'Have any significant advances been made by your fraud squad in your recent use of technology'?**, a total of 60% (i.e. 21) people said that either significant advances had been made (i.e. 31.42%) or that minor advances had been made (28%). The remaining 40% (i.e. 14) did not feel that they had advanced in any significant fashion, despite the fact that 21.42% (i.e. 3) of those answering in this way, had acquired computer support for their own (sole) use since the publication of the Roskill Report.

An analysis of the advances reported to have been made shows that they relate mainly to the provision of computer support facilities, ranging from modest word-processing equipment to sophisticated computer systems with high graphic presentation capability, database, spreadsheet and case-management facilities. A number of those who responded spoke of a commitment to their force HOLMES and one fraud squad dubiously reported that they have acquired an Anacapa computer.

An interesting reply from one respondent indicated that, although the Crown Courts in his circuit area are not yet geared for presentations using technology in fraud trials, the expertise that is being developed by his fraud squad (with appropriate equipment) was recently used to brief counsel and the investigating officers who were engaged on a complex murder investigation. This example illustrates the growing importance of information technology, not only

as the medium for presenting evidence at court, but at all stages of an investigation - and, indeed, in appropriate non-fraud related circumstances.

5.3.

CAREER PROSPECTS AND TRAINING.

A question aimed at assessing improvements in fraud squad officer's career developments, was asked of representatives in this way, 'Has any change occurred regarding the career prospects of officers on fraud squads, since the publication of the Roskill Report'?¹ All 35 respondents answered this question, of whom 68.57% (or 24) said that there had been no noticeable improvement; 17.14% (or 6) said that there had been a slight change for the better; and 8.57% (or 3) of the respondents felt that the situation had improved considerably. The remaining 2 respondents (i.e. 5.71%) actually thought the situation had become worse. The combined total of those who thought that the situation had remained unchanged or had worsened, amounted to 74.29% (or 26) of those responding. In the opposing camp, the two groups who either felt that considerable or slight change had occurred for the better, amounted to just over 25% (or 9) of the people who replied to this question.

An important police initiative which began in October, 1986, relates to specialised training of fraud squad officers at the Police Staff College, Bramshill.² A question was therefore put to respondents, which sought to identify (a) the number of their officers that attended this course, and (b) what proportion of those specially trained officers were still employed on fraud squad

1. Ibid. Fraud Trials Committee Report, (1986a at paras. 2.9 and 2.75).

2. This is a four week course is designed to familiarise officers in computer crime investigation techniques; and is held twice yearly. The decision to commence this form of training has averted the need to send officers overseas to the FBI academy in Quantico, the high cost of which, not surprisingly, restricted the number of officers that could be trained in this way.

duties. Reference to Table 5, indicates the ratio of officers sent on the Bramshill Course, vis-a-vis the ratio of fraud squads in England and Wales, judging from the information given by those who responded to this survey.

Table 5.

Proportion of specialist trained fraud squad officers.

Ratio of fraud squads.	Proportion of their officers so trained.	Men trained.
7	0	0
19	1	19
7	2	14
1	3	3
1	5	5
35	Total number of trained officers	= 41

Although the figures in Table 5 above are encouraging in terms of officers who have received specialist training on computer crime investigation techniques, sadly there is a relatively high rate of wastage amounting to 29.27% (or 12) of these skilled trained personnel, due to their transfer to non-fraud squad duties. Had these 41 skill trained officers still remained in post, this would have meant that 6.97% of the total number of fraud squad officers in England and Wales¹ had received the benefit of this form of training. Due to the wastage rate, however, this figure has been reduced to 4.93% (or 29) skill-trained officers, pro rata the national average.

A question put to respondents, to determine the availability of courses in such subjects as accountancy,

 1. In the Fraud Trials Committee Report, (ibid. 1986a at pp. 231-232), it is estimated that the combined total of fraud squad officers in England and Wales in 1985, amounted to 588 officers.

etc, provoked the response of 60% (i.e. 21) people, who reported that there had been no increase in course availability, and a response rate of 14.29% (i.e. 5) from people who felt that course availability was declining. Collectively, these figures indicate that nearly three-quarters of fraud squad representatives felt that the situation had either worsened or had remained the same. Conversely, 22.86% (or 8) felt that a few more courses were now available, whilst 2.86% (or 1) expressed the opinion that there were many more courses available.

In terms of training needs for fraud squad officers in the analysis and presentation of complex information, 65.71% (i.e. 23) of those responding said that much more could be done to remedy the situation, whilst 25.71% (or 9) thought that some of the existing courses already covered these topics; and 8.57% (or 3) said that specialists, such as accountants, provided this service on their behalf.

When asked, **'Do your officers have ready access to Anacapa trained personnel'?**, 51.43% (or 18) of the people considered that usually they had ready access to such expertise; 28.57% (or 10) felt that there was some degree of access but only subject to availability; and 20% (or 7) respondents answered that access was severely restricted. This aspect of the research indicates that 80% (or 28) fraud squad representatives were of the opinion that there was either some access (or even ready access) to Anacapa trained personnel. Although these findings leave no room for complacency, they nevertheless support the theory that such techniques are becoming more widely available in this important area of Police Science.

Relative to their use of modern techniques in recent trials, respondents were asked to indicate their preparedness to employ such methods. Only 26 people

answered this question, of which 38.46% (i.e. 10) said that such techniques were sometimes used and 3.85% (i.e. 1) considered that modern methods were regularly used. However, although 57.69% (or 15) of the people answered that the traditional methods were preferred, it was evident from some of the accompanying remarks that there should have been a further option for respondents to choose from; since the mere fact that traditional methods were in current use did not necessarily mean that they were the ones that would otherwise have been chosen, given the availability of suitable expertise and equipment.

Nevertheless, this part of the research does at least indicate that as many as 42.31% (or 11) of the fraud squads either sometimes, or regularly, use modern techniques and that there is an indication from some of the others that modern techniques would be used if the proper facilities were available.

5.4.

REFORM AND INITIATIVES.

This section of the questionnaire sought the views of fraud squad representatives apposite to recent legislative reforms¹ and initiatives originating from within the police service in general. Regarding legislation to improve the lot of investigators in their campaign against fraud, there were 31 replies to this question and 61.29% (i.e. 19) of them said that they felt the proposed reforms should be sufficient, whilst 38.70% (i.e. 12) of them felt that the reforms appeared to be inadequate. A miscellany of other issues proposed by respondents, in relation to their views, was also received in answer to this question.

In terms of further police initiatives, fraud squad representatives were asked, **'Do you see any potential benefits in holding a National Fraud Conference for fraud squad officers'?**² All 35 respondents answered this question, of whom 28.57% (i.e. 10) considered that there would be many potential benefits arising from such a conference, 48.57% (or 17) said that there would be some potential benefits, 8.57% (or 3) expressed the opinion that there would be too few potential benefits from holding such a conference, and the remaining 14.29% (or 5) considered that there were no potential benefits at all. Thus, this aspect of the research supports the view that a national fraud squad conference would have some or many potential benefits, judging from 77.14% (or 27) of the replies that people gave to this question, and that only 22.86% (or 8) expressed a contrary opinion. Topics

-
1. Particularly in relation to the Criminal Justice Act 1987 and the Criminal Justice Act 1988.
 2. It should be noted, that plans are currently being laid by the Metropolitan and City Police Company Fraud Department to arrange a National fraud squad conference at the Police Staff College, Bramshill, in 1989.

which would be suitable for discussion at a conference of this nature, were suggested by a number of those who favoured the concept.

A question which related to the feasibility of disseminating a national fraud squad bulletin, was also answered by all 35 respondents. Of these, 31.43% (or 11) felt that there would be many potential benefits, and 51.43% (or 18) said that in their view, there would be some potential benefits. Thus, those who appeared to favour the concept of a national fraud squad bulletin in principle, collectively accounted for 82.86% of those responding. The remaining 17.14% (or 6) held contrary views. A number of those responding favourably also suggested suitable topics for publication and discussion.

5.5. REGULATING COMPUTER GENERATED EVIDENCE.

A question aimed at determining the various methods used by fraud squads nationally, in relation to computer generated evidence, was put in this way, 'When submitting evidence prepared by fraud squad officers from a computer (i.e, computer graphics and spreadsheets, etc), how frequently is the 'PACE' certificate¹ completed'? There were replies from 28 of the fraud squad representatives who completed this question and 46.43% (or 13) of these said that the certificate was usually completed. A further 3.57% (or 1) said that the certificate was completed, but only infrequently. Together these replies accounted for 50% (or 14) of those who considered that the appropriate certificate was completed some of the time, and was therefore relevant in terms of authenticating computer generated evidence. By contrast, 35.71% (or 10) said that the certificate was rarely completed; and 14.29% (or 4) people said that in their opinion the certificate was not considered applicable.

This aspect of the research indicates that some fraud squads unnecessarily run the risk of defence challenge when submitting evidence which is derived from a computer, due to lack of authentication as required by the Police and Criminal Evidence Act 1984.²

A similar question was asked in relation to the monitoring of computer malfunctions. Thirty people answered the question in these ways, 23.33% (or 7) said that a special log was kept on-site, 36.67% (or 11) reported that

1. The 'PACE' certificate is that which is submitted in accordance with the Police and Criminal Evidence Act 1984, a specimen copy of which may be found by reference to the last page of Appendix 'A', of this thesis.

2. As noted at pp. 44-47, above.

someone from another department monitored their computer malfunctions, and a further 13.33% (or 4) said that no particular arrangements existed - albeit that these people had previously said they had their own computer and that it was for their sole use. The remaining 26.67% (or 8) respondents represented fraud squads without their own computers. Analysis of other information in the questionnaires of the group which answered that someone from another department monitored their malfunctions, revealed that 81.82% (or 9) of these people had previously reported having their own computer. This aspect of the research exposes another area of vulnerability, vis-a-vis unnecessary exposure to risk from defence challenge, in relation to documents which are derived from computers. Which impinges on their failure to keep on-site logs in relation to the proper operation of their computers.

In terms of a designated member of fraud squad staff with the responsibility of computer manager, there were 25 replies from people who responded to this question, of whom 28% (or 7) said that a delegated member of their staff performed this function; 64% (or 16) from respondents who said that someone from another branch had the particular responsibility; and 8% (or 2) people said that nobody was designated to perform that function. However, one of the respondents in the latter group had previously said that his fraud squad did not have its own computer. Of those stating that someone from another branch acted as their computer manager, 56.25% (or 9) of them had previously said that they had their own computers. This aspect of the research also supports the theory, that vulnerability to computer derived evidence exists in 40% (or 10) of those fraud squads whose representatives answered this question. This risk also impinges on their lack of ability to authenticate the proper operation of the computer equipment that was used.

5.6. SUMMATION OF QUESTIONNAIRE FINDINGS.

The combined total of fraud squad personnel in England and Wales (based on the data given in the returned questionnaires), is now estimated to account for only .047% of manpower nationally. These figures indicate a dwindling of the manpower resources being allocated by police in the campaign against fraud, when compared with the statistics given in the Fraud Trials Committee Report, (based on data for the year 1985) which indicated that fraud squads represented .048% of all police manpower. In that sense, there has been a lack of response towards increasing the resources that are being devoted to fraud investigation.¹ Although it could also be argued that establishments have neither increased or decreased in real terms. On the other hand, there has been a considerable increase in computer support to fraud squads² although quite a number of fraud squads still badly need computer support³ or better computer systems than at present,⁴ and improved training facilities for their computer operators.

Facsimile machines are a welcome investigative tool, but there are still a high proportion of fraud squads that do not have their own.⁵ Although other factors are adding to the already high caseloads of some fraud squads, such as those which now involve drugs profit confiscation investigations, resulting from the Drugs Trafficking Offences Act 1986,⁶ data examined in these questionnaires reveals an almost unanimous view from those who felt that here is a high degree of inter-fraud squad cooperation in terms of resource sharing and that, claims for reimbursement were not normal in such cases.⁷

1. See at p. 111-112 above.

2. See at p. 113 above.

3. See at p. 114 above.

4. Supra footnote 3, above.

5. See at p. 14 above.

6. See at p. 114-5 above.

7. See at p. 115 above.

There now appears to be an increasing awareness among fraud squad officers regarding developments in technology, vis-a-vis case presentation to juries¹ involving the use of computer graphics² and spreadsheets,³ and there is evidence to support an argument that advances in technology are being made by fraud squads due to their recent use of computer systems.⁴ There is also a moderate awareness amongst fraud squad officers who felt that the use of visual aids had increased during the presentation of complex information.⁵

On the question of career prospects,⁶ the majority of respondents felt that little change had taken place. There had been an important police initiative in terms of training fraud squad officers in computer crime investigation techniques,⁷ although the wastage rate of these skill-trained officers to other duties was relatively high. There is little evidence of improvement in terms of other specialist training for fraud squad officers, according to most of the replies that have been received to this questionnaire,⁸ but the degree of access to Anacapa trained personnel is considered to be high in the majority of cases.⁹

Whilst there is evidence which indicates that modern techniques are increasingly being used in current trials,¹⁰ the rate of legislative and other changes affecting the work of fraud squad officers, has revealed the need to cross-fertilise views between fraud squads, via the medium of a national conference¹¹ and published material.¹² In terms of safeguarding computer generated evidence, there appear to be weaknesses in the procedures

1. p.118 above.
2. p.116 above.
3. p.116 above.
4. p.118 above.

5. p.117 above.
6. p.120 above.
7. p.120 above.
8. p.121 above.

9. p.122 above.
10. p.122 above.
11. p.124 above.
12. p.125 above.

used by a fairly high proportion of fraud squads, relevant to authenticating the proper operation of computer systems as required under existing legislation.¹ These shortfalls could risk the admissibility of evidence which may have taken months of arduous investigation and preparation.

There are many initiatives currently being developed by fraud squads but these are often made in isolation from others. The police service has not yet begun a coordinated approach towards the standardisation of computer systems relevant to the needs of fraud investigators, as they have with HOLMES, in the case of other complex and serious crimes. There is therefore a pressing need to consider the future technological requirements of those fraud squad establishments falling under the influence of the Home Office, if a good standard of effectiveness in fraud investigations is now to be achieved, and in order that plans may be laid for the next decade of fraud policing.

The Ministry of Defence Police have been pioneering the development of a hand picked, multi-user computer system with many sophisticated devices, which is catering for the needs of an investigation from the time that it commences, until the evidence is presented at court. The degree of success which has been achieved by this one branch of the police service, (even though funded by another government department), could be matched by their Home Office counterparts, given the right level of commitment. To fail to plan in this developing area of police science and technology, will add to important initiatives being delayed, or perhaps even lost to the service forever. The end result must surely be a proliferation of fraud squads which are neither efficient nor cost-effective.

1. See p. 44-47, above.

B. FINAL CONCLUSIONS AND RECOMMENDATIONS.

The need for this research developed from an awareness that rapid advances in technology and apposite legal reforms, were poised to envelop the traditional arena of fraud policing. As heralds of this conception, the Frauds Trials Committee drew attention in their Report (ibid. 1986a) to the lack of resources devoted to the campaign against fraud, by the police and other agencies having investigative responsibilities. Gathering their evidence from witnesses in the police service and elsewhere, this Committee pressed for change in two significant areas. It proposed that adequate legislation be introduced to enable complex evidence to be presented to juries in ways that were more palatable, and that there should be a more effective and efficient approach to the investigation of fraud. However, the Fraud Trials Committee (1986a at p. 2) were insistent that many of the reforms that they had proposed, had potential benefits to a wider range of criminal cases.

Since the Committee focussed criticism at all levels of the criminal justice system, it was inevitable that the police service as an integral part of that infrastructure, should also attract its fair share of culpability for resilience towards change. The inability of the system to handle complex trials effectively, amounted to a denial of justice to the society which it served. The basis for this belief having arisen from certain miscarriages of justice which had enabled slick fraudsters to escape justice because the complexity of their crimes exceeded the perceived levels of jury comprehension. In other circumstances, defendants against whom there was insufficient evidence, were being denied their right to a prompt trial, which as members of a fair and democratic

society they, or a close member of their family, would be entitled to expect under such conditions.

Due to the timely commencement of this research, it has been possible to monitor key legislative reforms in tandem with their progress. Furthermore, it has also provided the platform from which to assess the effectiveness of technology, both as the medium for managing complex information and its consequential effect in helping to improve the quality of justice that may be dispensed through its use in the higher courts.

Several key issues have emerged during the process of this research which serve to demonstrate the practical advantages offered by technology. Such benefit in terms of fraud investigation and its essentially high investigative input, is the potential for computers to reduce human effort in its application to complex tasks. Juxtaposed with trends in modern society which require higher standards of case-work presentation,¹ computers are very likely to provide at least part of the solution to the problem created by the inadequacy of resources, which are apportioned to the investigation of serious fraud.

Although there is evidence to show that fraud squads are now responding to the challenge of technology more positively through their increased use of computer systems, the overall approach amounts to a piecemeal attempt. Sadly, these fragmented efforts are contributing to delays in improvements to fraud policing nationally.² This constitutes a failure to draw upon recent past

1. Which is noted at p. 11 above.

2. This not only impairs progress in matching the current IT strategies that are rapidly becoming necessary in modern fraud policing, but also casts a gloomy prediction for future developments in computer science.

experiences¹ which have shown that it is uneconomical for novices to embark upon uncoordinated experiments aimed at attempts to identify their user needs of expensive equipment. The fact that this state of affairs has been allowed to develop is particularly unfortunate, when taking into account the fact that the Home Office and the police service have at their joint disposal, many experts² with a wealth of experience in computer science.

There is every reason to suppose that reforms in legislation will enable 'techno-evidence' to be furnished to juries in ways that will make it easier for them to understand it. Providing that investigators are prudent enough to ensure that techno-evidence is properly authenticated when derived from computers, such evidence should have as beneficial effect upon the process of a complex investigation and the business of the courts, as they are already having upon the business of the modern world. However, there is clear evidence to show that further reforms are necessary to the law, to allow for the drafting of sustainable charges against computer fraudsters.

In terms of improving still further the the quality of justice that may be dispensed by the courts, valuable lessons have been learned from a study of the American criminal justice system. In that sense, technology has come to the rescue in a number of important areas. The use

-
1. As was the position during the development of HOLMES for example, when similar problems were encountered.
 2. The Ministry of Defence Police fraud squad, however, have been much wiser than their Home Office counterparts in their sensible use of computer scientists to project manage an ideal system which totally satisfies their multi-user requirements.

of electronic tagging devices is helping to ease the burden on prison establishments, through the provision of a monitoring system which allows for the release of more defendants on parole. As noted above,¹ there has also been a successful campaign to reduce re-offending. The scheme which concerns drug-in-body defendants, requires them as a condition of their bail to submit urine samples, so that tests can be carried out electronically for controlled substances.

Such is the speed of development in information technology, as well as the increasing demand for it in all areas of policing, that it has been necessary to comment on some further issues in a brief addendum section to this thesis. Recent proposals² to extend the admissibility of electronically produced documents to cases involving purely traffic violations will, if implemented, herald the seemingly limitless application of information technology to a diverse range of criminal investigations. With this philosophy in view, the need to safeguard the propriety of such evidence, is even more profound.

This research has demonstrated that information technology has an unequivocal part to play in improving the quality of justice in modern society. In order that the police service may continue to ensure that fraud policing, in particular, is conducted in accordance with the principles of effectiveness, efficiency and economy, action is now required to set in train these necessary reforms. The key issues that will enable fraud policing to increase its contribution towards a higher standards of justice are formulated within a number of recommendations that follow in the next part of this chapter.

1. At p. 96

2. See for example footnote 2, at p. 140, below.

RECOMMENDATIONS ARISING FROM THIS RESEARCH.

This research supports the theory that, apposite to the investigation of fraud, there have been a number of important initiatives within the Police Service since the publication of the Fraud Trials Committee Report in January 1986.¹ However, there is also a strong argument in favour of the need to increase these initiatives if the police role in regulating serious fraud and other complex crimes is to keep pace with developments in modern technology. The following recommendations therefore seek to address some of the more pertinent issues.

Serial No.	Recommendations.	Thesis Page No.
1	That ACPO consider giving their approval to a two year plan to further a standardised approach to the IT strategies and needs of fraud squads in England and Wales, based on all or some of the recommendations which follow. ²	130

1. For example, see p. 25 above, regarding the development of an expert system by the Metropolitan Police fraud squad, with funding provided by the Home Office. See pp. 120-121 above, with reference to the computer crime investigation techniques training course at Bramshill Police College. See p. 93 above, regarding the joint police and other-agencies initiative, during the information technology conference held at Hendon Police College in March, 1988. There was a management exchange between the Metropolitan and Ministry of Defence Police in 1987, in furtherance of an IT strategy awareness program, in the investigation of serious fraud. Finally, there was a joint initiative between the Metropolitan Police fraud squad and members of the Institute of Chartered Accountants in England and Wales, which sat as a working party to consider the IT needs of fraud squads, and techniques of presenting evidence to juries.

2. These further recommendations are continued overleaf.

Serial No.	Recommendations.	Thesis Page No.
2	That a national fraud conference be held ¹ at the Police Staff College to further the awareness of IT strategies and other developments in fraud policing.	124-5
3	That a national fraud bulletin be published quarterly, ² in furtherance of promoting strategies in fraud policing.	125
4	That a coordinator be appointed to address the national shortfall in computer operator training ³ revealed during this research.	114
5	That the Home Office be requested to fund research into fraud squad computer and other technology, requirements. ⁴	25

-
1. Plans are already being laid by the Metropolitan Police fraud squad, to promote this concept.
 2. This could be separately edited as a news sheet, but published in tandem with the Information Desk Bulletin, which is issued by the Home Office Police Requirements Support Unit. A similar strategy was used to promote the concept of HOLMES.
 3. The aspect of training could be expanded to include presentational techniques, which are becoming increasingly significant in the light of the Criminal Justice Acts 1987 and 1988. The scheme as envisaged, would be similar to the national training program which operated during the infancy of HOLMES. There many other useful issues that a national coordinator of fraud training could address, including a collation plan of computer systems suitable for fraud squads whose variation in manning levels range from between 130+ officers, to as low as only 2.
 4. Such a move would help to avert duplication of physical and financial effort. More importantly, it would help smaller fraud squads to identify their user needs.

Serial
No.

Recommendations.

Thesis
Page No.

- 6 That ACPO examine the problems 126-7
 created by the use of different
 policies by fraud squads, in terms of
 their computer generated evidence,
 and consider guidelines accordingly.

The following recommendation is addressed
to the Metropolitan Police, in particular.

- 7 That, in view of recent 26
 legislation, a working party
 be formed to address the issues
 and implications arising from the
 Criminal Justice Acts 1987/1988,
 with relevance to the perceived
 increase in the use of information
 technology during investigations
 and in the presentation of complex
 evidence at court.

ADDENDUM.

This short section seeks to consider some of the almost daily developments in information technology that are beginning to affect all aspects of modern policing. One example of this growing awareness is reflected in the recent efforts of ACPO (Association of Chief Police Officers, which organised a conference¹ at the Police Staff College, Bramshill, during April 1988 to deal with the national issues relating to the police use of video technology. A further indication of commitment by senior police management towards developments in information technology, is marked by the participation of the Commander of the Metropolitan and City Police Company Fraud Department at Holborn, as a member of an ITAC (Information Technology And the Courts) working party on the use of IT, for the presentation of evidence.

There is another significant area of change which is mirrored by the formation in January 1987 of the Police Staff College Research Unit. Included in the various tasks undertaken by this unit, are the functions of liaison with ACPO Technical and Research Committee, the Police Requirements Support Unit, the Home Office Scientific Research and Development Branch,³ and like organisations.⁴ Growing demands for the development of new technology and its use during the presentation of evidence at court, have

-
1. See Drew. B., (1988) A Report to the ACPO Requirements and Research Group of the Technical and Research Committee, unpublished conference notes held at the Police Staff College library.
 2. A sub-committee of the Society for Computers and the Law.
 3. Who were responsible for coordinating the development of HOLMES and other IT projects.
 4. See Annual Report of the Commandant of the Police Staff College, London: HMSO.

also contributed to increased scientific workloads at the Metropolitan Police Forensic Science Laboratory and elsewhere.¹

Other recent studies in the area of information technology include an assessment of the costs and benefits of mobile data terminals and the feasibility of computerisation in Regional Crime Squads.² The computerised system FACES (Facial Analysis, Comparison and Elimination System) has also been developed to the prototype stage and will play a prime role in the identification process.³ Important developments in DNA profiling⁴ to forensic examination, provide significant proof of the effect of information technology in all aspects of policing.

Countless media reports⁵ also draw attention to the progress that is being made in the use of information technology during the investigation of child abuse cases, and the implementation of live video links as the medium for communicating their evidence. Due to the degree of interest in this particular topic and the speed at which it is developing, workshops are now being designed at a

-
1. Annual Report of the Commissioner of Police for the Metropolis, (1987) at p. 35. London: HMSO.
 2. Annual Report of Her Majesty's Chief Inspector of Constabulary, (1987) at p. 46. London: HMSO.
 3. Supra note 2 above.
 4. Supra note 2 above, at p. 47.
 5. As for example, Use of Video in the Investigation of Child Abuse, (supra note 2, above at p. 48). Child Evidence on Video Plan Probe - Judge to Head Advisory Group, The Job Newspaper dated 8.7.88 at p. 2. Child Abuse Cases - TV Links Approved, The Job Newspaper dated 20.1.89 at p. 9. and Rape Victim Makes Legal History in Court Video Link, The Police Review dated 13.1.89.

number of academic institutions¹ to satisfy the thirst for knowledge in this poignant area of criminology.

Final proof of the growing significance of technology as an investigative tool, and, as the medium for presenting evidence, featured as an article in a recent newspaper report² and heralds the almost limitless range of IT potential in criminal prosecutions, due to the proposed admissibility of photographic evidence in support of traffic violations by motorists. If legislation is passed to render this form of evidence admissible, it will almost certainly minimise the need for high speed car chases. Thus, in this extreme example, the use of technology as a medium for presenting evidence at court, could well have the consequential effect of reducing danger to human life.

-
1. Such as the Faculty of Law at Southampton University. See for example Proposed Workshop on the Legal Applications of Video Technology, an unpublished loose minute to prospective participants, postdated 7.1.89.
 2. Move to Catch Bad Drivers on Camera, Daily Telegraph dated 8.2.89 at p. 1.

Appendix A.

TEL. 559122
EXT.
TELEX 47661



FACULTY OF LAW
THE UNIVERSITY
SOUTHAMPTON
SO9 5NH

25th August, 1988

Dear Colleague,

I am currently undertaking research into various aspects associated with visual forms of evidence. A more precise description of my study proposal is:

EVIDENCE VISUALISED: (The effect of legislation and other initiatives on the investigation, prosecution and presentation of visual evidence in serious fraud cases).

The principal focus of my research is the reaction of the Police Service towards certain of the recommendations which were contained in the Fraud Trials Committee Report, when published on 10th January, 1986. It is quite evident that a number of important initiatives have already begun since the Roskill Report was released, although conflicting demands on police resources elsewhere, appear to have inhibited what might otherwise have been a more favourable response.

A copy of the completed thesis will be presented to the library of the Police Staff College at Bramshill, in due course. A brief summary of the results of this questionnaire will be provided to applicants on request. It may become necessary to pursue any significant developments a little further and hopefully, those who wish to cooperate, will indicate accordingly at the end of this questionnaire.


No individual will be named in my text and any other wishes you may have regarding anonymity and/or confidentiality, will be strictly observed. No person other than myself will have access to your replies. Should you require the return of your questionnaire once I have processed it, please indicate hereon. (A photocopy will not be kept under these circumstances).

This exercise is worthwhile and the information is not available to me from other sources. Please, take part by completing the questionnaire and mailing it to me at the above address.

Please complete and mail:

By 5 P.M. ON FRIDAY, 23rd September, 1988.

Thank you for your help.


Phil Whittick.

(Ps. I can normally be contacted in my study most afternoons, on telephone No; 0703.768923 Ext 207. Please note that I will be abroad from 1st until 19th September.)

EVIDENCE VISUALISED:

(The effect of legislation and other initiatives on the investigation, prosecution and presentation of visual evidence, in serious fraud cases).

QUESTIONNAIRE.

No. .

Guidance notes for completion. Please read carefully.

1. Read each question and consider your answer.
2. Preferably, use RED, yes RED ballpoint, fibre-tip or coloured pencil (for ease of processing responses).
3. Tick [✓] the box adjacent to the appropriate answer for questions of fact, or the most appropriate for opinion.
4. Please ensure that you answer all questions: estimated time around 15 minutes to complete - you may decide to spend longer.
5. Please post your completed questionnaire to;

A.P. Whittick,
The Faculty of Law,
The University,
Southampton, SO9 5NH.

by 5 P.M. ON FRIDAY, 23rd September, 1988.

Please turn to SECTION ONE 

QUESTIONNAIRE: 'EVIDENCE VISUALISED.'

SECTION ONE: RESOURCES.

Please complete each question by putting a red tick in the box by the appropriate answer(s).

1. HAS THERE BEEN ANY VARIATION IN THE ESTABLISHMENT OF YOUR POLICE STAFF SINCE THE ROSKILL REPORT WAS PUBLISHED ON 10th January, 1986?.

(tick one)

1 There has been an increase.....
 2 There has been a decrease.....
 3 There has been no variation.....
 1a HOW MANY OFFICERS DO YOU NOW HAVE?..... 4

Q1.

2. HAS THERE BEEN ANY VARIATION IN THE ESTABLISHMENT OF YOUR CIVIL STAFF SUPPORT SINCE THE ROSKILL REPORT?.

(tick one)

1 There has been an increase.....
 2 There has been a decrease.....
 3 There has been no variation.....
 2a HOW MANY CIVIL STAFF DO YOU NOW HAVE?..... 4

Q2.

3. HOW ARE YOU OFF FOR COMPUTER SUPPORT SINCE THE ROSKILL REPORT?.

(tick one)

1 We now have our own computer(s).....
 2 We still do not have a computer.....
 3 We don't have a computer any longer.....
 3a AN INCREASE OR DECREASE OF HOW MANY?..... 4
 3b HOW MANY COMPUTERS DO YOU NOW HAVE?..... 5

Q3.

QUESTIONNAIRE: 'EVIDENCE VISUALISED.

4. IF, YOU HAVE ACCESS TO COMPUTER SUPPORT, HOW AVAILABLE IS IT?.

(tick one)

We have our own computer which is for..... 1
our sole use only.

Other police officers share our computer..... 2

We share police owned equipment, with..... 3

Q4

We share the equipment of an outside agency... 4



4a WHICH OTHER AGENCY? 5

5. TO WHAT EXTENT HAVE FINANCIAL CONSTRAINTS INHIBITED YOUR PLANS FOR COMPUTERISATION?.

(tick one)

We badly need any computer support system..... 1

We need better equipment..... 2

We do not require computers at all..... 3

Q5.

We have sufficient computerisation..... 4

6. HOW ARE YOU OFF FOR COMPUTER OPERATOR TRAINING?.

(tick one)

It is arranged on site..... 1

We have facilities within the force..... 2

External training is arranged..... 3

Suitable training isn't available..... 4

Q6.



6a WHERE? 5



QUESTIONNAIRE: EVIDENCE VISUALISED.

7. WHAT IS YOUR DEGREE OF ACCESS TO A FACSIMILE MACHINE?.

- We have sole use of our own..... 1
- We have easy access, even though we share..... 2
- We do not have easy access to one..... 3

Q7.

7a HOW ADVANTAGEOUS ARE FACSIMILE MACHINES TO FRAUD INVESTIGATORS?.

- They are most advantageous..... 4
- They have some advantages..... 5
- They have hardly any advantages at all..... 6

8. WHAT HAS BEEN THE EFFECT OF THE DRUGS TRAFFICKING OFFENCES ACT 1986, TOWARDS INCREASING THE WORK OF YOUR OFFICERS? (ie, assistance to other branches in asset tracing, network analysis and asset sequestration).

- It has considerably increased our workload.... 1
- We have experienced some increase..... 2
- Little increase in our workload is evident.... 3

Q8.

9. WHEN OPERATIONAL ASSISTANCE IS REQUIRED, HOW MUCH HELP ARE OTHER FRAUD SQUADS IN SHARING RESOURCES?.

- They frequently help..... 1
- We are mostly refused help..... 2
- We are always refused help..... 3

Q9.

9a WHEN ASSISTANCE IS RECEIVED, HOW FREQUENTLY ARE YOU REQUIRED TO REIMBURSE THE OTHER FORCE?

- We are mostly required to pay..... 4
- We must pay, 50% of the time..... 5
- We are not usually required to pay..... 6

QUESTIONNAIRE: EVIDENCE VISUALISED.

10. HOW HELPFUL ARE YOU WHEN OTHERS SEEK YOUR OPERATIONAL SUPPORT?.

(tick one)

We help most of the time..... 1

We help 50% of the time..... 2

Financial constraints prevent us from helping. 3

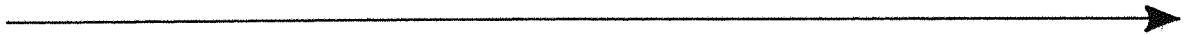
Q10.

10a IN THE EVENT THAT YOU ASSIST OTHER FRAUD SQUADS, HOW FREQUENTLY DOES YOUR FORCE REQUIRE REIMBURSEMENT?.

We are mostly obliged to seek reimbursement 4

We sometimes seek reimbursement..... 5

We avoid asking for reimbursement..... 6



QUESTIONNAIRE: 'EVIDENCE VISUALISED'.

SECTION TWO: DEVELOPMENTS IN TECHNOLOGY.

11. HOW MUCH IMPORTANCE IS ATTACHED TO THE USE OF COMPUTER GRAPHICS (ie, bar charts etc) BY YOUR FRAUD SQUAD, FOR THE PRESENTATION OF STATISTICAL INFORMATION?.

- (tick one)
- We attach a great deal of importance..... 1
- We attach some importance..... 2
- Very little importance is attached..... 3

Q11.

11a HOW FREQUENTLY ARE COMPUTER GRAPHICS USED?.

- They are used frequently..... 4
- They are sometimes used..... 5
- They are hardly ever used..... 6

12. HOW MUCH IMPORTANCE IS ATTACHED TO THE USE OF SPREADSHEETS BY YOUR FRAUD SQUAD?.

- (tick one)
- We attach a great deal of importance..... 1
- We attach some importance..... 2
- Very little importance is attached..... 3

Q12.

12a HOW FREQUENTLY ARE SPREADSHEETS USED?.

- They are used frequently..... 4
- They are sometimes used..... 5
- They are hardly ever used..... 6

QUESTIONNAIRE: EVIDENCE VISUALISED.

13. TO WHAT EXTENT HAS THE ROSKILL REPORT INFLUENCED ANY INCREASE IN THE USE OF VISUAL AIDS? (ie, of whatever simplicity or complexity).

(tick one)

- The increase in use is considerable..... 1
- The increase is only moderate..... 2
- Hardly any increase in their use has 3 taken place.

Q13.

14. HAVE ANY SIGNIFICANT ADVANCES BEEN MADE BY YOUR FRAUD SQUAD IN YOUR RECENT USE OF TECHNOLOGY?.

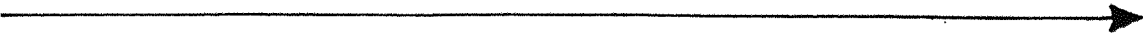
(tick one)

- There have been significant advances..... 1
- There have been minor advances..... 2
- Nothing of any significance has occurred..... 3

Q14.

14a WHAT ADVANCES?

Continue here if necessary.



QUESTIONNAIRE: EVIDENCE VISUALISED.

SECTION THREE: CAREER PROSPECTS AND TRAINING.

15. HAS ANY CHANGE OCCURRED REGARDING THE CAREER PROSPECTS OF OFFICERS ON FRAUD SQUADS, SINCE THE PUBLICATION OF THE ROSKILL REPORT?
(ie, is there now a career structure within the fraud squad itself)

- (tick one)
- The situation has improved considerably..... 1
 - There has been a slight change for the better. 2
 - There has been no noticeable improvement..... 3
 - The situation has worsened..... 4
- 15a HOW? 5
- Q15.

16. PLEASE INDICATE WITH A [✓], IF ANY OF YOUR OFFICERS HAVE RECENTLY ATTENDED COURSES ON THE INVESTIGATION OF COMPUTER CRIME, AT ANY OF THE FOLLOWING ESTABLISHMENTS

- (a) Police Staff College, Bramshill..... 1
 - (b) FBI Academy, Quantico..... 2
- 16a HOW MANY HAVE ATTENDED THIS BRAMSHILL COURSE? 3
- 16b HOW MANY OF THESE OFFICER(S) HAVE SINCE LEFT THE FRAUD SQUAD?..... 4
- Q16.

17. ARE COURSES IN SPECIALISED SUBJECTS BECOMING MORE AVAILABLE TO FRAUD SQUAD OFFICERS?.(ie, accountancy etc).

- (tick one)
- There are now many more courses available..... 1
 - There are a few more courses available..... 2
 - There is no increase in course availability... 3
 - Course availability is declining..... 4
- Q17.

QUESTIONNAIRE: EVIDENCE VISUALISED.

17a PLEASE GIVE REASONS FOR YOUR ANSWER TO QUESTION 17.

18. COULD MORE BE DONE TO TRAIN OFFICERS IN THE ANALYSIS AND PRESENTATION OF NUMERICAL AND OTHER COMPLEX INFORMATION?.

- (tick one)
- Much more could be done..... 1
- Some courses already cover this..... 2
- Specialists such as, accountants do this..... 3
on our behalf.

Q18.

19. DO YOUR OFFICERS HAVE READY ACCESS TO ANACAPA TRAINED PERSONNEL?.(ie, people who analyse statistics and prepare charts with information flows).

- (tick one)
- Ready access is usually available to us..... 1
- We have some access, subject to availability.. 2
- Access is severely restricted..... 3

20. HAVE ANY OF YOUR OFFICERS BEEN INVOLVED AT CROWN COURTS WHERE MODERN TECHNIQUES HAVE BEEN USED TO PRESENT EVIDENCE DURING A COMPLEX TRIAL?.

- (tick one)
- We regularly use modern techniques..... 1
- We sometimes use such techniques..... 2
- We prefer the traditional methods..... 3

Q20.

20a IF ANY NOTEWORTHY METHODS HAVE BEEN USED, PLEASE SUPPLY DETAILS OF OFFICER IN CASE HERE, (FOR COMMUNICATION PURPOSES), FROM WHOM FURTHER INFORMATION MAY BE OBTAINED.

20b IF YOU KNOW OF OTHER OFFICERS IN YOUR FORCE WHO HAVE USED NOTEWORTHY MODERN TECHNIQUES, PLEASE ALSO SUPPLY THEIR DETAILS FOR COMMUNICATION, PURPOSES.

QUESTIONNAIRE: EVIDENCE VISUALISED.

SECTION FOUR: REFORM AND INITIATIVES.

21. HOW EFFECTIVE DO YOU SEE THE PROPOSED REFORMS TO THE LAW BEING, IN THE CAMPAIGN AGAINST FRAUD?

- (tick one)
- The proposed reforms should be sufficient..... 1
 - The proposed reforms seem inadequate..... 2

Q21.

21a PLEASE STATE YOUR REASON(S) FOR THIS VIEW. _____

22. DO YOU SEE ANY POTENTIAL BENEFITS IN HOLDING A NATIONAL FRAUD CONFERENCE FOR FRAUD SQUAD OFFICERS?.

- (tick one)
- There are many potential benefits..... 1
 - There are some potential benefits..... 2
 - There are too few potential benefits..... 3
 - There are no potential benefits at all..... 4

Q22.

22a IF A NATIONAL FRAUD CONFERENCE WERE TO BE HELD, WHAT SUBJECTS WOULD YOU LIKE TO SEE BEING DISCUSSED? (PLEASE STATE YOUR OPINION UNDERNEATH HERE).

QUESTIONNAIRE: EVIDENCE VISUALISED.

23. DO YOU SEE POTENTIAL BENEFITS, IN ISSUING A NATIONAL FRAUD BULLETIN TO FRAUD SQUAD OFFICERS ON A REGULAR QUARTERLY BASIS?.

- (tick one)
- There are many potential benefits..... 1
- There are some potential benefits..... 2
- There are too few potential benefits..... 3
- There are no potential benefits at all..... 4

Q23.

23a. IF A FRAUD BULLETIN WERE TO BE ISSUED, WHAT SUBJECTS WOULD YOU LIKE TO SEE INCLUDED? PLEASE GIVE YOUR OPINION UNDERNEATH HERE.

QUESTIONNAIRE: EVIDENCE VISUALISED.

SECTION FIVE: REGULATING COMPUTER GENERATED EVIDENCE.

24. WHEN SUBMITTING EVIDENCE PREPARED BY FRAUD SQUAD OFFICERS FROM A COMPUTER (ie, computer graphics and spreadsheets etc,) HOW FREQUENTLY IS THE 'PACE' CERTIFICATE COMPLETED?.(See appendix 'A').

- (tick one)
- Usually it is completed..... 1
 - It is completed infrequently..... 2
 - It is rarely completed..... 3
 - It is not considered applicable..... 4

Q24.

25. WHAT METHOD DO YOU EMPLOY FOR MONITORING MALFUNCTIONS OF THE COMPUTER?.

- (tick one)
- A special log is kept, 'on-site'..... 1
 - Another department monitors our malfunctions.. 2
 - No particular arrangements exist..... 3
 - We don't have our own computer..... 4

Q25.

26. DO YOU EMPLOY A COMPUTER MANAGER?.

- (tick one)
- A delegated member of our staff does it..... 1
 - Someone from another branch does it..... 2
 - Nobody has that particular responsibility..... 3

Q26.

26a IS IT A POLICE OFFICER OR MEMBER OF CIVIL STAFF?

- (tick one)
- A police officer performs this task..... 4
 - It is done by a member of the civil staff..... 5
 - We don't have our own computer..... 6

QUESTIONNAIRE: EVIDENCE VISUALISED.

27. IS THERE ANYTHING YOU WOULD LIKE TO SAY BY WAY OF CLARIFICATION OF YOUR ANSWERS TO ANY QUESTION(S)?

Q. No.	Additional comments/information

Q27.

28. WOULD YOU BE WILLING TO PARTICIPATE FURTHER?

Yes..... 1

No..... 2

Q28.

PLEASE CHECK THAT YOU HAVE NOT MISSED ANY QUESTIONS.

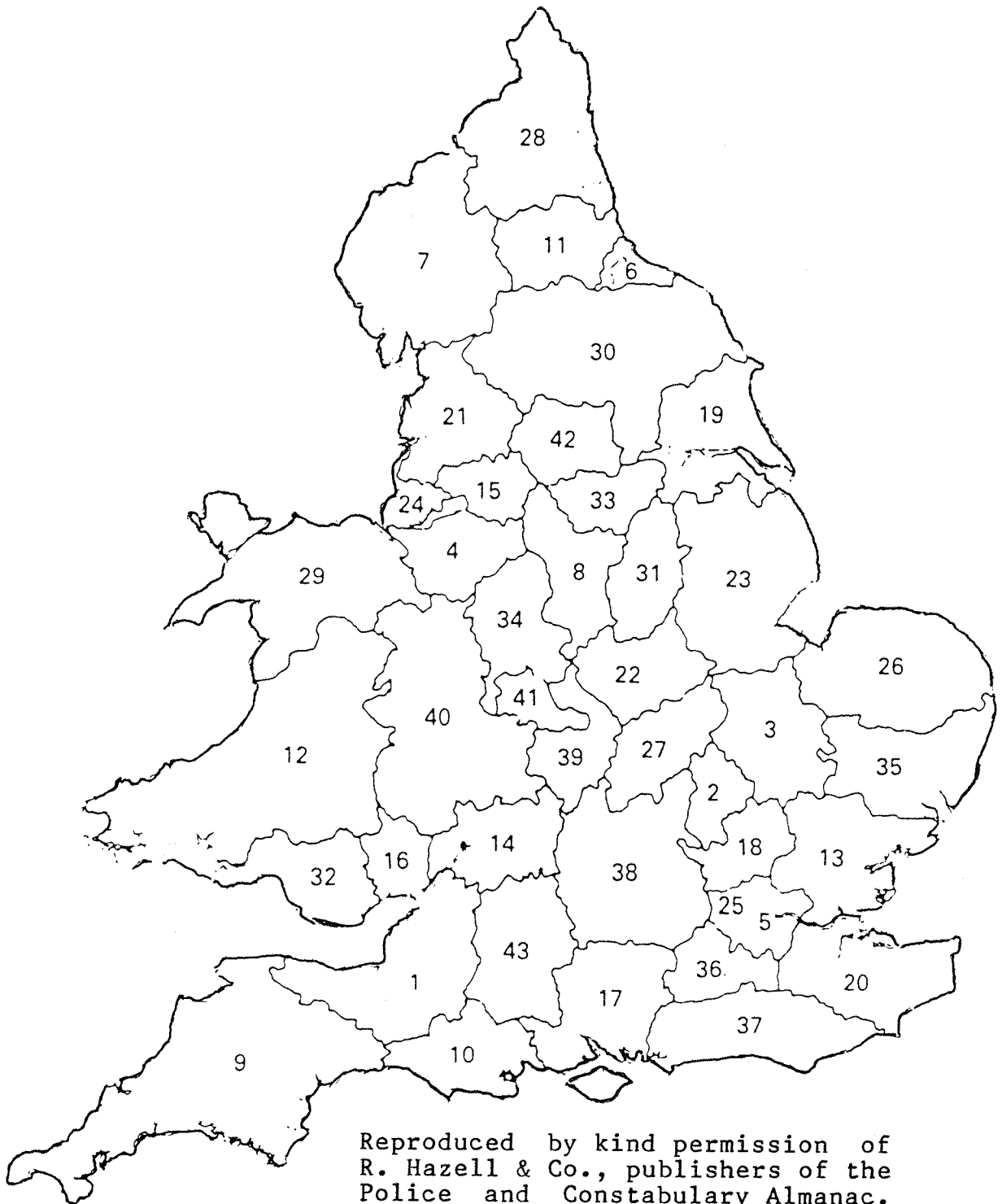
PLEASE POST TO ME, USING THE ENCLOSED STAMPED ADDRESS ENVELOPE

BY 5 P.M., FRIDAY, 23rd September, 1988.

THANK YOU FOR YOUR COOPERATION: A summary of results will be available on request from 1st January, 1989 onwards.


Phil Whittick

25th August, 1988.

Appendix B.**MAP OF POLICE FORCES IN ENGLAND & WALES**
(Forces are identified by their NRC number)

Reproduced by kind permission of
R. Hazell & Co., publishers of the
Police and Constabulary Almanac.

- 1 Avon & Somerset 2 Bedfordshire 3 Cambridgeshire 4 Cheshire 5 City of London
6 Cleveland 7 Cumbria 8 Derbyshire 9 Devon and Cornwall 10 Dorset
11 Durham 12 Dyfed-Powys 13 Essex 14 Gloucestershire 15 Greater Manchester
16 Gwent 17 Hampshire 18 Hertfordshire 19 Humberside 20 Kent 21 Lancashire
22 Leicestershire 23 Lincolnshire 24 Merseyside 25 Metropolitan 26 Norfolk
27 Northamptonshire 28 Northumbria 29 North Wales 30 North Yorkshire
31 Nottinghamshire 32 South Wales 33 South Yorkshire 34 Staffordshire 35 Suffolk
36 Surrey 37 Sussex 38 Thames Valley 39 Warwickshire 40 West Mercia
41 West Midlands 42 West Yorkshire 43 Wiltshire 44 R.U.C.

BIBLIOGRAPHY.

- American Bar Association, Computers in Litigation (1979).
- Amory. B., and Poullet. Y., Computers in the Law of Evidence - A Comparative Approach in Civil and Common Law Systems. Revue Internationale de Droit compare, 2, 1985, 331.
- Anacapa. Undated course literature, circa 1979.
- Appleby. R.C., (1972). Modern Business Administration. London. Pitman.
- Baldwin. D., Fraud in a Good Light. The Police Review Aug 9th, 1985 at p. 1622.
- Bender. D., Computer Evidence Law: Scope and Structure 1 Comp. L. J. 699 (1979).
- Bergsten. E., Legal Value of Computer Records: Report of the Secretary-General United Nations Commission on International Trade Law. 1 Comp. L. & Prac. 205 (1985).
- Bernacchi. R., and Larson. G., Philosophy, Data Processing and the Rules of Evidence. 10 Law Notes 11 (1974).
- Bigelow. R., The Use of Computers in the Law. 24 Hast. L. J. 707 (1973).
- Blair. A., Price fixing and Problems of Proof: The Computer Lends a Hand. 43 Mo. L. R. 686 (1978).

- Boyce. R., Judicial Recognition of Scientific Evidence in Criminal Cases. 8 Utah L.R. 313 (1963).
- Brereton. H., The Admissibility in Evidence of Microfilmed Records. 59 A.B.A.J. 500 (1973).
- British Computer Society, Computer Generated Output as Admissible Evidence in Civil and Criminal Cases, (1982).
- Bronstein. D., and Engelberg. D., A Preliminary Assessment of the Reception of Computer Evidence: report of the Computer Evidence Survey Project. 21 Jurimetrics J. 329 (1981).
- Brown. R., Computer-Produced Evidence in Australia. 8 Univ. Tas. L.R. 46 (1984).
- Budnitz. M., Problems of Proof When There's a Computer Goof: Consumers Versus ATMs. 1980 Computer Law Journal 49.
- Burnside. J., Computers and Law: Evidence and Discovery. 12 Aus. Bus. L.R. 370 (1984).
- Campbell. M.R., A Background Guide to the Financial Markets and Institutions. Unpublished research monograph, circa December, 1986.
- Cantor. G., Reconsideration of the Admissibility of Computer-Generated Evidence. 126 U. Pa. L.R. 425 (1977).

- Caplin. M., What written Records Must Companies Keep When Using Electronic Data Processing? 16 J. Tax. 373 (1962).
- Carr. H., Criminal Search Warrants under the Copyright Act. (1986) 4 E.I.P.R. 95.
- Chandler. J., Crime and Computer Evidence. 97 L.Q.R. 23 (1981).
- Connery. E., and Levy. S., Computer Evidence in Federal Courts. 84 Comm. L. J. 268 (1979).
- Crown. D.A., The Role of the Questioned Document Examiner in Computer Crime Investigations. Computer Security Readings from Security Magazine (1987) at pp. 289-292.
- Curtis. I., The Use of Computers in Magistrates Courts. Training Guide to the Development of Human Resources. London. Unpublished Home Office research monograph, dated February 1987.
- De Hetre. J., Data Processing Evidence - Is It Different? 52 Chi-Kent L.R. 567 (1976).
- Delves. E., The Influence of Computers on Business Record Keeping. 5 Modern Uses of Logic in Law 46 (1964).
- Dombroff. M., Demonstrative Evidence: Computer Reconstruction Techniques. 18 Trial 52.
- Du Cann. R. (1964). The Art of the Advocate. Mdx. Penguin Books.

- Duggan. M., Computer Evidence. 5 Litigation 293 (1986).
- Dutton. J., The Official Records Exception to the Hearsay Rule in California. 6 Santa Clara Law. 1 (1965).
- Eastin. C., Use of Models in Litigation: Concise or Contrived? 52 Chi-Kent L.R. 610 (1975).
- Ebden. A., Computer Evidence in Court. (1985) S.A.L.J. 687.
- Elliott. D., Mechanical Aids to Evidence. (1958) Crim. L.R. 5.
- Evans. J., Proof of Business Records Kept or Stored on Electronic Computing Equipment. 11 A.L.R. 3rd 1378 (1967).
- Ewald. T., Discovery and the Computer. 1 Litigation 27 (1975).
- Fenwick. W., and Davidson. G., Use of Computerised Business Records in Evidence. 19 Jurimetrics J. 9 (1978).
- Foreman. S., Evidence - Admissibility of Computer Print-Outs. 52 N. Car. L.R. 903 (1974).
- Fraud Trials Committee Report (1986a). London: HMSO.
- Fraud Trials Committee Report (1986b). Improving the Presentation of Information to Juries in Fraud Trials: A Report of Four Research Studies. HMSO: London.

- Freed. R., Evidence and Problems of Proof in a Computerized Society. 4 Modern Uses of Logic in Law. 171 (1963).
- Freed. R., A Lawyer's Guide through the Computer Maze. 6 Prac. Law. 15 (1960).
- French. M., The Admissibility of Computer Records in South African Law of Evidence. (1982/3) Natal U.L.J. 113.
- Fromholtz. H., Discovery, Evidence, Confidentiality and Security Problems Associated with the use of Computer-Based Litigation Support Systems. 1977 Wash. U.L.Q. 445.
- Galbraith. J.K., The New Industrial State, 2nd edn, Deutsch. (1972), pp. 12-13; Penguin edn, (1974) pp. 31-32.
- Gaukroger. J., (1988). Information Technology in the Office. London: McGraw-Hill Book Co.
- Goger. T., Proof of Public Records Kept or Stored on Electronic Computing Equipment. 71 A.L.R. 3rd 232 (1976).
- Hans. V.P., and Vidmar. N., (1986). Judging the Jury. New York. Plenum.
- Golden. A., Law Report R. v. Gold and Another. 57 Computers and Law. Sept. 1988. at p. 14.
- Hawkins. M.J. (ed.), (1987). The Oxford Reference Dictionary. Oxford: Oxford University Press.

- Hederman. C., Data Exchange between Magistrates' Courts and other Agencies. Undated research monograph. London: Home Office Planning Unit.
- Holliday. A.H., Computers in the Court - How Computer Graphics were used to Present Evidence at the Old Bailey. Computers and Law 57. Sept. 1988 at p. 19.
- Home Office. (1987). Evaluation of the use of computers in Magistrates' Courts. London: Home Office Pilot Phase Report.
- Institute of Chartered Accountants (1987a) Combatting Fraud. London: Ernst and Whinney.
- Institute of Chartered Accountants (1987b). Countering Computer Fraud. A Report of the Information Technology Working Party. London; Institute of Chartered Accountants in England and Wales.
- Institute of Chartered Accountants. Report on the Progress of Joint Accountants/Police Working Party on Presentation of Evidence to Fraud Trials Juries (forthcoming).
- Jacobson. M., The Use of Computer Printouts as Evidence in Commercial Litigation. 82 Com. L.J. 14 (1977).
- Jaffe. K., and Spierer. L., (1988). Misused Statistics. New York. Marcel Dekker Inc.

- Jenkins. M., Computer-Generated Evidence Specially Prepared for Trial. 52 Chi-Kent L.R. 600 (1976).
- Johnstone. R., A Guide for the Proponent and Opponent of Computer Based Evidence. 1 Computer L.J. 667 (1979).
- Karmel. M., Procedure and Proof, in Goode. R., (ed), Electronic Banking - The Legal Implications. (1985).
- Keating. M., Computer Evidence. 12 Litigation 35 (1985).
- Kelman. A., Computer Evidence and the Police and Criminal Evidence Act 1984. 134 New L.J. 237 (1984).
- Kelman. A., and Sizer. R., The Computer in Court (1982).
- Khan. A., Is a Computer Printout Admissible Evidence? 48 J. Crim. L. 31 (1984).
- Kinney. E., Use of Computer in Pre-trial Statistical and Financial Data Analysis, in Computer Framework for Complex Litigation. (1976), 59.
- Korn. H., Law, Fact and Science in the Courts. 66 Col. L.R. 1080 (1966).
- Laughlin. C., Business Entries and the Like. 46 Iowa L.R. 237 (1961).
- Levi. M., (1987). Regulating Fraud. White Collar Crime and the Criminal Process. London: Tavistock Publications.

- Levi. M., (1988). The Prevention of Fraud. Crime Prevention Unit Paper No 17. London: Home Office.
- Levin. R.I, and Kirkpatrick C.A., (1966) Planning and Control with PERT/CPM. New Delhi. McGraw-Hill Inc.
- Lord Chancellors' Department. (1987) Computerisation of County Court Procedures in Debt Cases. The Claims Registry. London. The Lord Chancellors' Department.
- Lowman. G., Evidence: The Admissibility of Computer Print-Out in Kansas. 8 Washburn L.R. 330 (1969).
- Lloyd-Bostock. S., Psychology and the Law: A Critical Review of Research and Practice. Brit. J. of Law and Society. 8, pp. 1-28 (1981).
- Madden. T., Information Management in Complex Litigation. 4 Litigation 12 (1969).
- Mackay. E., La Traitment de la Documentation Juridique par Ordinateur au Canada. 8 La Revue Themis 323 (1973).
- Maclean. D, (1986) Report on the Evaluation on the use of Computers in Magistrates' Courts. Costs of Magistrates' Courts Computer Systems in relation to workload. London: Home Office Research and Planning Unit.
- Maclean. D, (1986) Report on the Evaluation on the use of Computers in Magistrates' Courts. The Way Forward. London; Home Office Planning Unit.

- Maclean. D., (1987) Report on Computers in Criminal Justice: The Promise of Reality. London: Home Office Research and Planning Unit (draft report).
- Marcellino. J., Expert Witnesses in Software Copyright Infringement Actions. 6 Comp. L.J. 35 (1985).
- McCoid. A., The Admissibility of Sample Data into a Court of Law: Some Further Thoughts. 4 U.C.L.A. L.R. 233 (1957).
- McFarlane. G., Criminal Trials and the Technological Revolution. 133 New L.J. 327 (1980).
- McNiff. F., Computer Documentation as Evidence. 1 J of Law and Information Science 45 (1981).
- Meachum. M., Texas Business Records Act and Computer Printouts. 24 Bay. L.R. 161 (1972).
- Miller. J., The Admissibility of Computer-generated Evidence in Georgia. 18 Ga. St. Bar J. 137 (1982).
- Mills. L., Lincoln. K., and Lanhead. C., Computer Output - Its Admissibility into Evidence. 3 Law & Comp. Tech. 14 (1970).
- Mitchell. S., (ed.) (1982). Archbold Pleading and Practice in Criminal Cases. London: Sweet and Maxwell.
- Morris. J., (1983). Crime Analysis Charting. An Introduction to Visual Investigative Analysis. Orange Vale, California. Palmer Enterprises.

- Murray. D.J., Report on Computers in Magistrates' Courts. Outline Operational Requirements for Magistrates' Courts Computer Systems. London: Home Office.
- Murray. R., Discovery, Evidentiary, Confidentiality and Security Problems associated with the Use of Computer Based Litigation Support Systems in Computer Framework for Complex Litigation. (1976).
- Naughton. J., (ed.) (1981). Living with Technology. Introduction to a Foundation Course. London: The Open University Press.
- Nelson. D., Impact of Computers on the Legal Profession. 30 Bay. L.R. 829 (1978).
- Niblett. B, and Boreham. G., Cluster Analysis in Court. (1976) Crim. L.R. 175.
- Note: Admitting Computer Generated Records. 18 J. Mar. L.R. 115 (1984).
- Note: Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence. 1977 Wash. U.L.Q. 59.
- Note: Can IBM Impeach Their Own Documents? 20 Datamation 107 (Dec., 1974).
- Note: Computer Discovery in Federal Litigation: Playing by the Rules. 69 Ga. L.J. 1465 (1981).
- Note: Computers and California Law. 11 Santa Clara Law. 280 (1971).

- Note: Computing in the Courtroom: Using Computer Diagrams as Expert Opinions. 5 Comp. L.J. 217 (1984).
- Note: Guidelines for the Admissibility of Evidence Generated by Computer for the Purposes of Litigation. 15 U.C.D.L.R. 951 (1982).
- Note: No Access to Taped Evidence. 32 Am. U.L.R. 257 (1982).
- Note: Police Requirements Support Unit. Open Systems Interconnection - An Overview. Information Desk Bulletin No. 26. June 1987 at para. 3. London: Home Office.
- Note: Police Requirements Support Unit. Holmes Newsletter. Information Desk Bulletin No. 29 at p. 33. London; Home Office.
- Note: Police Requirements Support Unit. Home Office IT Research Grants. Information Desk Bulletin No. 29 at p. 4. London: Home Office.
- Note: Police Requirements Support Unit. Information Technology Strategy for the Police Service. Information Desk Bulletin No. 9 at p. 23.
- Note: Report on Fraud Policing/Management Exchange Between the Metropolitan Police and the Ministry of Defence Police. (1987) Unpublished internal memorandum.

- Note: Tantum. M., When a Loss Becomes a Crime - The Serious Fraud Office Approach to Computer Fraud. Unpublished guide to the work of the Serious Fraud Office, dated 9.8.88.
- Note: The Discovery and Use of Computerised Information: An Examination of Current Approaches. 13 Pepp. L.R. 405 (1986).
- Note: Televised Courts Aim to Demystify the Legal System. The Lawyer Magazine, vol. 2. iss. 9., dated 5.5.88, at p. 14.
- Ontario Law Reform Commission, Report on the Law of Evidence. (1976) pp. 188-192.
- Overend. S, (1988a) Presentation of Evidence in the Courtroom - How IT can help. 56 Computers and Law at pp. 12-13.
- Overend. S, (1988b) The National Conference on Court Technology. 57 Computers and Law at pp. 20-24.
- Ovum Ltd. (1988). Expert Systems in Britain. London: Department of Trade and Industry.
- Painter. D, The Place of Reprographics in Management. Office and Information Management International. Journal of the Institute of Administrative Management. vol. 1, No. 5. Oct, 1987, at p. 29.
- Pate. W., Evidence: Admissibility of Computer Print-outs as Business Records. 9 Wake Forest L.R. 428 (1973).

- Pengilley. P., Machine Information Is It Hearsay? 13
Melb. U.L.R. 617 (1982).
- Poirier. C, Robb. G., and Mosher. J., Computer-based
Litigation Support Systems: the
Discoverability Issue. 54 U.M.K.C.L.R. 440
(1986).
- Ponsford. K, Visual Displays. Report No. 17/70 (1970).
An unpublished research monograph held at the
Police Staff College library at Bramshill.
- Prendergast. T., The Use of Data Processing in Litigation.
10 Loyola L.A.L.R. 285 (1977).
- Quade. V., Computing the Evidence: Technology Moves into
the Courtroom. 69 A.B.A.J. 882 (1983).
- Reese. R., Admissibility of Computer-Kept Business
Records. 55 Cornell L.R. 1033 (1970).
- Rentschler. J., Garbage In, Gospel Out: Establishing
Probable Cause Through Computerized Criminal
Information Transmittals. 28 Hast. L.J. 509
(1976).
- Roberts. J, Practitioners' Primer on Computer-Generated
Evidence. 41 Univ. of Chicago L.R. 254 (1974).
- Roberts. M, Are Punched Cards and Magnetic Tapes Tax
Records? 1971 Journal of Accountancy 76
(April).
- Robinson. J., Admissibility of Computer Print-outs Under
the Business Records Exception in Texas. 12
So. Tex. L.J. 291. (1971).

- Saxby. S., (ed.) Presentation of Evidence in the Court Room - How IT Can Help. Vol. 4, iss. 1, The Computer Law and Security Report (1988) at p. 12.
- Saxby. S., (ed.) The Serious Fraud Office. Vol. 4, iss. 1, The Computer Law and Security Report (1988) at p. 6.
- Schuck. C., Technique of Proof of Complicated Scientific and Economic Facts. 40 F.R.D. (1986).
- Scott. M., Computer Law (1984) ch. 10.
- Scottish Law Commission, Evidence Scot. Law. Com. 100 (1986) pp. 34-40.
- Securities and Investments Board (1986) Self-Defence for Investors. London: City and Financial Printing Services Ltd.
- Sherman. B., (1985). The New Revolution; The Impact of Computers On Society. Chichester. John Wiley and Sons.
- Skeen. A., Evidence and Computers. 101 S.A.L.J. 675 (1984).
- Smith. J.C, The Admissibility of Statements by Computer. (1981) Crim. L.R. 387.
- Smith. N., Admissibility of Computer Business Records as an Exception to the Hearsay Rule. 48 N.C.L.R. 687 (1970).
- Soma. J., Computer Technology and the Law. (1986).

- South African Law Commission, Project 6 Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers. (1982).
- Spencer. J.R., Child Witnesses and Video Technology Thoughts for the Home Office. 51 Journal of Crim. Law. (Pt. 4) Nov. 1987.
- Sprowl. J., Admissibility of Sample Data in Court of Law: A Case History. 4 U.C.L.A. L.R. 222 (1957).
- Sprowl. J., Evaluating the Credibility of Computer-Generated Evidence. 52 Chi-Kent L.R. 547 (1976).
- Staniland. H., Computer Evidence in South Africa: Admissibility in Civil Proceedings. 2 Comp. L. & Prac. 21 (1985).
- Steele. J., Computer-produced Printouts - Reliable as Evidence. 100 S.A.L.J. 505 (1983).
- Strawn. D., Discovering Computerised Records. 71 A.B.A.J. 72 (April, 1985).
- Susskind. R. (1987). Expert Systems in Law. Oxford University Press.
- Symposium on Science and the Rules of Evidence. 99 F.R.D. 187 (1983).
- Tapper. C., (1988) Computer Evidence unpublished research monograph.
- Tapper. C., Use of Computer Printouts in Criminal Cases. 2 App. Comp. and Comm. L.3. (April., 1985).

- Tapper. C., Computer Law (3rd ed., 1983) Ch. 6 and pp. 224-230.
- Tapper. C., Computer Output as Evidence. (1982) Ox. J. of Leg. St. 128.
- Tapper. C., Evidence from Computers. 8 Georgia L.J. 562 (1974).
- Tapper. C., Computers and the Law. (1973) Ch. 2.
- Taubner. A, The Computer as Expert Witness: Toward a Unified Theory of Computer Evidence. 19 Jur. J. 274 (1979).
- Varley. H., (ed.) (1980) Colour in Psychology Marshall Editions Ltd: The Netherlands. Smeets Offset B.V. Weert.
- Vergari. J, Evidential value and acceptability of Computer Digital Image Printouts. 9 Rutgers Comp. and Tech. L.J. 343 (1983).
- Wallace. R, Computer Print-Outs of Business Records and Their Admissibility in New York. 31 Alb. L.R. 61 (1967).
- Whittick. A.P., (1988) Visual Technology Unpublished research monograph.
- Young. J., Computer Generated Evidence. 21 Trial 14 (1985)
- Younger. I, Computer Printouts in Evidence: Ten Objections and How to Overcome Them. 2 Litigation 28 (1975).

Younger. I, On Technology and the Law of Evidence. 49
Univ. of Colo. L.R. 1 (1977).

Zorkoczy. P., (1982) Information Technology An
Introduction. Bath: Pitman