HANDBOOK OF PERSONAL DATA PROTECTION

Masden, Wayne, UK, Macmillan, (1992), 1026 pages including index, $A198.00 from Macmillan in Melbourne (see flier enclosed with this issue).

This book is a 'comprehensive manual for those involved in both national and international aspects of personal data protection. While the United Nations, OECD and EEC have made some strides towards an international view of data protection, most people would predominantly be impacted by data protection legislation within their own country. Thus, a reference work of this type and scope is much needed and will prove useful to a wide range of readers.

The book is divided into two major parts. Part ONE (chapters 1-8) discusses the relevant aspects of various national and sub-national data protection issues and presents a concise summary of the relevant statutory and administrative initiatives in the geographic area concerned. These include: Western European Initiatives (ch 2); East European Data Protection (ch 3); the US (ch 4); Australia, NZ and Canada (ch 5); Japan and Hong Kong (ch 6); Asia, Africa and South America (ch 7) and International developments (ch 8).

Part TWO contains a collection of national and international laws on data protection. Especially valuable will be data protection legislation which was not previously available in English, but was specially translated for this publication.

In addition to the valuable reference material, both primary and secondary, readers will also appreciate Chapter 1 of Part One which provides a highly readable and insightful historical and contemporary perspective on data protection issues ranging from a survey of the legislation, trans-border data flow restrictions, adoption in some countries of blocking laws, data protection in the lesser developed nations, personal data abuses, police files, marketing of data, protection of sensitive medical data, storeage methods of personal data, network and on-line privacy and the use of electronic work place monitoring.

The overall production copy of the book is also excellent and its attractive hard cover and high quality paper will withstand the heavy use which occurs with reference books. My only suggestion for improvement is that the bibliography on such an important topic and otherwise comprehensive book was inadequate. Perhaps later editions might consider adding major articles and even cases from each jurisdiction.

Overall, the book delivers what it promises: a comprehensive manual on national and international aspects of personal data protection.

Review by Eugene Clark, Lecturer in Law, University of Tasmania.

DATA SECURITY REFERENCE GUIDE

Abingdon, Sophos Ltd., 1991/92. 290 pages plus glossary and index. $35.00 U.S.

Automated systems and technology have expanded rapidly to all functional areas and operations in most organisations. These functional areas of operations can be critical to the organisation and extended disruption of these systems could result in severe financial loss. Therefore, an important need exists in ensuring the security of data. In the past few years corporate data security requirements have changed considerably. This change is reflected in the contents of this reference guide by Sophos Ltd, a company which specialises in and sells a range of data security products.

This very readable and interesting book discusses the strategy behind data security, the numerous attacks on software with a large section on computer viruses and finally a section on data security products that are available by Sophos. This book will be of great interest, not only to data security managers, accountants, auditors, lawyers, computer scientists, and any computerised organisation, but also the person with only a basic background in computer science.

Data Security Reference Guide can be divided into four areas: 1) data security strategy; 2) software attacks; 3) additional information; and 4) data security products.

The first chapter identifies the basic strategy applied to ensure a 'completely secure shell' is placed around the vulnerability of stored and communicated data. The methods used include: 1) encryption - re-arranging or disguising information so that it cannot be understood by an unauthorised person (A method used as early as the Etruscan times and now being applied to computer-based systems in modern society); 2) authentication - a technique used between the sender and receiver to validate the source and the text of a message (Disputes over the contents of a message can be avoided, and forgeries, tampering or transmission errors will be detected.); 3) secure erasure - a method used to remove file contents completely from magnetic media such as disks (Using standard system commands only remove the file name and not the contents from the disk.) (p13). The first chapter also discusses the dangers to stored information and to information in transit. The next three chapters go into more depth regarding the three strategies that are available.

Chapter 5 identifies the four basic forms of software attacks on computer systems which include: 1) Trojan horses - a program which performs services beyond those stated in its specification; 2) logic bombs - are simple If statements which release damage routines when triggered by some condition such as time, or the presence or absence of data such as a name; 3) viruses - have four essential characteristics, replication, executable path, side-effects, and a disguise; and 4) worms - rogue programs similar to viruses that do not need a carrier (p40 - 43).

A lengthy chapter 6 focuses on all known computer viruses. It explains in more depth what a computer virus is and some simple rules for

employees to observe. It also discusses all virus types and how they infect. In addition to simple rules set out for employees, anti-virus procedures are also suggested.

Chapter 7 is a conglomerate of information ranging from various data and computer Acts in existence in the UK, a discussion on access control, a brief summary of the 'Orange Book' published by the US Department of Defense on formalised criteria for the evaluation of the security of a computer system, a brief explanation of a UK security product certification scheme, a listing of periodicals, books, and conferences on data security, to a group of commonly asked questions on data security.

The balance of the chapters discusses data security products. The first problem encountered by clients is how to choose a security product. Chapter 8 provides a chart that lists the problems and the appropriate Sophos products that can be used to solve the particular problem. It also identifies the variety of computer systems that can run Sophos software. In the same chapter, six case studies are presented outlining a problem and a suitable solution. The rest of the chapters provide a description, a list of features, the applications, and technical details of all the available products from Sophos on data security.

As indicated earlier, the book will be useful to a number of individuals who will find this book easy to read and a good basic introduction to data security. However, the book is only a reference guide and the discussions are at a very basic level with the solutions to data security problems directed towards Sophos products.

Review by Pat Clark, Accounting and Finance Department, University of Tasmania.

INFORMATION SECURITY HANDBOOK

William Caelli, Dennis Longley, Michael Shain, Editors. New York, Macmillan Publishers Ltd, 1991, 798 pages plus index, $180.50.

The use of computers has extended in to areas such as universities, commerce and industry, the military, and even into our own homes from one computer in one room to millions half way around the world. So pervasive is the use of and dependence upon computers that the 1990s have begun with determined efforts to address the problem of information security. The Information Age began during the Second World War when energies were devoted to cracking German machine ciphers. A by-product of this activity was the first digital computer. The information age has gone full circle from attacking information security, to gearing information security, to using ciphers to protect the computer system. The publication of this book is one effort to address this problem.

The book has three editors, Professor William Caelli, Professor Dennis Longley, and Michael Shain. Professor Caelli is the Director of the Information Research Centre at the Queensland University of Technology and Technical Director and Founder of Eracom Pty Ltd. He has extensive experience in both computer technology and information. He leads the research and development team for a company that manufactures a range of cryptographic equipment for the finance and banking industry and encryption sub-systems for the personal computer market. Professor Longley is Dean of the Faculty of Information Technology at the Queensland University of Technology and has presented numerous papers on data security at international conferences. He is joint author of several books as well. Michael Shain is a Senior business consultant with GE Information Services, providers of the world's largest commercially available computing network. He designs and implements secure systems for the banking and financial services industry and has co-author several books. The individual authors of each chapter come from all around the world with expertise in the area of their writing.

The size of the book appears daunting at first. However, the book is well planned in that it provides a comprehensive discussion in the areas of managerial, legislative and technical aspects of information security. Each chapter is presented in such a way as to enable an isolated study of that topic with cross references to other chapters when the topic impinges on other areas. There are eleven chapters, each averaging about a hundred pages. This very readable book will appeal to a large audience from academics and professionals to anyone with a general interest in the topic of data security.

Chapter One by Michael Shain presents an overview of security. He first identifies what information is at risk and how the increasing number of PCs being used in many organisations has weakened the stringent controls that characterise most mainframe computing. Security is a broad concept and most organisations and people will express theirs needs in terms of confidentiality of sensitive information, integrity of information and programs, and availability of a prompt computing service. Security policy is a fundamental responsibility of management. Therefore, management should

design controls to prevent security breaches by ensuring individual accountability, separation of certain duties, and by auditing the services provided. Determining how much security is required will depend upon an assessment of the risks. An organisation will need to decide where it is vulnerable, what countermeasures are available and undertake an analysis of possible threats which are then balanced against available security countermeasures, their effectiveness and costs. Shain suggests that security is like a chain with many links and that it is important that all links are of equal strength. Management should ensure that all parts of the computing system are fully secure. Any weaknesses and the chain could break.

Chapter Two by Paul Dorey, Head of Information Security for a major British bank, is entitled 'Security Management and Policy'. The purpose of the is chapter is to view information security from the perspective of managing people in a commercial organisation. He emphasises that the responsibility must first fall on the Board of Directors to develop security guidelines and the risk taking profile that the Board wishes the business to follow. A manager is then directly responsible for implementation of the policy reporting back to the Board periodically. He also stresses that it is essential that security issues are routinely considered as part of any business decision. Security is concerned with people, and can only be achieved if adequately managed.

Chapter Three, 'Risk Management' by Alison Anderson, a university lecturer, and Michael Shain, highlights the special kind of risk pertaining to computerised information systems. They explain its relation to conventional notions of risk and then demonstrate how risk modelling can be a powerful tool in managing risk.

Imagine arriving to work one morning, the air is filled with smoke, the sky is greyish black, and red flames are shooting six metres in the sky. This is the subject of Chapter Four, 'Contingency Planning and Damage Avoidance' also by Paul Dorey. Information technology is the life blood of many organisations. When the phones go dead, the computer system goes down, the fax machine malfunctions, an organisation, if not prepared, can be critically damaged. A prudent organisation will have a contingency plan. However, an adequate plan is not an after thought, but part of the systems design process.

'Information Security and the Law' by Ian Walden, a lecturer and consultant on computer law, is the title of Chapter Five. This chapter should be great interest to the legal profession. This chapter considers how information security policy is impacted, either directly or indirectly, by the national and international legal framework. Walden divides this chapter into four major sections, Legislative Solutions, Contractual Solutions, Evidential Issues, and International Activity. The first section, Legislative Solutions, is primarily descriptive, based on legislation in the areas of information security (eg data protection), information technology (eg copyright, patent, evidence), and information security issues (eg US Computer Security Act 1987). The second section, Contractual Solutions, focuses on the use of contracts as a way of ensuring legal security in the absence of legislation. This section is of a prescriptive nature and suggests areas and issues that businesses should consider when drafting agreements. Legal problems of

proof, evidence that information has been held, used, delivered and unaltered are considered in the third section, Evidential Issues. It should be noted that information security law covers not only criminal law, but civil and administrative law as well. The last section, International Activity, offers an overview of the most prominent organisations in this area.

Chapter Six, 'Monitoring and Audit Control' by Ken Slater, a Managing Consultant specialising in information technology, will be of great interest to Auditors. This chapter identifies and describes the responsibilities and activities of those in the area of monitoring the existing controls. Those individuals include internal and external auditors, the quality assurance team, and the Information Security Officer.

In Chapter Seven, 'Applications and Theory of Cryptography', the authors, Longley, Caelli, and Ed Dawson, a university lecturer, concentrate on the application and management of cryptographic systems. Cryptographic is concerned with protecting the secrecy of information. It involves mathematical transformations of information to ensure the integrity of the information and proving that it originated from the proposed sender. This chapter considers the algorithms themselves and also current developments in the field. Even those not mathematically inclined will nevertheless appreciate the complexities of the topic.

The proof of identity is a crucial process in computer and network control. If an attacker can provide the proof demanded of a legitimate user then the security system will be completely bypassed. Controlling access to a computer system is the subject of author, Longley's Chapter Eight. Proof of identity may take one of three forms, either individually or in combination, something the user knows, something the user possesses, something the user is. The major part of the chapter is devoted to this aspect of access control.

Chapter Nine also by Longley is devoted to 'Security of Stored Data and Programs'. The data security of a database system raises problems of a degree of complexity greater than those of file access because access to a data item may be formed from information contained in more than one file. It has been suggested that database security, in its entirety, may not be possible with the current generation of computer hardware. This chapter explores the nature of this problem.

The protection of software is a much less demanding task because software is not normally changed by users. Software is generally 'read only' data. It was generally only vulnerable to programmers until the advent of the 'virus' and the 'worm'. The second part of this chapter deals with malicious code and investigates the implications of the virus and the worm on the security of organisational software assets.

In recent years, there has been a dramatic increase in the use of telecommunications in many organisations throughout the world. Because of the number of transactions being transmitted through telecommunications services a number of organisations are highly dependent on the service being both continuously available and of guaranteed integrity. Any disruptions put an organisation at risk. As a consequence, the control, management and

security of communications networks have emerged as major information technology issues of the 90s as highlighted in Chapter Ten, 'Communications Security' by Caelli and Alan Tickle, a university lecturer.

The final chapter, 'Formal Models of Secure Systems' by Longley focuses on the formal models presented in the Orange Book (US Department of Defense, 1983) and ITSEC (European Commission, 1990). Computer and communication systems have become extremely complex, making it impossible for one individual to have an overview of the complete system including a detail knowledge of the hardware and software of each component part. Because of the complexity, it makes it very difficult to determine how secure the system is. The concept of a formal secure systems model is to view the complex system from the viewpoint of security alone, separating the components of the system. In a sense, the purpose of the formal models is to 'measure' security. It is a highly specialised area and one with very few experienced personnel.

The 1990s have begun with a determined effort to address the problem of information security. Information Security Handbook is one such effort to address the problem by providing an excellent collection of writings that were informative and thought provoking on issues that should concern use all as we march forward into the 21st century.

Review by Pat Clark, Accounting and Finance Department, University of Tasmania.

DATA PROTECTION IN AUSTRALIA

Gordon Hughes, Sydney, Law Book Co. Ltd., 501 pages plus index, $79.50 (U.S.).

The introduction of the computer age and the development of the databank has greatly enhanced the storage of personal information by private and public bodies. Associated with this storage of information is the increased possibility of the unauthorised release and/or misuse of the computerised data.

With this in mind Gordon Hughes examines the 'extent to which the law protects personal information stored in computer databanks.'[1] The author considering that 'The increasing tendency to computerise data of a personal nature, in both the public and private sectors, together with the increasing capacity of computers to retain information which may be out of date, inaccurate or no longer necessary for the purpose for which it was originally collected, justifies the specific legal regulation of certain data processing activities.'[2]

Chapter 1 is titled 'The Computerisation Phenomenon' and introduces the reader to the need to distinguish between computerised and manual systems as well as the difference between information obtained in the public sector, and data that is accumulated by the private sector. Some specific privacy concerns are also raised, such as the collection of information, its disclosure/storage and possible abuse. Hughes sets the theme for the remainder of the book by stating that, 'The reader may conclude that the present level of protection is significantly deficient, and that increased regulation is required.'[3]

Prior to considering the legislative initiatives in this area, Hughes commences with an examination of privacy as a legal concept. He contrasts the attitude of the Australian and English courts with the approach of the judiciary in the United States of America. The courts in the latter jurisdiction recognising privacy in four broad areas: intrusion, public disclosure, placing an individual in false light and the appropriation of name or likeness for monetary advantage. 'The fact remains that courts in the United States have demonstrated a creativity in the field of privacy which, presumably, is capable of further development. This gives rise to the question of whether courts in Australia or the United Kingdom are capable of demonstrating a similarly innovative approach.'[4] After further discussion of the precedents in Australia and England the conclusion is reached that the 'prospect of an effective policy being implemented at common law is virtually non-existent.'[5]

---

1 p.18

2 p.17

3 p.18

4 p.27

5 p.33

Chapters 3 through to 5 examine the legislative initiatives introduced at both a State and Federal level within Australia, chapter 3 also discussing overseas legislative endeavours. Hughes considers that the introduction of data protection legislation in many jurisdictions indicates a global concern for some form of control over the use and storage of computerised data.[6] The author then fully explores the Commonwealth initiatives. The Australian Law Reform Commission report on Privacy is detailed as is the Senate Standing Committee Tax File Number Report of 1988. Hughes also scrutinizes the *Privacy Bill* of 1986, the *Privacy Act* 1988, *Privacy Amendment Act* 1990 and the *Data-Matching Programme (Assistance and Tax) Act* 1990. The reports and legislation are given detailed treatment with the strengths and weaknesses of each examined closely. Two major weaknesses are exposed by the writer. One, 'there appears to have been inadequate recognition of the threats to privacy posed by the computerisation of personal information'[7], and two, 'the lack of willingness to comprehensively embrace the private sector.'[8]

The author undertakes the same process in considering the privacy reforms that the States have implemented. A detailed account of reports emanating from the New South Wales Morison Report of 1973 is undertaken as well as consideration of legislative initiatives. The legislation falling into three broad categories. 'First, there has been legislation specifically addressing the right of privacy. Secondly, a number of attempts have been made to regulate the activities of credit bureaux, principally as a result of concern over the computerisation of credit data. Thirdly, legislation has been successfully introduced in two States establishing a statutory privacy guardian.'[9] However, much the same pessimism that clouded the Commonwealth legislation is evident in the author's concluding comments on the State legislation. 'Differing views as between States have been expressed on the desirability of privacy legislation and the form privacy legislation should take....Most significantly, in the present context, there has been no philosophical acceptance that legislation specifically regulating the handling of computerised personal information is necessary.'[10]

Chapter 5 is devoted to Freedom of Information legislation that has been introduced at both a Commonwealth and State level. The context in which this is relevant to the theme of the book is that the concept of privacy includes the right of access to information and the right to amend if the data is inaccurate or misleading. The exemptions to the legislation are fully canvassed as well as the provisions for amendment of personal records. Hughes considers that problems result from lack of uniformity between the

---

6 See the comments by Hughes, p.40

7 p.115

8 p.115

9 p.132

10 p.164

States[11] and the failure of some states to legislate in this area.[12] This leads Hughes to comment; 'Unfortunately, the extent of non-implementation of freedom of information legislation exemplifies the unlikelihood of future uniform legislation to regulate the flow of information, in computerised or other form, ever being achieved in this country.'[13]

Chapter 6 provides an analysis of the Breach of Confidence Action, this action being the most likely to address the problems created by the computerisation of personal information. The doctrinal basis, elements, defences and the remedies available are considered as the action's relationship with the *Privacy Act* 1988 (C'th). The author also lists the limitations (as noted by the Australian Law Reform Commission) on privacy protection afforded by the action for breach of confidence. Because of these limitations the action does not provide an adequate supplement to the privacy legislation.[14]

The next chapter raises a number of miscellaneous causes of action which, in addition to breach of confidence, may allow a remedy for the abuse of information contained in a data bank. The possible actions, amongst others, include trespass, conversion, nuisance and inducing breach of contract. However no action is entirely satisfactory and that 'in view of the numerous inherent deficiencies in the miscellaneous remedies, a satisfactory level of protection can only be achieved through comprehensive legislative intervention on a national scale.'[15]

The various legislative criminal sanctions for computer abuse, both at a State and Federal level, are raised[16], and consistent with the motif of the book, it was stated; 'It now seems beyond question that traditional criminal laws cannot adequately regulate threats to the security of personal data associated with computerised information storages.'[17] Hughes submits that a uniform approach is required as many instances of computer abuse will involve activity which arises in more than one jurisdiction. Furthermore he considers that the Commonwealth has failed to fully exploit its constitutional power to enact national legislation in this area.[18]

The final chapter deals specifically with problems caused by conflicts of law between jurisdictions. While the author recognises that jurisdictional issues are not unique to computer-related activities, 'the prospect of remote

---

11 See the comments by Hughes, p.195

12 It should be noted that the Tasmanian Parliament passed Freedom of Information legislation in 1991.

13 p.196

14 See the comments by Hughes, p.223

15 p.255

16 Though I do note the omission of the *Criminal Law Amendment Act* 1990 (Tas)

17 p.298

18 See the comments by Hughes, p.298-299

access to or dissemination of electronically stored data across jurisdictional boundaries represents a fertile area for future dispute.'[19]

The book also contains three major appendices containing extracts from Official Reports/Privacy Guidelines and Second Reading Speeches. In addition to the full bibliography I found these to be an excellent research source for people working in this area.

Overall the book is thoroughly researched and its theme of inadequate data protection regulation in Australia is convincingly established. The reader is left in no doubt that Australia's laws in this area are deficient and in need of national review. The legislators, academics and practitioners in the field of data protection will find the book interesting and a stimulus for further discussion in the area.

Review by Lynden Griggs, Lecturer in Law, University of Tasmania.

---

19 p.331

CRIME AND THE COMPUTER (OXFORD MONOGRAPHS ON CRIMINAL LAW)

Martin Wasik, Clarendon Press, Oxford, 1991. 240 pages and Index, £35.00 (U.K.)

In the year following the appearance of this book, its author published an article which could serve as an illuminating introduction to it. In fact, anyone intending to read the book would benefit from studying the article first. It is entitled, "Computer Misuse: The Role of the Criminal Law in the Control of Misuse of Information Technology".[1] In it, Martin Wasik, relying as he said, partly on the views of a German scholar, Sieber,[2] reviewed and analysed in a most useful way legislative developments over the last two decades relating to "computer misuse". Sieber's analysis shows, according to Wasik, that there has been broad similarity in the stages of development in western countries in that period of criminalisation of information technology abuse. There have been three stages, they say. The first was the development of data protection laws, such as the United Kingdom *Data Protection Act, 1984*; though there were earlier examples in other European countries. Then came the enactment at the beginning of the nineteen-eighties of new laws in response to computer-related economic crimes; and lastly, a trend, still continuing, towards improvement of intellectual property protection. An example of the latter is the United Kingdom *Copyright Designs and Patents Act, 1988.*

Perhaps if the author had had Sieber's insight at the time of writing the book, he might have arranged his subject matter to delineate more clearly than he has done developing patterns over time of legislation against computer misuse. But if this is a criticism of the book, it is one of form and not substance. It is easy for a reviewer to have second thoughts on behalf of an author. Probably he has had some himself. The method chosen in the book is to subdivide the subject matter as a whole into appropriate components, so that we are given an overview which begins with the nature and scale of the problems of computer misuse, and then proceeds to detailed consideration of the main areas in which it occurs, and the kinds of response which various western countries have adopted to each variety. Having done this in a scholarly way with copious references to statutes, cases and relevant writings, the author ends with two useful chapters on the detection, prosecution and proof of such offences, and on the international dimensions of computer misuse. Overall, the work provides a very thorough and complete treatment of the subject.

The term "computer misuse" is chosen in the title because one of the central problems for the law maker in this field is whether and to what extent various kinds of reprehensible activity which relate specifically to

---

1 *The Computer Law and Security Report*, Portsmouth, England: Solent Legal Exchange, Vol. 8. (1992), pp. 25 and following.

2 U. Sieber, "General Report on Computer Crime: The Emergence of Criminal Information Law", 13th International Congress of International Academy of Comparative Law, University of Bayreuth, 1990.

information technology should or not on balance be penalised by the criminal law. Wisely, the author deprecates a too ready or heavy-handed application of the criminal law to conduct by "hackers" and other manipulators of the computer environment which may or may not be sufficiently serious to warrant applying society's most potent weapon for deterrence and punishment. Nevertheless, he is firm in the view, again rightly, in this reviewer's opinion, that it is simplistic and mistaken to think that there is nothing special about computers in any situation which requires the enactment of special offences. One writer elsewhere has described in perceptive terms the challenge which development of information technology with accompanying opportunities for abuse poses for criminal law:

> "The ease with which electronic impulses can be manipulated, modified and erased is hostile to a deliberate legal system which arose in an era of tangible things and relies on documentary evidence to validate transactions, incriminate miscreants, and affirm contractual relations".[3]

There are undoubtedly some kinds of computer-related anti-social conduct with which orthodox criminal law cannot adequately cope. This book discusses elaborately the principle examples. Policy discussions on such matters as the kinds of conduct by "hackers" and other manipulators of the computer environment which should be criminalised, industrial spying, electronic eavesdropping, the relationship between computer misuse and white-collar crime, copyright and intellectual property issues, and the like, are one of the strongest features of the work.

The first two chapters, titled "The Nature of Computer Misuse", and "The Scale of the Problem", make a valiant attempt to deal with both the consuming reliance of modern society on computerisation, and consequent vulnerabilities to loss, damage and tragic accident from predatory misuse. Bearing in mind the great mass of detail available, the author has done very well to produce a discriminating but thorough account of both. Throughout the book each chapter is subdivided under appropriate heads. In the first chapter by that means we are taken through definitional problems, a generalised and non-technical description of computerisation, the increasing extent of reliance upon computers in every phase of modern business, science and education, public attitudes to computerisation, privacy issues, and the broad categories of computer misuse.

The second chapter, dealing with "the scale of the problem", first discusses the unsatisfactory nature of sources of information as to the extent of computer misuse, and reports and information uncovered by various agencies and inquiries in Britain, the remainder of Europe, the United States, Canada and Australia. Then the discussion proceeds to more detailed analysis of the various kinds of computer misuse, and the classifications which different experts have made. The author comes to the conclusion that there are three broad heads of misuse - unauthorised access and unauthorised use, fraud and information theft, and associated offences. He writes:

---

3 "Common Law for the Electronic Frontier", by Anne W. Branscomb, *Scientific American*, September 1991, pp. 112 and following.

> "In this book we are concerned both with describing various aspects of computer misuse and with identifying substantive criminal law issues, and so a mixture of approaches is adopted".[4]

The "mixture of approaches" involves identifying the substantive criminal law issues in relation to each of his three main kinds of computer misuse, and discussing in turn as he goes the responses adopted to each. This is done in chapters three, four and five, which are titled accordingly.

In chapter three, under the heading, "Unauthorised Access and Unauthorised Use", there is an elaborate discussion of the debate which occurred in the United Kingdom after the House of Lords' decision in *Regina v. Gold and Schifreen*[5] disclosed that "basic hacking", that is, obtaining unauthorised access to a computer or computer network, was not an offence within the ambit of the law of forgery under the *Forgery and Counterfeiting Act 1981*. The basic argument in the debate was whether such unauthorised access, if not accompanied by further evil intent, (as it was not in *Gold's Case*) should be criminalised. There was little disagreement that hacking for a further purpose should be an offence. In the United States, where much development had already taken place in criminalising computer misuse, the "basic hacking offence", or "computer trespass" as it was sometimes called,[6] had been made a crime under a number of statutes in different States. Eventually, the United Kingdom Government followed the same path. It adopted the recommendation of the Law Commission's Report and supported a private member's bill which resulted in enactment of the *Computer Misuse Act 1990*. The Act became law in August, 1990, and created three new criminal offences; which were basic unauthorised access, unauthorised access with intent to commit certain crimes, and corruption or erasure of computer programs and data. The author points out that this Act, in criminalising the initial computer trespass, regardless of whether it was accompanied by further evil intent, is apparently based on the view that computerisation is so important to modern societies, and the information and data held on computers often so sensitive and valuable, that there should be a sanction against initial wrongful access.

Chapter three also discusses wire tapping and eavesdropping, data protection offences, and misuse of computer time and facilities.

Chapter four deals with "Fraud and Information Theft". This has proved one of the most difficult areas to address because of its inherent challenge to orthodox criminal law concepts, as well as being the field in which most computer-related misconduct occurs. Many attempts to prosecute such offences under existing criminal law as "deceptions" have foundered upon the basis of incapability of a machine to be deceived. Law makers have become reconciled to the view that either fresh offences must be created, or old concepts expanded by artificial definition. In Australia there are examples

---

4 Chapter 2, p. 42.

5 (1988) 1 AC 1063.

6 E.g., S.9A of the *Crimes(Computers) Act 1988* of Victoria (No. 36 of 1988).

of both approaches. The *Crimes(Computers) Act 1988* of Victoria, for instance, follows the latter course. It amends the *Crimes Act 1958* of that State by defining "deception" to include:

> "an act or thing done or omitted to be done with the intention of causing
>
> (i) a computer system ..... to make a response that the person doing or omitting to do the act or thing is not authorised to cause the computer system ... to make";

and by providing that a reference to inducing a person to accept a false document as genuine, or a copy of a false document as a copy of a genuine document, is to be taken as including a reference to causing a machine to "respond to the document" etc. as if it were genuine. By contrast, the Tasmanian *Criminal Law Amendment Act 1990*, (which was enacted too recently to be noticed in the book under review), introduces to the Criminal Code a wide-ranging new offence called "computer fraud", which is very detailed but amounts to providing that anyone who interferes with a computer or computer data "with intent to defraud" is guilty of the crime of "computer-related fraud". The book, which deals in some detail with the Australian situation up to 1989, emphasises the diversity of approaches which have been followed in this country. It is a pity that Australian jurisdictions could not have co-ordinated their efforts in this of all criminal law fields, in which uniformity is most desirable, and problems of extraterritoriality are endemic by the nature of the medium. It is to be hoped that the present combined Federal and State Committee of departmental officials working on a draft Uniform Criminal Code for Australia, under the aegis of the Committee of Attorneys-General, will give attention to the problem.

Chapter 5 of the book is entitled, "Associated Offences". It deals with several varieties of nefarious conduct connected in one way or another with the use of a computer or data held on it, other than those which come within the rubric either of fraud or unauthorised access. It covers such matters as destruction and damage, particularly of programs or data, and the question whether these intangibles qualify as "property" under the *Criminal Damage Act 1971* of the United Kingdom (the usual answer given by courts apparently being affirmative); denial of access to an authorised user of a computer; use of a computer to cause death or physical injury to persons - for example by destroying or corrupting hospital or air traffic control data; using computer hardware or software as a means of blackmail; corruption in relation to unauthorised disclosure of computerised material and the like; unauthorised disclosure of official secrets; and aspects of secondary liability. The latter subsection is concerned with the manufacture and sale of devices which in fact or design can be used to aid the perpetration of computer misuse, such as software and devices which can be used to overcome computer security measures or software protection, radar speed traps, and so forth; and with the use of bulletin boards for exchange of destructive or invasive information between hackers, and other misusers.

The final chapters of the book deal with two interesting and complex areas of the subject, which are in addition closely inter-linked. Problems of "Detection, Proof, and Prosecution" are many, even where there is no international complication. The Tasmanian case of *Hollingsworth*, mentioned

in the book (p. 112), is an example. It was an "insider" offence where the perpetrator, a computer systems manager of a bank, made some rather intricate alterations of code to divert and transfer moneys to an interstate account. Had he not pleaded guilty (to an offence of which it might have been very difficult to convict him as a matter of law), and described to investigators how he had carried out the fraud, a conviction might have been impossible.

Such difficulties are made more complex by "The International Dimension". The author points out in this final chapter that the trans-national complexion of computer networking is rapidly becoming so pervasive that substantial fraudulent schemes will almost inevitably cross national boundaries. Many have done so already. Problems of territoriality were mentioned earlier. Modern statutes concerning computer crime have had to introduce quite elaborate provisions to deal with them - for example, ss. 4 to 11 of the United Kingdom *Computer Misuse Act 1990.* Detection and prosecution efforts have almost routinely to be co-ordinated internationally. The two final chapters give a very good account of these matters; though necessarily, because they are so complex and broad in scope, as indeed are each of the other chapter subjects, the account is compact. Despite some minor criticisms made in this review, the work is one of the most competent and satisfying overall treatments of the subject one has seen so far.

Review by The Hon. F. M. Neasey AO, Research Fellow, University of Tasmania.

COMPUTER LAW

Chris Reed (Editor), (London, Blackstone Press Limited) (1990) 267 pages plus index, £17.95 (U.K.)

Not being a particularly good traveller and usually unable to read or sleep on long flights, I nevertheless decided to read this book on an 8 hour flight from Sydney to Hong Kong. I should also mention that at the time of reading I had almost finished my lectures in a Commercial Law course which I teach at the University of Tasmania Law School. To my pleasant surprise, *Computer Law* held my attention the entire time. For commercial lawyers especially, it is an absorbing and timely work which applies the general principles of business law specifically to the purchase, sale and use of computers.

Included are chapters on hardware contracts, software contracts, liability for computer software, copyright, patentability of computer software, design protection, protection of confidential information, computer crime, computers and evidence, data protection, expert systems and EEC computer law.

Although this work focuses primarily on English and EEC Law, there is also a liberal use of cases and legislation from other jurisdictions, most notably the United States. The result is a work which will have wide appeal to most people involved in the computer industry regardless of jurisdiction.

The timeliness of such work is articulated by editor Chris Reed who notes in his introduction,

> '. . . it is only since 1984 that interest in the subject has grown to the extent that courses are now offered to students and major law firms have set up information technology departments. Journals such as *Computer Law and Practice* and *Computer Law and Security Report* deal exclusively with matters in this area, and books on specific aspects of the field are becoming increasingly common.
>
> This increasing interest in computer law derives from the rapid advances in the information technology industry. Computing has changed from an arcane art practiced in isolated and air-conditioned rooms in a few large companies to an activity that will soon be carried out by the majority of the population, and even now affects the lives of every one of us . . . It has been said that we are moving into the 'information age', where the processing and dissemination of information made possible by computers represents the true possession of wealth.[1]

Although *Computer Law* is divided into a number of discrete topics which stand alone in their own right, the work is united by a number of important themes or conflicting tensions which characterise this rapidly growing area of the law. As discussed in Mr Reed's introduction, included among these themes are:

---

1 at 1-2.

- *'Information or knowledge as a species of property.'* The patentability of computer software, problems of reverse engineering, the protection of computer chip design etc are just a few of the challenges which information technology presents to traditional notions of property law.

- *'Privacy versus the dissemination of information.'* As huge and increasingly sophisticated data bases are being formed to perform tasks previously thought impossible, they also bring with them new and real threats to the invasion of privacy. This is especially so in areas relating to medical records, credit reports, and the reporting requirements imposed by governmental agencies.

- *'Information technology as a substitute for human endeavour.'* Increasingly, computers are assuming functions (medical diagnosis, purchase decisions, weather predictions etc) which previously would be performed by a human agent. This situation gives rise to the question of who is liable in these contexts. Also, consumers' increasing expectations of computers are also challenging traditional notions of liability.

- *'Trading in information products.'* The trade in information products has also challenged traditional commercial law. For example, is computer software a 'good' so as to be regulated by Sale of Goods legislation? What about a mixed package of hardware and software? Should courts and legislatures tackle these problems by expanding existing laws or create a new legal regime to deal with such products?

- *'Harmonisation of national laws.'* Information technology has rapidly become an international area of trade. Accordingly, licensing and other arrangements will be more effective to the extent that national laws are made uniform. Indeed, the demands of the computer industry have placed enormous pressure on governments to harmonise their laws in this important area of commerce. A good example of such harmonisation is the publication of recent EEC Privacy Directives.

In summary, *Computer Law*, edited by Chris Reed, provides a very useful and readable guide to the legal issues raised by information technology.

Review by E. Eugene Clark, Lecturer in Law, University of Tasmania.

THE LAW OF ELECTRONIC COMMERCE: EDI, FAX, AND EMAIL: TECHNOLOGY, PROOF, AND LIABILITY

Benjamin Wright. Boston, Little, Brown and Company (1991) 432 pages, including glossary and index, $42.00 (U.S.)

This book, written for lawyers and business people alike, examines the legal and practical implications emanating from the use of electronic messaging technology. The major thesis of Wright's book is that 'if implemented intelligently, electronic communication can confidently be used for legal transactions. It rejects the attitude that technology deserves suspicion.'[1]

The Law of Electronic Commerce is divided into six major parts. Part I introduces various electronic technologies and discusses their application in a broad range of business settings. The technologies include fax, email, telegraph/telex, electronic data interchange (EDI) and electronic funds transfer (EFT). EFT's are of course used widely in modern banking systems. I found the discussion of EDI's to be especially interesting. EDI's involve the 'movement of electronic business messages, such as purchase orders, from computer to computer.'[2] These messages are structured and coded in such a way that the receiving computer, without the aid of human intervention, can immediately transfer it to a wide range of accounting and inventory management software. Indeed, the author suggests that in the near future interactive EDI's will be programmed so that computers themselves will be able to negotiate, initiate offers and counter-offers, and make acceptances. Chapter 3 discusses the 'players' (each of whom would have an interest in reading this book), who will have a major stake in the use of these new technologies. They include information systems professionals, consultants, user managers, attorneys, accountants and auditors and record retention managers.

Part II considers the practical risks and trustworthiness of electronic commerce. Wright's argument here is that '[O]ne cannot dismiss an electronic transaction application just because the controls that may practically be imposed on it are imperfect. The typical controls over paper documents are imperfect too.'[3] The author notes that electronic media are increasingly being used and accepted in legal settings. For example, the Federal Communications Commission in the US permits signed petitions, leadings and briefs to be filed by fax and the US Patent Office accepts certain patent application documents by fax. The remaining chapters in this part also discuss how documentation authentication, security and the design records for audit can all be achieved using electronic commerce.

---

1 at xxvii.

2 at 9.

3 at 45.

Part III deals with legal proof issues and is especially relevant for lawyers. While the law is almost exclusively based upon US examples, the issues considered should nevertheless be of interest to lawyers generally, and especially those in common law countries. Amongst the topics discussed are: the admission in court of electronic records; authentication of electronic evidence and how to establish authenticity; the hearsay rule and electronic messages; and the best evidence rule and electronic messages.

Part IV is concerned with the legal requirements of record keeping and internal control, ie 'the presence of procedural safeguards to ensure transaction authorisation, correctness, completeness, efficiency, and consistency with management policies.'[4] The purpose of such controls is to deter fraud, correct errors and permit proper evaluation of business progress by management and auditors. Again, the examples are largely from the US and include a discussion of legal record keeping and control requirements under the Foreign Corrupt Practices Act, Federal Income Tax Act and other regulations governing financial institutions, commodities trading, transportation carriers and customs. From a comparative perspective, there is a brief discussion of tax record keeping experience in other countries and a report of the Trade Electronic Data Interchange Systems programme under which the EEC sponsored a study of the legal obstacles to EDI in member states. A special section also addresses the problem of electronic fraud and the civil and criminal responses to the problem.

Electronic Contract Issues are focused upon in Part V and the development is made especially interesting because of the inclusion of a considerable amount of comparative material. Central to the discussion are various model codes of conduct which have been created to cover trading partner agreements. These include the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UNCID) developed through the joint efforts of several international organisations and published by the International Chamber of Commerce. While the UNCID has had little following in North America, it has become a usage or trade custom elsewhere. According to Wright the UNCID requires that EDI users:

1. abide by their chosen EDI standard;
2. communicate with care;
3. instruct networks not to change messages without authority;
4. properly identify themselves in messages;
5. acknowledge or confirm good receipt when requested to do so;
6. take remedial action if a received message is not in good order or wrongly delivered;
7. maintain the security of protected data;

---

4 at 168.

8. keep an unchanged log of exchanged data;

9. designate a person to certify the log; and

10. refer questions of UNCID interpretation to the ICC.[5]

North American traders are more likely to utilise either the American Bar Association Model EDI Trading Partner Agreement or the Canadian Model Form of EDI Trading Partner Agreement. In the UK, the EDI Association has developed a Standard Electronic Data Interchange Agreement (2d edition) in August 1990 which in most respects follows rules similar to the UNCID. Of course, many businesses elect not to follow a model agreement. An alternative is to draft their own agreement or to adopt a more informal 'electronic trading letter' which tends to be briefer than a model agreement and focuses only on primary issues. Illustrating the practical aspects of this publication, a sample letter is contained in the appendix. Other contractual aspects dealt with in this part are the trading partner relationship, mailbox rule or postal acceptance rule, delivery rules, statute of frauds and enforceability rules and problems connected with the battle of the forms.

The final part of the book turns to the topic of network service providers and customers. The main issues discussed are liability for deficient service and data protection. Legal liability issues include warranty, disclaimers, force majeure clauses, negligence, and other statutory bases of liability on the part of network providers. Data protection issues emphasise predominantly US legislation and constitutional guarantees regarding privacy and confidentiality.

Finally, the appendix contains some very helpful practical information including suggestions for using fax machines, EDI and similar technologies for legal purposes, as well as some sample contractual documents which might be used by trading partners. There is also a useful glossary of technical terms. The layout and presentation of the book, with its clear diagrams and useful references, also contribute to its readability and value .

In sum, considering the technical nature of the subject matter, this is a highly readable book which should appeal to a broad range of readers. While it is aimed primarily at the North American market, the concerns and issues raised should be of interest to anyone involved in the world of electronic commerce.

Review by E. Eugene Clark, Lecturer in Law, University of Tasmania.

---

5 at 237.

THE COMPUTERISED LAWYER: A GUIDE TO THE USE OF COMPUTERS IN THE LEGAL PROFESSION

Philip Leith. Springer-Verlag, London, Berlin, Heidelberg, New York, Paris, Tokyo, Hong Kong (1991) 217 pages including index, £17.95 (U.K.)

This excellent book discusses the impact of the computer on the legal profession. The first four chapters provide a valuable and highly readable introduction to computers generally. This is especially useful to lawyers and/or students new to the area. Chapter 1 explains and illustrates the concepts of algorithm, 'a sequence of instructions for carrying out some process step by step.' (p. 5), computer hardware, peripherals, diskettes, computer programs etc. The author is to be commended for explaining these concepts in plain language, making good use of several illustrations.

Chapter 2 considers the rapidly expanding area of computer communications. For lawyers the type of communications include: 1) access to central information held on a large mainframe, eg LEXIS, various credit reference systems, and various computerised government systems; 2) access to central in-house systems, eg in-house data bases, client records; 3) videotext and teletext information services, eg those which provide information on markets and other financial information; 4) document passing, eg between lawyers in different practices and 5) electronic mail. The chapter also describes the various means of transmission and raises the issues of data security and viruses. The author quite rightly suggests that these and future developments in communication hold the potential to change the very way we think about law. This is because law itself 'is an institution built on the creation, storage, processing, and communication of information.' (p. 51, citing Katsh, *The Electronic Media and the Transformation of the Law.*

Chapters 3 and 4 continue to explore the application of the computer to the work of the lawyer. Data processing, data bases, searching , informational retrieval and indexing are all discussed. Especially interesting is the section on hypertext. Hypertext 'is a means of having blocks of text interconnected, so that we can move - at random, and at will - from one piece of test to another.' (p. 93). Thus, one can move from the legislation to look, for example, at cases interpreting a particular passage, legislative history, and relevant articles. In Australia, Graham Greenleaf of the University of New South Wales has done some pioneering work using hypertext to develop a package concerned with privacy legislation. Brent Fisse of the University of Sydney has done the same with the *Cash Transactions Reports Act.* Such projects offer great potential as a legal and training resource for lawyers and other professionals working in the area.

Chapters 5, 6 and 7 discuss a variety of current applications in law. These chapters, especially, illustrate how rapidly this area is expanding because several new developments have occurred since the book's publication. Chapter 5 treats primary legal information retrieval. Leith illustrates the chapter by a detailed discussion of LEXIS and to a lesser extent WESTLAW. The author also notes, that while the use of full text legal data bases such as LEXIS has not caught on as fast as experts predicted, their growth has

nevertheless been significant. Also, lawyers are finding increasing uses for such data bases, most notably cite checking and downloading and print facilities. Thus, for example, in the US, state legislation is now routinely made available on disk form so that lawyers can cut and paste the relevant statutory sections into a case brief or other document on which they are working.

Chapter 6 introduces the topic of secondary legal information retrieval. Included in the discussion is in-house information retrieval in which full-text or relational database techniques are used to store and search through a legal practice's own collection of precedents and other written materials. Leith also discusses litigation support packages used to help the lawyer manage a case in which there are a large number of documents. Finally, he discusses other legal research systems which are on-line and provide information and advice to lawyers rather than providing primary legal materials. Examples of such systems are *Compu-Mark* which carries out searches of trademarks, *ABA/net* designed by the American Bar Association for the legal profession, and *Lawtel* which provides summaries of cases, statutes, indexes to law journals etc. Other *utilities* specifically designed for lawyers are also mentioned, eg *Checkcite*, *CiteRite*, and *Fullauthority* which are all used to ensure that authorities in documents are properly cite; and *CompareRite* which is used to check two documents and underline any differences between them. Still other packages enable the lawyer to computerise diaries, notebooks, phone lists and so on.

Chapter 7 surveys legal office and court systems. Leith makes the important points that: 1) there is a severe shortage of systems analysts who are specifically experienced in designing systems for legal settings; and 2) that it is critically important, in purchasing a system to seek professional advice from one experienced with legal settings. If possible, it is also a good idea to talk to other law firms who are using similar systems. The reason for such caution is that such systems represent a substantial purchase and many small businesses have met with disaster when purchasing off-the-shelf products without giving due consideration to the suitability of the system purchased. Courts especially, which must of necessity handle large numbers of cases and documents seem ideally suited to computer applications; and numerous packages to handle jury selection, computer-aided transcription, court records, scheduling, case flow and other tasks have been developed and continue to expand. The author by his own admission suggests that a future edition of this work greatly expand this chapter; and I would suggest that so great has been the recent expansion in this area that time has already arrived.

Finally, Chapters 8 through 10 deal with the topic of artificial intelligence in the law, again another area in which rapid developments are occurring all the time, as evidenced by the Third Conference on Artificial Intelligence and the Law held in July 1991 at Oxford. There is little doubt that artificial intelligence programs in law have not lived up to the claims made by some of their early proponents. The reasons for this and the philosophical debate underlying the quest to develop such artificial intelligence systems are discussed. For an extension of this debate, readers are referred to the article by Bob Moles in the previous edition of this Journal

as well as the article by John Zeleznikow and Daniel Hunter in this present edition.

Given the increasing impact of technology on the Legal Profession, *The Computerised Lawyer* is an important and timely work. It will be of interest both to lawyers and legal educators who want to familiarise themselves with computer applications in the law firm. It will also be of interest to computer specialists seeking an excellent case study illustrating the application of computers to a particular profession.

Review by E. Eugene Clark, Lecturer in Law, University of Tasmania.

THE LEGAL ENVIRONMENT OF COMPUTING

Peter Knight and James Fitzsimons, Addison-Wesley, 1990, 354 pages, $34.95.

The authors of this book, Peter Knight and James Fitzsimons, are partners of the Australian law firm of Abbott Tout Russell Kennedy and both have wide experience in technology law. Peter Knight is also seconded to Apple Computer, Inc. as its senior counsel for Asia-Pacific Operations. This is an Australian book by Australian authors, but there are many examples relating to generally accepted legal principles and the law in other countries.

This is a book for computing professionals rather than lawyers, although it would be useful to lawyers learning about the computing industry. To this end, the authors provide an introduction to basic computing technology, programs and semiconductor chips.

According to the authors in the preface, this book

> "... is about legal issues relevant to the computer industry, based on a great body of well understood law but applied to a new industry, the computer industry, and its products. In essence it is made up of the answers the authors have given to questions asked over and over again by people in the computer industry."

This gives the reader a good idea of the flavour of the book. Many of the chapter subheadings are in the form of a question. For example, *"Employees and Contractors -What's the difference?"* and *"What is copyright?"*, *"When is information regarded as confidential?"* and so on. As a computing professional I found the answers to many questions I have often been asked to consider in the course of my working life. Other sections come under subheadings defining common legal terms. For example, *"Defamation and injurious falsehood"*, *"Injunctions and other mandatory orders"*, *"Consideration"*, *"Mitigation of loss"* etc. Also, throughout each chapter there are a number of illustrative hypothetical examples dealing with typical scenarios in the computing industry. For example, from chapter 10, Antitrust - Competition Law:

> **"Trade boycotts/'exclusionary provisions'**
>
> 'Exclusionary provisions' are agreements whereby competitors agree that none will supply goods or services to, or obtain goods or services from, certain people or types of people. These sorts of arrangements, classically market or customer sharing deals which are the special target of the Sherman Act, may include much more common occurrences, such as the following.
>
> *Example*
>
> *The credit controller of ABC Computers is very concerned regarding the increasing debt of one of its dealers, XYZ. He telephones a friend at DEF Systems, a competing hardware supplier, and explains his concern, asking whether DEF Systems has the same problem. Together, they agree to put pressure on*

> *XYZ: ABC Computers will supply XYZ on a cash basis as long as DEF Systems does the same.*
>
> *Clearly this is an illegal arrangement and the employers of both credit controllers would be liable to penalty (as well as civil action from XYZ). Had ABC Computers made the decision on its own, it would not be a breach of this prohibition, but it would have faced the risk that XYZ would simply shift its purchases to DEF Systems."*

Examples like this make this book very easy to read and understand for a computer professional with no legal training.

The book has basically three sections. The first section, *Summary of Legal Issues,* is in the form of chapters covering: Introduction (including "How the law works"), Employees and Contractors, Copyright, Other Forms of Protection, Confidential Information and Trade Secrets, Unfair Competition and Trade Mark Law, Contracts, Mistake and Misrepresentation, Negligence, Antitrust-Competition Law, Data Protection, Privacy and the Freedom of Information.

One question that is always of particular interest to computing professionals is "what is considered to be professional negligence?". The chapter on negligence in this book is very useful. The authors first define negligence in common law as "conduct which has 'accidentally' caused harm". Furthermore, they state that:

> "With the growth in the application of the law of negligence, so has it become more important to carefully define its limitations. For example, it was initially only negligence that resulted in physical injury to goods or person that gave a right of action in the court - 'mere' economic loss would not entitle a person to compensation. The development of the law away from this limitation is one of the greatest importance, which we will examine later. In addition, one can only sue the actual or real causer of injury - if a person is the mere vehicle of someone else's fault (for example, is forced into doing the wrong which resulted in injury) then one must sue that other person, provided he or she is not too 'remote'. Finally, it is not any behaviour resulting in injury which is 'negligent' for the purposes of gaining compensation: a mistake is not always a negligent mistake."

The authors go on to define terms (including examples) appropriate to the law of negligence including "duty of care", "standard of care", "proximate cause" and foreseeability". The second half of the chapter deals with the concepts of "Negligence and self preservation", "'Mere' economic loss", "Vicarious liability" and a mention of insurance. Included here is the example of *Mackenzie Patten v British Olivetti* and a discussion of the litigation involving alleged defects in software in the Lotus 1-2-3 spreadsheet package.

The second section, *Sample Contracts,* takes the reader step by step through some typical contracts that they may encounter in the computer industry. There are eighteen of these examples and include: Boilerplate clauses, Software Maintenance Agreements, Hardware Purchase Agreements,

Assignment of Copyright, Software Distribution Agreements, and many others.

A third section contains four appendices of signatories of copyright conventions and the International Contract Convention and membership of the International Patent Cooperation Union and the Paris Union.

In summary, this is a very useful and readable book for any computer professional or senior student of computer science and would be a very good reference or text book for a tertiary course in computer science or information management.

Review by Linda Dawson, Lecturer in Computer Science, University of Tasmania.

COMPUTERS, ARTIFICIAL INTELLIGENCE AND THE LAW

Mervyn E. Bennun (Editor), England: Ellis Horwood Limited, 1991. 132 Pages Inc. Index, £24.95.

This book contains six chapters, each of which probes the social implications that underlie the extensive research efforts which are currently being undertaken into the application of AI techniques in the legal domain. The cautionary approach adopted by this book stands in contrast to the often unrealistic and overenthusiastic claims which have previously been espoused for legal expert systems.

Blay Whitby sets the general tone of the book in the first article entitled 'AI And The Law: Proceed With Caution.' The chief problems addressed by Whitby in this chapter are de-skilling, lack of awareness by computer scientists of the social consequences of their work, and the hidden effects of shifting constitutional power caused by the introduction of AI-based systems in the legal domain.

While some successful expert systems have been implemented, Whitby asserts that researchers have typically been more interested in solving theoretical problems than in producing commercial systems. He states that the immediate consequence to the law may be in the development of ideas and methodologies rather than in the form of working technology. These changes are largely occurring with little comment or even recognition by the legal profession. The imposition of new ideas by computer experts on the sole basis of technical expediency requires that the legal profession "fully examine the developments and to ensure that they are generally beneficial."[1] Similarly the effects of 'social feedthrough' should be carefully considered by AI researchers who should accept responsibility for the fact that:

> "The technical considerations involved in the design and production of a piece of technology have an important influence over the social implications of the general use of that technology."[2]

However the legal profession should not reject these developments outright. Instead, Whitby urges that AI specialists should adopt codes of good practice and software standards, and recognise the social consequences of their actions. He believes that the reticence of computer scientists to adopt such measures will ultimately leave the legal profession with the central responsibility.

The author also warns that the introduction of AI-based technology may result in employee de-skilling effects similar to that which occurred in the manufacturing sphere. Trained professionals may find themselves reduced to the level of technician. Assumptions that lead to de-skilling could be avoided. He believes that researchers should adopt the approach becoming

---

1 p. 5.
2 p. 9.

popular in computer based education, namely that it is more useful to design legal-aids rather than computerised lawyers.

Legal expert systems have typically been applied to statues of a highly specific and self-contained nature. Questions of social consequences have been avoided by tackling legal areas that contain little ambiguity or whose interpretation have been limited by the inclusion of ouster clauses. Expert systems, it is asserted, may be an even more effective means than ouster clauses in permitting the legislature to circumvent the judiciary.

The second article written by Jan Goossenaerts and Johan Lewi differs from the generalised approach of the rest of the book by dealing in depth with a modelling technique that emphasises the representation of real-world institutions. The stage-prop-actor network (SPAN) method developed by the authors provides a framework for reasoning about organisations and their activities. This system may assist in the modelling of rule-governed organisations by permitting the rights and duties of individuals to be inferred from the legal entities that relate to the organisation.

SPAN is a development of semantic networks which provides enhanced conceptual support over traditional object-oriented languages and offers richer primitives than frame-based approaches. The system allows for consistent rule updates, improved rule comprehensibility, provides inherent security features, and defines pre and post conditions on the state of the knowledge system. The SPAN method allows knowledge to be extracted from sources and to structure this so as to reflect the structure of the organisation from which is was developed. In this way it attempts to limit the breakdown of context which occurs in formulating a knowledge representation.

The detailed descriptions presented in this chapter would perhaps only be of interest to researchers who are active in the field. The authors admit that SPAN does not offer the "plurality of views that is so typical of legal activity, both in case-based law, and in law that is based on a set of mutually referring rules."[3] The difficulties of developing a conceptual schema for legislation are acknowledged and short of urging "the legislator to be explicit about all the rules and to consider the interaction of all members of an organization with the rules"[4] the SPAN method seems to offer little to the process of legal analysis.

Some of the problems associated with implementing legal reasoning on a computer are addressed in the article by Peter Sparkes entitled 'Artificial Intelligence Models Of Legal Reasoning'. The author commences his discussion by reviewing whether AI systems should represent the law "derived from its sources or upon the law as interpreted by expert practitioners of the law"[5] The decision is between rule-based approaches and heuristic re-interpretation. The best approach would depend upon the needs of the individual user.

---

3 p. 37.
4 p. 34.
5 p. 41.

The fundamental question of whether the law may be reduced to simple rules is addressed by Sparkes. Reducing statutory provisions to the restrictive format required by computers (such as decision trees) must introduce at least subtle changes in context. Sparkes states that "if such reduction is not possible in all cases, and that must be the suspicion, then the issue of the technical feasibility of computerization remains at large."[6]

The assumptions underlying traditional legal research tools tend to be both visible and verifiable. However, in the case of computer-based systems (in particular the inference engine of an expert system), the "unarticulated assumptions will, if inaccurate, compromise the validity of the legal adaption."[7] Expert systems attempt to overcome this problem by introducing 'transparency'. Just as a legal professional supports his reasoning with relevant authorities, so one of the strengths of expert systems is their ability to explain their reasoning so as to justify their advice. However in light of inaccuracies in the knowledge base, such as missing or unused (though relevant) authorities, such self-validation may be misleading. As Sparkes states:

> "Such errors are wholly undiscoverable, except by a person who is already so expert that they could derive no benefit from the use of the expert system. The object must be to disseminate an expert's expertise and not simply to play to an already expert audience".[8]

The 'principles' that underlie the law are what determine the outcome of novel cases. That concepts such as 'reasonableness' defy computer representation is perhaps a reflection of the fact that the determination of many decisions is not possible until they have been tested in case law and adjudication passed. The usefulness of fuzzy logic in this area is rejected on the basis of the inherently qualitative nature of the law with the accuracy of probabilities being necessarily vague.

To attain accuracy in the legal domain it is generally necessary to use the text of legal materials for the knowledge database. Sparkes uses the example of conveyancing law as an example of a field not directly based upon its case-law. It is argued that to accurately portray such an area would require the use of a largely heuristic system. It is well beyond the scope of current systems to reason from statutory materials, yet the reformulation of statutory material for computer representation can compromise its meaning. It is argued that the cost of maintaining a consistent legal expert system in a dynamic area of law may be prohibitive. The author concludes that the significant problems facing computer-based legal reasoning would severely limit the usefulness of legal expert systems and instead urges the investigation of specifically targeted decision support tools and training systems.

Chapter 4, 'Computerising Criminal Law: Some Basic Problems' by Mervyn E. Bennun, considers elements of criminal law that may pose specific problems to implementing decision-support systems. Particular

---

6 p. 44.
7 p. 46.
8 p. 48.

emphasis is placed upon the nature of the mens rea and its relationship to 'fault'. Attention is drawn to the difficulties in analysing strict-liability crimes where there is no explicit mens rea. A section that is silent as to mens rea requires the circumstances outside the act to be considered before determining liability and it is at this point that expert systems encounter difficulties.

Bennun asserts that the determination of general rules that may be embodied in an expert system is made impossible by the shear number of statutory offences in which no explicit mens rea is stated. In such situations the principles of statutory interpretation are so unclear that it is not possible to predict what outcome will be likely for any given case. Given the open texture of the language and the unpredictability of human nature, the author argues that the process of human adjudication will always be required in legal reasoning. The author concludes:

> "Increasing the power of the inference engine will increase the sheer volume of data which can be taken into account - both in terms of the complexity of the facts and the range and complexity of the rules surveyed - but cannot solve problems which require the human mind."[9]

In Chapter 5, 'How Long Is A Piece Of String: Exploring The Hidden Agenda Of Rule Based Systems', David Cairns and David Marshall continue the discussion on the difficulties in formalising legal expertise and reasoning for computer representation. They note that computers deal with *data* not *information*. Computers may only make symbolic changes to data under the direction of human supplied rules with no meaning or context being associated with these rules. The attribution of meaning to the output is performed by the recipient of the data. On this basis the current state of natural language processing is critiqued for handling only elementary denotative meaning rather than the richer meanings implied by semiotic theory. The authors believe that:

> "Expertise resides not solely or even mainly in technical knowledge but in the heuristics of its application."[10]

The authors emphasise the requirement for reasoning-transparency, as also raised in the earlier chapter by Sparkes. This is required to permit the determination of the systems reliability and the degree of authority to be placed in the machines data and decisions. They warn that the lure of algorithmic rather than heuristic reasoning may result in the implicit adoption of expert systems as a measure of the performance of traditional tribunal systems. They argue that lawyers engage in complex semiotic analysis by considering all relevant information "including all those matters that the client has communicated by inference or silence."[11]. The inability of expert systems to deal with such problems limits their usefulness to only the most routine of cases. Such systems may therefore have little significance to lawyers.

---

9 p. 74.
10 p. 86.
11 p. 85.

The final chapter, 'Realism, Responsibility and Rationality' by Julie Browne and Andrew Taylor, focuses upon the reasoning behind the design decisions made by the authors in implementing a decision support system for Adjudication Officers in the field of social security. Their approach does not stem from the theoretical debate over the adequacy of logical models of legislation nor the suitability of a rule-based approach. Instead the authors considered the needs of Adjudication Officers and the capabilities of existing technology to assist in improving the standard of decision making. They observe:

> "The designer of a system has to concentrate on what it is that the users need in order to do their task more effectively, not on some detached model of 'legal knowledge'."[12]

The main aspects addressed include creating and maintaining a large legal database and the issues of the practical, organisational and social implication of introducing a decision support system. This chapter provides an interesting look at how the criticisms raised elsewhere in the book have been dealt with in the development of a working commercially viable system. The problem of avoiding de-skilling, the difficulties of what should be included in the knowledge base, the legal status of the system, its effects upon the organisation, the social impact of the system and the responsibilities of its designers are all addressed.

In conclusion, AI techniques have the potential to produce significant changes in both jurisprudence and legal practice. The contributors to the book recommend that AI experts should not design systems that de-skill or threaten the responsibilities of their users. They urge that the implicit constitutional changes that may result from the technical decisions of scientists should not go unchecked without public debate. It may therefore be necessary for legal professionals to acquire an understanding of the problems and potential of AI. This book is commendable for raising these important issues, with its central ideas being significant to both lawyers and AI researches alike.

Reviewed by Peter A. Jones, Computing Systems Officer, University of Tasmania.

---

12 p. 117.