FOR REFERENCE ONLY

Data Communications Security
- Legislating and Contracting for Legal Security -

Ian Newark Walden

A thesis submitted in partial fulfilment of the requirements of the Council for National Academic Awards for the degree of Doctor of Philosophy

June 1992

Nottingham Law School, Nottingham Polytechnic

PKO SLC

cp_//wfy_ Ref.

The integration of computer and telecommunication technologies, `telematics', has enabled organisations to communicate electronically. The benefits of such data communications can significantly facilitate trade, particularly within the global economy. However, the widespread and successful adoption of such communication systems depends on users having confidence in their secure operation. The three components of such security are confidentiality, integrity and availability. Although attention is increasingly being paid to the technical aspects of data security, the thesis addresses the critical complementary legal aspects of achieving security in data communications. The legal security issues impose obligations, as well as protection, for companies communicating electronically. The thesis discusses the role and impact of legislation as a means for controlling the use of telematics. Current commercial legislation can restrict the use of telematics, or fail to extend existing protection, due to the paper-based assumptions upon which past legislation was drafted. The impact of recent legislative initiatives, addressing the security issues for data communications, are discussed in the context of the conflicting interests involved. Currently, legislative sources of data security regulation are not significant. The thesis argues that companies need to focus on their contractual agreements as the primary, or as an alternative, forum within which to construct a legally secure framework. The thesis considers two primary contractual relationships that concern a data communications user: the rules and procedures for exchanging data with trading partners, and the agreement with a supplier of the communications network. The thesis concludes that to facilitate telematic security, requires critical consideration to be given to the legal aspects of confidentiality, integrity and availability.

To my Mother and Father

For their support and encouragement of this work, I would especially like to acknowledge my supervisor, Professor Nigel Savage, Nottingham Law School and Tarlo Lyons.

CONTENTS

III **The Legislative Framework**

4. Data Protection

4..1 Definitions
4..2 The scope of data protection legislation
4..3 International law
4.3.1 Council of Europe
4.3.2 OECD
4.3.3 The United Nations
4.3.4 The European Community
4.3.4.1 Background
4.3.4.2 Draft Directive
4.3.5 The Data Protection Principles
4.4 National data protection legislation
4.4.1 International data transfers
4.4.2 Data security
4.4.3 Legal persons
4.5 Impact on the private sector
4.5.1 International data transfers
4.5.2 Data security
4.5.3 Legal persons
4.6 Developments in data protection
4.6.1 Technological developments
4.6.2 Self-regulation/differentiation
4.7 Comment

5 Commercial Law Framework

5.1 The Paper Environment
5.1.1 The legal nature of communications
5.1.2 Statutory requirements
5.1.2.1 Document
5.1.2.2 'Writing'
5.1.2.3 Signature
5.1.2.4 Contract Formation
5.1.2.5 Negotiability
5.1.2.6 International trade law
5.1.2.7 Comment

5.2 Evidential Issues

5.2.1 Record maintenance
5.2.2 Admissibility
5.2.3 Integrity and Authentication
5.2.4 Comment

IV **Contract Law**

6.1 Contractual relationships
6.1.1 Form of contract
6.1.2 Private international law
6.1.3 Comment
6.2 Data protection contracts
6.2.1 The issues
6.2.2 Draft terms
6.2.3 Comment

Chapter 1 **INTRODUCTION**

1.1 Introduction

"Information is power, and economic information is economic power."[1]

The so-called `information revolution' has been described as the third major revolution to fundamentally alter the way human societies operate; the previous revolutions being agricultural and industrial[2]. One distinctive element in this current period of rapid development is the means by which information is communicated.

Communication is the "imparting or exchange of information"[3], and it is the technological developments in the means of processing, storing and distributing information that have contributed to the increasing value of information as an economic resource. The key technological development of the information revolution is, of course, the computer, in its seemingly ever-expanding number of manifestations, from ATMs to washing machines.

This thesis deals with a particular aspect of the information communication revolution[3a] : the impact of law on the use of commercial data communication techniques[4]. The law can both restrict the use of data communications techniques, by regulating certain types of data transfers; or protect such systems, by enabling users to take legal action against infringers. Throughout this thesis, the term `legal security' will be used to describe both these aspects.

The central focus of this study will be an analysis of specific legal issues that arise through the use of data communication systems, and a consideration of the use of contractual

---

[1] Statement of Louis Joinet, French Magistrate of Justice, at the OECD Symposium on `Transborder Data Flows and the Protection of Privacy', Vienna, 1977.

[2] For a general discussion of this phenomena see Saxby, S., *The Age of Information*, Macmillan Press, 1990.

[3] Oxford Dictionary. This definition obviously includes broadcasting and other predominantly one-way communication technologies, however, the thesis will focus on two-way communication techniques.

[3a] This era has also been labelled simply the "communications revolution": Robert Murdoch, quoted by John Pilger, *The Guardian*, p23, 14/9/92.

[4] See Chapter 2 for a general review of such technology.

provisions to overcome legal obstacles and ensure a `legally secure' environment; thereby facilitating the use of data communications techniques.

1.2 The Subject

> "Crucial to managing international operations is the availability of accurate and timely information.."[5]

The growth of telecommunications and computing, known collectively as `telematics'[6], has enabled businesses to establish new means of managing their information flows, internally and externally, nationally and internationally. The essence of `data communications' is that information is transferred in a machine-readable form[7].

Electronic alternatives to traditional paper-based methods of communication offer users substantial benefits, not only in terms of cutting the cost of administration, but also in accelerating the whole transaction chain. More efficient business practices facilitates trade by providing room for trade to expand; while, the use of data communications can also enable companies to offer new types of goods and services. As a consequence, commerce can become dependent on computer systems and telecommunication links to an extent that it never did on older techniques, such as telex[8].

The most recent manifestation of `telematics' is the development of Electronic Data Interchange (EDI)[9]. EDI is a more sophisticated mode of data communications to batch file transfers, replacing standard paper documentation, such as an invoice, with structured electronic messages. EDI facilitates trade, particularly international trade, where traditional paper documentation represents a significant percentage of the value of a product, and creates a major source of inefficiency.

---

[5] Kelly, Michael, `Surveys Show Strategic Importance of TDF', p20, *Transnational Data Report*, vol.VII, no.1 [Jan/Feb 84].

[6] `a French term coined to describe the combination of computers and telecommunication networks' *Dictionary of Information Technology* (3rd Ed), Macmillan 1989. `Teleinformatics' is an alternative term; see Eger, "The Global Phenomenon of Teleinformatics: An Introduction", pp.203-234, 14 Cornell International Law Journal, 1981. Throughout this thesis, the terms `data communications', `transborder data flows', `electronic data interchange', `electronic messaging systems' and `telematics' should be considered to be interchangeable. The thesis will not be considering voice telephony, telex or fax, since they are not generally machine-readable. However, even in these areas, technological developments, such as fax cards for the PC, can mean the removal of the paper interface.

[7] `Data' is a particular means by which information is both held and communicated: "Programs, files or other information stored in, or processed by, a computer system"; Dictionary of Information Technology [3rd ed.], Macmillan, 1989. See also Seipel, P., *Computing Law*, LiberFörlag, Stockholm, 1977: "A representation of facts, concepts, or instructions in manner suitable for communication and processing by...automatic means". The UK Data Protection Act 1984 defines `data' as "information recorded in a form in which it can be processed by equipment operating automatically..", at s.1(1). Sizer, R. and P. Newman, define `data' as a "means of communication of information", in *The Data Protection Act 1984*, Gower, 1984. The term `electronic communications' will also be used in the thesis, however, it should be seem as interchangeable with `data communications'.

[8] See Bergsten, E., "Trade Data Transmission: A Uniform Code (UNDID) - The Challenge for the drafters", p.6, The Computer Law and Security Report, vol.3, no.3, 1987.

[9] See further Chapter 2, at 2.2.4.

This thesis is primarily concerned with data communications between legal entities, whether commercial or regulatory. It will not be concerned with data communications that arise through direct interaction with individual consumers, such as teleshopping and videotex services[10]; nor with communication networks internal to an organisation, except to the extent that they raise common legal issues.

1.3 The Law

This thesis will focus on three major legal issues in data communications:

- Legislation which imposes security obligations and restrictions upon the use of data communications[11];
- Legislation, regulations and administrative rules that inhibit the use of data communications because the terminology within which they are framed presupposes a paper-based environment[12];
- Contractual means by which trading partners can surmount the restrictions imposed by the current legal framework, and establish `legal security'[13].

Data protection legislation is an example of `sui generis' UK legislation, aimed at controlling the use of `telematics'. Although data protection legislation is intended primarily to protect the subject of the communication, it is also fundamentally concerned with the need to ensure the integrity and security of data. Data protection concerns are also an example of the need for international harmonisation of legislation when attempting to regulate an international technology.

Computer misuse legislation is another example of a statutory initiative that has arisen out of concern for the consequences of the spread and penetration of `telematics' into organisations. Over recent years, the industrialised nations have recognised and promoted the need to offer data users the protection of criminal law against those wishing to interfere with IT systems[14]. Such legislation has, however, only recently been passed in the UK, and therefore its impact has yet to be fully and adequately assessed[15].

The second legal concern is the potential restrictions that the traditional commercial-legal

---

[10] See generally, Poullet, Y. & G.P.V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law*, No.1 Computer/Law Series, Kluwer/The Netherlands 1988.

[11] See Chapter 4. See also Chapter 3.

[12] See Chapter 5.

[13] See Chapter 6.

[14] See Chapter 3, at 3.4.3.

[15] See Chapter 3, at 3.4.3.2.

framework poses for the acceptance and effective exploitation of telematic techniques: For example, requirements for documents to be `in writing' or `signed' and the requirements of statutory authorities for the presentation of paper-based information in compliance with specific regulations.

The legislative framework has always, inevitably, lagged behind developments both in technology and business practice; however, this lag can create serious obstacles to the use of data communications. Many companies, most notably in the US, continue to send paper documentation as a back-up to the electronic messaging systems, because of a perceived uncertainty regarding the acceptability of electronic records in court[16].

Legislation designed to regulate data communications, and legislative requirements that fail to accommodate the use of such technology, give rise to legal security concerns for companies:

- how can we ensure that our commercial operations comply with the existing legal framework; ie. do our data communication practices fulfil the requirements?;
- how can we ensure that the necessary level of security is implemented by those with whom we communicate (security is only as strong as the weakest link)?

Contract law has traditionally been the means by which companies have mitigated against legal insecurity in their commercial operations. The use of contractual agreements enables the communicating parties to make explicit provision for the acceptance of electronic records; specify their respective responsibilities and liabilities, and determine the level of security that each party expects of each other and the system as a whole. Contractual provisions can give communication procedures certainty and enforceability, and therefore legal security.

When considering international data communications, questions of public and private international law are inevitably raised. Public international law is primarily concerned with "the rights and duties of sovereign States towards each other"[17]. In the context of the international flow of data, recent discussion has focused on whether a `right to communicate' exists in international public law and, if so, its potential extent. The relevance of public international law for international data communications is reviewed in Chapter 3.

---

[16] See further Chapter 5, at 5.3.

[17] Mozley & Whiteley's *Law Dictionary* (10th Ed), Butterworths 1988.

Private international law, on the other hand, concerns "the rights and duties of the private individuals of different States towards each other"[18]. It is therefore usually a question of establishing under which particular jurisdiction a dispute is to be resolved. These issues can, for example, arise when a commercial transaction, giving rise to obligations and responsibilities for parties in a number of different countries, is carried out across a European communications network. The nature of `conflict of laws' issues tends to be similar whether the long distance contract was communicated via paper or electronically.

Most public, and indeed some private, international law emanates from initiatives of various international and regional supra-national organisations. These organisations are the primary source of international law, in the form of conventions, recommendations and directives. Throughout the thesis, the work and influence of such organisations will be reviewed.

The range of issues raised by international data flows is extensive:

> "the issues raised under the TDF label relate to national sovereignty, national security, competitiveness and productivity regulation, employment, culture, privacy protection and computer related crime"[19]

Each of the areas quoted can give rise to forms of governmental regulation, ranging from legislation to protect the domestic data processing industry[20]; to national security regulations preventing the use of certain forms of encryption techniques[21]. Different types of data communication may require differing legal treatment; for example, personal data as against an electronic funds transfer. On the hand, such a diversity of regulation can, in itself, be seen as a obstacle to the adoption of telematics by business[22].

Little directly relevant English case law exists in the area of telematics[23]. The major reasons for this situation seem to be:

- The relatively recent development, use and dependence on such techniques within a commercial context;

---

[18] Ibid.

[19] Robinson, P., "Legal Issues Raised by Transborder Data Flow", p.295, 11 Can.-U.S. Law Journal, 1986.

[20] See Chapter 3, at 3.5.1.

[21] Such techniques are commonly adopted to protect data communications. See further Chapter 2, at 2.3.3; and Chapter 3, at 3.4.5., on encryption regulation.

[22] Poullet, Y., "Privacy Protection and Transborder Data Flow: Recent Legal Issues", p.30, in Vandenberghe, Prof. G.P.V., (ed.), *Advanced Topics of Law and Information Technology*, No.3 Computer/Law Series, Kluwer/The Netherlands 1989.

[23] However, see "Survey predicts 33% growth in computer-related litigation", p.11, in The Computer Law and Security Report, Vol.6, No.3, Sept-Oct. 1990.

- the fact that, current exploitation of data communications has tended to be between trading partners with whom a considerable amount of trust exists, based on a long-term trading relationship[24];

Another possible reason for the lack of disputes in the area of telematics is the possible expectation by companies using data communications that problems will arise!

This dearth of case law itself creates legal insecurity, since trading partners have no precedents upon which to base their actions. In the area of information technology generally, Tapper has noted:

> "In many areas there is no United Kingdom case or statute to illustrate or govern explicitly the application of general legal principle to computers."[25]

Indeed, one of the UK respondents to the EDI survey[26], suggested, as a possible solution to this lack of "established and trustworthy law", that:

> "The EDI community should establish (via sponsoring litigants?) precedents fast".

The vast majority of commercial disputes are settled by negotiation before reaching the courts, and this can be expected to be even more of a truism when dealing with an aspect (eg. data communications) that is one step removed from the actual commercial deal. In addition, the lack of precedent will encourage dispute resolution through alternative channels, usually relying on the judgement of industry experts, rather than the courts.

The impact of statute law on data communications has been of concern to both national governments and international organisations over the past three decades. Statutory initiatives establishing `positive' legislative restrictions, such as data protection legislation, was the dominant concern from the mid-1970s until the mid-1980s; while the `passive' legal restrictions, such as requirements for a `writing', have come sharply into focus in the 1980s and 1990s, particularly with the emergence of EDI.

The controversial, and therefore political, nature of `positive' legislative initiatives contrasts sharply with the low profile of the `passive' restrictions. However, the establishment of the European Community, and the current drive towards the `Single Market' by 1993, has brought these issues closer together: the removal of unnecessary legal restrictions and the harmonisation of legislation to establish a common degree of protection. As emphasised in

---

[24] See Chapter 2, at 2.2.4.

[25] Tapper, C., *Computer Law*(4th edition), p.xlv, Longman 1989.

[26] See Appendix B.

the European Commission's White Paper on the `Single Market'[27], the ease of information flows between economic entities is viewed as an essential condition for the free movement of goods and services and closer European co-operation.

It is therefore important to consider how European Community initiatives have been developed to facilitate the flow of data:

> "Regarding the legal and regulatory framework required for a free flow of information....apart from regulatory issues related to the conditions of provision and use of telecommunications services, convergent solutions should be found in a number of areas of legitimate public interest profoundly affecting the future environment for the free flow of information in the Community"[28]

The framework of European law will be considered in Chapter 3; however, each chapter will analyse the specific activities of the European Community.

There are additional legal areas which either directly impinge on data communications, such as intellectual property laws and telecommunication regulations; or which give rise to similar legal issues, for example, broadcasting law[29]. The former range of legal topics will be reviewed in Chapter 3.

In particular, recent years have seen the appearance of `data security law', as a distinct and legitimate area of study. In some countries, legislation has been passed dealing directly with data security issues; while it is also increasingly recognised that data security provisions should form an integral part of traditional commercial-contractual considerations.[30]

Finally, in addition to legislative and contract law, international data communications are obviously dependent on a wide range of technical regulations[31]. As has been stated by Stuurman:

---

[27] COM (85) 310, final, June 14, 1985.

[28] European Commission, Green Paper on the development of the common market for telecommunications services and equipment, COM(87) 290 final. The Green Paper gives some examples of such areas, including data protection, electronic fraud and authentication of transactions.

[29] "The growing computerization of all types of information accentuates the convergence of mass media and transborder data flow questions" in Bortnik, Jane, "International information flow: The developing world perspective", p333-353, 14 Cornell International Law Journal, 1981. See also Morris, B. and M. Hutchings, "Cross Frontier Broadcasting and the Law", Law Society's Gazette, No.22, 11/6/1986 and Castell, S., "Broadcasting and Cable - The New Framework", pp.20-24, The Computer Law and Security Report, Vol.6, No.1, 1990.

[30] Some of these issues are discussed in Chapter 3, at 3.3.4. See also Caelli, W., D. Longley, and M. Shain, *Information Security for Managers*, Macmillan Stockton Press, 1989, at Chapter 7; Phleegen, *Computer Security*, at Chap. 14; Reed, C., "The Legal Aspects", p.86-94, in Potts, R.J., (ed.) *An Introduction to the Security of Computer Systems*, PLC Consultancy Services, 1988; Walden, I., "Information Security and the Law", p. 179-238, in Caelli, W., D. Longley, and M. Shain, *Information Security Handbook*, Macmillan Stockton Press, 1991; "The Legal Aspects of Computer Crime and Security: A comparative analysis with suggestions for future international action", document prepared for the European Commission's Legal Advisory Board, December 1987, and Slater, Ken, *Information Security in Financial Services*, Touche Ross/Macmillan, 1991, at appendices 14-16.

[31] Eg. the Comité Consultatif International Télégraphique et Téléphonique (CCITT), which establishes technical and

"In our information society, more and more technical standards are used in formulating laws, regulations, decisions etc...standards are becoming more important in drafting contractual obligations and interpreting the meaning thereof, whether or not in the courtroom."[32]

Although such technical standards and regulations will be noted, it will only be to the extent that they impact either directly or indirectly on the achievement of legally secure data communications.

1.4 The Scope

As has already been noted, the thesis will be considering the legal aspects from both a national and international viewpoint; as Lowry has stated:

"The problems of computer networks are difficult enough to solve within a unified law district. The difficulties increase exponentially when they arise in the international arena.."[33]

However, this thesis will have three distinct tiers of examination. The primary focus will be upon the legislative framework within the United Kingdom, such as the Data Protection Act 1984. Secondly, frequent comparisons with European States will be made, primarily from within the European Community, since the approach of the `Single European Market' means that data communications between Member States can be expected to expand rapidly.

Thirdly, reference will be made to other legal jurisdictions, primarily the United States, which have similar legal traditions to that of the UK, and could therefore be expected to deal with the issues in a similar manner[34].

1.5 Methodology

When considering the impact that the law can have on the use of data communications technology, it is important to balance the analysis of the legislative and contractual framework, within which businesses operate, with the reality of commercial operations: Does the law create real obstacles to the commercial adoption, development or reliance on electronic means of communications?; and under what form of legal agreements do

---

operating standards and tariff guidelines for international networks. See further Chapter 2 and 3.

[32] Stuurman, C., "Legal aspects of standardization and certification of information technology and telecommunications: an overview", p.11, paper presented at FIRLITE Conference: `Data Security in Computer Networks and Legal Problems', 23-24 September,1991, Hanover.

[33] Lowry, Houston Putnam., "Transborder Data Flow: Public and Private International Law Aspects", Houston Journal of International Law, vol.6 part 2 (1984), p159.

[34] Since the IT industry in the United States is considerably more mature than that found in Europe, significantly more relevant legal jurisprudence exists, such as case law.

companies currently operate?

In an attempt to find answers to these questions, the following surveys and reviews were carried out:

- A survey of 15 UK-based multinational companies[35]. The companies were asked to fill in a general questionnaire covering data protection, data communication restrictions and data security. In most cases, the questionnaire was followed up by a face-to-face interview[36] (Survey A).

- A survey of 42 European companies which use EDI communications in some aspect of their commercial activities. The companies were asked questions concerning the difficulties they experienced when implementing EDI; the security procedures used; the issue of evidence and the types of contractual agreements entered into[37] (Survey B).

- A review of 32 different forms of agreement, from around the world, drafted specifically to establish legal security between trading partners communicating electronically[38] (Review A).

- A review of 26 contractual agreements issued by companies offering data communication services[39] (Review B).

The results of Survey A are not intended to be quantitative, since the sample size is too small for the results to be statistically significant. The results were garnered within a qualitative research tradition[40]: the in-depth interview process was designed to offer the author an insight into the range of issues that confront companies when using data communications[41].

Survey B is, as far as the author is aware, the only such study carried out in this field in Europe. The study shows that, although legal issues are recognised to be important, few companies are adequately incorporating legal security issues into their implementation strategies.

---

[35] For comparative purposes, a number of companies in Germany and Sweden were also sent questionnaires and interviewed. Sweden was chosen because it was the first country to pass data protection legislation, in 1973, and has a high profile in the literature regarding transborder data flow restrictions; while the German data protection act would seem to have imposed minimal burdens on the private sector use of data communications.

[36] See Appendix A1/A2/A3, and Chapter 2 & 4.

[37] See Appendix B1/B2/B3, and further Chapter 2.

[38] See Appendix C1/C2, and further Chapter 6.

[39] See Appendix D1/D2, and further Chapter 6.

[40] See generally Miles, M.B. and A.M. Huberman, *Qualitative Data Analysis*, 1984, Sage, London.

[41] Most of the issues raised have also been borne out in larger-scale studies, to which the author has referred to throughout the text.

The agreements considered in Review A, represent a new form of contractual relationship between data users. Over the past four years, a considerable range and number of organisations have issued model agreements for use by companies wishing to communicate electronically. In Chapter 6, a clause by clause analysis is carried out of the standard provisions used in such agreements, and consideration is given to the future form and, indeed, real need for such agreements.

Data communications pass over telecommunication networks. The recent liberalisation of the telecommunications industry[42] has given added impetus to the growth of a new form of telecommunications service provider: value-added network providers[43]. As companies become increasingly dependent on such networks for their data communications needs, the contractual agreement will assume a greater commercial importance. The review of the agreements considered in Review B, illustrates the current nature of such agreements and considers what `legal security' issues data users should ensure are built-in to the relationship.

1.6 The Thesis

This study is not a minute dissection of a small area of distinct law. Rather, it is a broad consideration of the interface that exists between law and the establishment of secure data communications:

> "Security is...a fundamental problem when replacing paper documents with structured ADP messages...possibly all the other questions...are functions of the general acceptability of the security and costs involved in different ADP approaches."[44]

The intended value of this study lies in its synthesis of law, as expressed within legislation and contractual agreements, with the three objectives of data communications security: Confidentiality, integrity and availability. Within this general aim, however, a number of additional themes can be recognised.

Data security issues have never been particularly prominent within companies, often reflecting a distinct lack of interest at board level[45]. Where security is considered, it is usually in terms of technical security procedures, such as `segregation of duties'. However, one objective of this thesis is to place `legal security' issues as an integral and critical aspect in the establishment of a secure data communications environment.

---

[42] See Chapter 3, at 3.3.2.

[43] See Chapter 2.

[44] UN/ECE, `An Overview of Legal Problems of Trade Facilitation', p.6, para.32, TRADE/WP.4/GE.2/R.102, 10 November 1977.

[45] See Warman, Dr A., "Organisational Computer Security Policies", L.S.E., London, 1991. 39% of respondents believed that their current procedures were insufficient.

Legislation in the field of data security is usually only able to create a framework of minimum requirements for protection, which will not necessarily meet the commercial needs of business. Consideration is given, therefore, to the role of contractual agreements in the achievement of `commercially reasonable security'[46]. The ability of legal entities to construct a private legal framework should facilitate the exploitation of data communications technology.

The major fear, particularly prevalent among US businesses, during the 1970s and early 1980s was that various legislative barriers to international data communications would be erected, such as through data protection legislation. This assertion would seem to have been largely unfounded. The majority of restrictions that exist concern the process of data transmission, rather than the content of the communication itself. Such quasi-legal restrictions are gradually being removed, at least within the European Community, through the liberalisation of the telecommunications industry.

One of the major issues raised by this debate, concerns the role of legislation in the regulation of technology. `Telematics' is "an international medium par excellence"[47], and therefore does not recognise national borders. Such technological independence creates specific control problems for a national legislative framework designed to regulate such flows. International harmonisation is required. Data protection legislation, for example, can create obstacles to international data flows; however, the problem primarily concerns the absence of protection in certain countries.

A final theme of this thesis, therefore, is the means by which harmonisation can be achieved. Harmonisation is not, however, simply a factor of statutory provision, it can also take account of other sources of legal controls, such as industry codes of conduct and contractual provision. What initiatives have been promoted, can be expected and are most suitable for data communications?

---

[46] term coined by Baum, M., "Analysis of Legal Aspects", p.129, in Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989. See also `Comments on the Draft Model Law on International Credit Transfers - Report of the Secretary-General', 15 May 1991, A/CN.9/346; p.25, at Article 4(2)(a) "the authentication is in the circumstances a commercially reasonable method of security...". In the US, see UCC, Art.4A [for electronic funds transfers], at § 202(c) "Commercial reasonableness of a security procedure is a question of law...".

[47] Hondius, F.W., *Emerging data protection in Europe*, p.5, North Holland, Amsterdam, 1975.

Chapter 2 **TECHNICAL BACKGROUND**

2.1 Introduction

In the past decades, the development of more sophisticated telecommunications systems, coupled with the growth in computing has resulted in a growing international trade in information and associated services[1]. Indeed, most aspects of our lives are now dependant in some degree on computer and telecommunications technology moving information around the world, ranging from news, education and manufacturing to national defence and weather prediction. Hondius[2] notes that there has been three major stimuli to the growth of international data flow over recent decades: the internationalisation of markets; increasing administrative relationships between states (eg. the European Community) and the activity of international organisations.

2.2 Data Communications

> "The transmission of data between a person and a program, or between one program and another, when the sender and receiver are remote from each other"[3]

---

[1] Eg. between 1979 and 1987, the number of transactions between data communication users was estimated to rise from 136 mill. pa., to 800 mill.; quoted in Sauvant, K P, *International Transactions in Services: The Politics of Transborder Data Flows*, The Atwater Series on the World Information Economy No 1, Westview Press/London.

[2] Hondius, F.W., *Emerging data protection in Europe*, p.242, North Holland, Amsterdam, 1975.

[3] Longley, Dennis, and Michael Shain, *Dictionary of Information Technology*, 3rd Ed., Macmillan, 1989. However, it has been stated that " `Data communications' has a much wider meaning than data transmission and embraces not just the electrical transmission but many other factors involved in controlling, checking and handling the movement of

Companies tend to communicate via one, or more usually a combination, of four major means: leased lines, the public data or telephone network and disk or magnetic tape[4]. The thesis is primarily concerned with direct data communications, via telecommunications links, rather than the physical transfer of electronic media. Telecommunications systems[5] operate via a number of means, copper cables, optical fibres, microwave and/or satellite systems[6]. The reason for such a focus is because direct data communications can fundamentally alter the way a business trades, such as the adoption of a Just-In-Time manufacturing process; while the physical exchange of electronic media, such as magnetic tape, is more akin to traditional postal/paper-based means of communication, although greatly enhancing efficiency.

2.2.1 Network Methodologies

Networks can be classified by four means:

- by ownership, whether public or private sector[7], although the private sector can be further divided between a private network for intra-company communications and `third-party' value-added network providers[8];
- by access, whether open or closed[9];
- by the service provided, basic or value-added[10] and

---

information in a communications-based computer system."; NCC, *EDI in Action* (3 vols.), at vol.3, s.2, p.7, NCC, 1989. Bender defines `data communications' as "the use of communications to transmit data for processing at a remote location", p.2-104, *Computer Law*, Volume 1-3, Matthew Bender, New York, 1991.

[4] Although `privately-owned' satellite communication systems can be used, satellite communications usually form part of the telecommunication infrastructure, and are purchased as a service, see fn.4 below.

[5] This range of techniques has been reflected in UK law, which defines a `telecommunication system' as being:
"a system for the conveyance, through the agency of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy, of:
(a) speech, music and other sounds;
(b) visual images;
(c) signals serving the impartation (whether as between persons and persons, things and things or persons and things) of any matter otherwise than in the form of sounds or visual images; or
(d) signals serving for the actuation or control of machinery or apparatus." [Telecommunications Act 1984, s.4(1)].
Such a wide definition would also cover such things as a door bell, but not necessarily fibre optic systems!

[6] Satellite business communication services have appeared over recent years; eg. Intelsat Business Service "offers a digital global service providing telex, voice, facsimile, data and videoconferencing facilities, distributed by satellite via aerials located on or close to end-user facilities"; see Saxby, S., *The Age of Information*, p.278, Macmillan Press, 1990.

[7] This distinction is disappearing; see Chapter 3, at 3.3.2.

[8] Such communication services are commonly known as `VANs'; `resale networks'; `managed data network services'; VADS (Value-Added and Data Services: the term used in the UK telecommunications licensing regime; as well as `Service Provider') or `enhanced service providers' (term used by the US Federal Communications Commission); see further Chapter 3, at 3.3.2. For the purposes of this thesis, the term `network provider' will be the primary term used. See European Commission Report, "Analysis of the market for Value Added Services in Europe", prepared by Scicon Networks, December 1989.

[9] Eg. BT's Telecom Gold (Email system) is an `open' system; while the SWIFT bank network (Society of Worldwide Interbank Financial Telecommunications) is a `closed' network.

- by form of communication, eg. voice, data or images[11].

In most countries, the basic networking infrastructure, consisting of lines, switches and nodes[12], are usually provided by the public telecommunication operators (PTOs)[13]. Private networks are therefore usually based upon leased lines[14] furnished by the PTOs.

A company that wishes to communicate electronically will have to decide whether to establish a direct communication link with its trading partner, perhaps through a leased line; or use the facility of a third-party, Value-Added Network[15]. The advantages of the latter are that they market a range of services, such as translation between different communication protocols and offer an international coverage, that would be costly for a individual company to maintain[16].

A Business International survey[17] showed that for private networks, leased lines were the favoured communication option by most multinationals, primarily for data security reasons; however, the cost requires significant volumes of data traffic to justify, and they have, certainly in the past, proven difficult to obtain in a number of countries.

2.2.2 Communication Methodologies

The previous section gave an overview of the physical links that are required for data communications to occur; however, for different computer systems to communicate also requires that they understand a common language that will allow them to interconnect. This section reviews the types of standards within which data communications occur.

The Comité Consultative Internationale de Télégraphique et Téléphonique (CCITT) is the

---

[10] The former are also classified as `reserved' services, such as voice telephony, as opposed to `competitive' services. With deregulation of the telecommunications sector, and developing technology, this distinction is becoming increasingly difficult to distinguish. See Petre, Blanche, "Network Providers", p8-18, Computer Law and Practice, Vol.7, No.1, Sept-Oct. 1990.

[11] Such a distinction is also increasingly irrelevant with the widening distribution of the Integrated Services Digital Network (ISDN), which is based upon "a fully digital telephone network of all-electronic, software controlled switching centres and totally digitised transmission systems", based upon CCITT I series recommendations; see ICC "Communications Network Security: an International Business View", p.8, Position Paper No.13, Doc.No. 373/103 Rev., July 1990.

[12] Known as either voice Private Automatic Branch Exchange (PABX) or data PABX (or ISDX for digital networks).

[13] Eg. Mercury and BT. The national network providers are also known as PTTs: Postal Telegraph and Telephone authorities.

[14] Leased lines are "exclusively assigned communications channels".

[15] The current major UK network providers are INS, AT&T Istel, Geisco, IBM, BT Tymnet and DIALnet.

[16] One study has noted seven value-added services offered in addition to message conveyance: message and data log storage; access controls; security procedures; system audit availability to customers; customer profiles; billing information and back-up facility - TPSP Commercial Study, carried out by Independent Monitoring (December 1989); quoted in Baum, Michael S., Henry H. Perritt, JR., *Electronic Contracting, Publishing and EDI Law*, at p.111, Wiley Law Publications, New York, 1991.

[17] Business International Report, *Transborder Data Flow: Issues, Barriers and Corporate Responses*(New York: BI, 1983) at p32. See also Sauvant, op.cit. supra n.1, at p.97-100.

major standards-making organisation for data communications. It operates under the International Telecommunications Union[18]. The CCITT works closely with the International Standards Organisation (ISO), which consists of the national standards committees of each member country.

2.2.2.1 Protocols

> "Protocols are the means by which data is allowed to flow through the communications channels...they do nothing to aid the understanding and use of the data received, but rather achieve an effective and orderly transfer between systems."[19]

Packet switching is the most common form of communication protocol under which the Public Switched Data Networks (PSDN) operate[20]. Packet switching involves the message being divided into distinct packets, with appropriate addressing information, which are then sent individually across the network, from node to node, according to a complex routing algorithm[21]. The protocol ensures that the packets are reassembled in the correct sequence and that the data is uncorrupted. Packet switching was originally developed in the 1960s, as a solution to the military need for network reliability[22]; it is also an extremely efficient technique for maximising network use.

Access to the public switched data network is usually via a leased line node connection, or by `dial-up' via the Public Switched Telephone Network (PSTN)[23]. Such national packet-switched services are usually connected internationally via the international packet switching service (IPSS)[24]. The European Commission has legally defined the provision of such `packet-switched services' as:

> "..the commercial provision for the public of direct transport of data between public switched network termination points, enabling any user to use equipment connected to such a network

---

[18] See Chapter 3, at 3.3.2.1. It has five levels of membership: Member States governments, private carriers (eg. AT&T, BT), industrial and scientific organisations, international organisations, and other interested bodies.

[19] "Telecomms: when will Europe be connected?", p.24-26, Electronic Trader, Vol.1, No.3, January 1991.

[20] Eg. BT's `Packet Switchstream' (PSS) and Mercury 5000. The universal packet design and PSDN interface standard is the CCITT X.25 recommendation. `Circuit' (line) switched networks are also operated by some national PTOs, and operate by establishing, as in the telephone system, a direct physical transmission path through the switching nodes between the sender and receiver.

[21] Because no direct transmission path is established between the sender and receiver, a communication session is known as a `virtual circuit'.

[22] See further NCC, op.cit. supra n.3, at vol.3, s.3, p.17.

[23] All of the multinational respondents to the survey (see Appendix A), stated that they used both `dial-up' and leased lines.

[24] International connections between PSDNs are based upon the CCITT X.75 recommendation, which includes internetwork accounting procedures.

termination point in order to communicate with another termination point."[25]

Message switching is a second important form of data routing protocol[26]. This system is described as a `store-and-forward' system because no direct interaction occurs between the recipient and sender. Instead, the sender submits the message to the network, where it is stored in the recipient's electronic mailbox until the recipient chooses to connect to the network, access his mailbox, and collect the message. This form of communication protocol is the basis upon which EDI messaging services commonly operate.

Over the years, a number of proprietary protocols have been adopted in certain communication environments, such as SNA[27] and DNA. As data communications has developed to embrace a wider range of information flows, between a larger data user community, there has been a demand for a common, international standard to be created. This pressure from users resulted in the development of the Open Systems Interconnection (OSI) reference model, as a framework network architecture, within which interconnect standards can be developed by various organisations[28].

The reference model is based upon seven-layers, which represent the various processes required for successful communications. These layers represent separate, but linked, functional processes[29]:

- The physical layer, "provides the mechanical, electrical and procedural means to establish, maintain and release a physical connection between systems"[30];

- the data link level is concerned with ensuring that the data arrives at the correct destination, that effective controls on the flow of data and error control procedures exist[31];

---

[25] The European Commission Directive on `Competition in the Market of Telecommunications Services' (90/388/EEC), at Article 1(1), ninth indent. See also Chapter 3, at 3.3.1.

[26] Eg. the X.400 series of recommendations for `message handling'.

[27] IBM's System Network Architecture.

[28] CCITT VIIIth Plenary Assembly, Malaga-Torremolinos, October 25, 1973 [28 UST 2510, TIAS No.8572]. The OSI initiative is primarily led by the CCITT and the ISO; although its development is strongly supported by the US, UK and the European Commission.

[29] See further Toye, P., "Review of OSI standards", pp.88-107, in Gifkins, M., *EDI Technology*, Blenheim Online/London 1989.

[30] See NCC, op.cit. supra n.3, at vol.3, s.4, p.11. The connection is between data terminal equipment (DTE) and data circuit-terminating equipment (DCE). Eg. analogue (V.24 & RS232) and digital (X.20 & X.21).

[31] Errors are usually corrected by requesting re-transmission. The two major protocols currently in use are basic mode and High Level Data Link Control (HDLC). Such Data Link Controls fulfil four main functions in the communication process: "Synchronization between the sender and receiver; controlling the sending of data; detecting and recovering transmission errors between two points and maintaining awareness of link conditions"; see Black, U.D., Data Communications and Distributed Networks (2nd Ed.), Prentice Hall International Editions, 1987, at Chapter 6.

- the function of the network layer is to establish, maintain and terminate the communication route through and between networks for the session period[32];

- the transport layer is the lowest level to deal with the end-to-end aspects of the communication[33];

- the session layer is concerned with the establishment, maintenance and termination of the correct link between the applications within the communicating end-systems;

- the presentation layer "deals with format and syntax of messages providing the links necessary for incompatible `intelligent' terminals to converse"[34];

- the application layer is the highest level of the model, and communicates directly with the user[35].

Within the application level, one of three modes of communication will need to be adopted, depending on user requirements: (a) batch mode (point-to-point), where both parties need to be available for a communication session to be established[36]; (b) store and forward, a mailbox system, as usually provided by VANs[37]; or (c) interactive systems, where a series of short messages pass between the parties during a communication session[38].

An additional key element in the creation of a truly open systems data communications environment, is the establishment of a single electronic `global logical directory' of addressing information. This would allow users to accept and send electronic messages to any other user, according to commercial requirements, without prior agreement, "provided that security services are used to authenticate the originator, and provided that payment is

---

[32] Eg. The X.25 Recommendation: Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment for Terminals Operating in the Packet Mode on Public Data Networks, was first published in 1976, and covers the bottom three layers of the model, including the network layer. The ISDN CCITT I series recommendations also cover these first three layers.

[33] This level provides for five classes of error detection and recovery and monitoring of service quality, according to perceived security need. Eg. the X.75 standard provides a gateway between different networks (based on X.25).

[34] Saxby, op.cit supra n.6, at p.292.

[35] Eg. CCITT X.400 Recommendations. The first version was produced in 1984, and the latest revision was in 1988. Under the protocol, an EDI Messaging System protocol, Pedi (X.435) has been developed which will allow large companies to establish their own network, without the use of a third-party network provider. See further Hill, Richard, *EDI and X.400: using Pedi*, Technology Appraisals, 1990 and DTI `Vanguard EDI and X.400 study', HMSO, 1988.

[36] Eg. The File Transfer, Access and Management (FTAM - ISO 8571) protocol. Most suitable for regular bulk data transfers.

[37] Eg. X.400.

[38] Eg. The Transaction Processing (TP - ISO DP 10026) protocol is being developed, within the OSI framework, for interactive communications, such as airline reservation systems.

suitably guaranteed"[39]. Within the OSI initiative, the X.500 standard is being developed to fulfil this role[39a] .

2.2.2.2 Messaging Standards

> "standardized ways of describing data items,...and of grouping and presenting these data items in the form of messages or trade information"[40]

Message standards do not fall under the Open Systems Interconnection (OSI) scheme, although they can be thought of as the eighth layer, above the application layer. Message standards are concerned with the actual representation of the information which is being exchanged between the parties. Upon receipt, the message will be translated into the format required by the particular application.

Messaging standards have been created within industry groups[41], national standards organisations[42] and at the international level[43]; and over recent years there has been a move towards the use of a common international standard: UN/EDIFACT[44]. Delay in the widespread adoption of this international standard does not just reflect a stubborn parochialism by various users, but is also based on the fact that a suitable message "can take between four and five years to agree".[45]

A message standard is usually drafted to reflect the options and alternatives, regarding information content, that the trading parties may wish to exchange[46]. The current major message standards are composed of a range of data segments, some of which are mandatory upon users; while others are conditional elements. Before such data communications can occur, therefore, the parties need to agree upon what data segments are to be exchanged.

---

[39] See Hill, op.cit. n.35, at p.95.

39a CCITT X.500 Recommendation series (ISO/IEC 9594). See Steedman, D., *X.500*, Technology Appraisals, 1992.

[40] NCC, op.cit. supra n.3, at p.9.

[41] Eg. Tradacoms, designed by the Article Number Association (UK), primarily for the retail trade.

[42] Eg. in the US, the X.12 standards are produced by the American National Standards Institute (ANSI). In the area of CAD/CAM data exchange, the most widely used format is IGES (Initial Graphics Exchange Specification), managed by the US standards body, the National Institute of Standards and Technology (NIST).

[43] Eg. Odette, the Organisation for Data Exchange by Teletransmission in Europe (primarily in the automotive industry), created the File Transfer Protocol (FTP) which runs on an X.25 base.

[44] The United Nations EDIFACT (EDI for Administration, Commerce and Transport) standard was adopted in September 1987 (ISO 9735). It is based upon the international standard Application Level Syntax Rules (ISO 9735) and the Trade Data Element Directory (ISO 7372). See further Berge, J., "EDIFACT - a technical introduction", pp.63-78, in Gifkins, M., *EDI Technology*, Blenheim Online/London 1989.

[45] Saxby, op.cit. supra n.6, at p.292.

[46] Eg. within a Tradacoms purchase order, the parties may choose whether to send data elements relating to both the `Date Order Placed by Customer' and `Date Order Received by Supplier'.

The major problem of current CAD/CAM data exchange activities is the fact that the existing messaging standards[47], both proprietary and international, do not achieve full compatibility: a percentage of the details and annotations on Company A's system will be lost in the communication process to Company B. Companies will therefore need to agree and "define the minimum requirements for a `successful' exchange"[48].

2.2.3 Electronic Data Interchange

Electronic Data Interchange (EDI) is a new mode of business communication, replacing standard paper documentation, such as invoices and purchase orders, with structured electronic messages: "the computer-to-computer transmission of business data in a standard format"[49]. EDI is usually distinguished from unstructured Email messaging systems and basic file transfers[50]. In essence, it is paperless trading.

The range of benefits using EDI are impressive, and are analogous to those gained with TDFs[51]. Organising the paper documentation created by a transaction is not only cumbersome and time-consuming, but it can represent as much as 10% of the value of the product[52]. EDI can significantly reduce such associated administrative costs and increase clerical productivity; for example, by removing the need to re-key the information at each stage of the trading cycle[53]. The use of EDI also increases the speed of information flow, and therefore the transaction as a whole; for example, it can enable the introduction of a `just-in-time' delivery system, and therefore reduce inventories. Such increased efficiency can offer businesses that use EDI a significant competitive advantage.

EDI can be used to facilitate trade, as well as a company's internal information management. The development of EDI has focused initially on replacing trading documents such as invoices, however, the definition of EDI also extends to electronic funds transfer (EFT)[54]; the

---

[47] Eg. IGES, SET and VDA-FS.

[48] "The Exchange Agreement: Guidelines for the successful exchange of product data", p.2, published by the CAD-CAM Data Exchange Technical Centre (CADDETC), Leeds 1990.

[49] The United Nations Trade Data Interchange Directory (UNTDID), TRADE/WP.4/R.721. See also generally: Gifkins, M. & David Hitchcock, *The EDI Handbook*, Blenheim Online/London 1988; Gifkins, M., *EDI Technology*, Blenheim Online/London 1989 and NCC, op.cit. supra n.3.

[50] *EDI in perspective*, Commission of the European Communities, EUR 11883 en (1989).

[51] See 2.2.5. below.

[52] European Commission COM (86) 662, final, December 1, 1986. A 1984 survey, conducted by Istel Ltd and the Institute of Physical Distribution Management, found that the cost of generating and processing commercial documents was around £10 each; while Pipe, R.G. and Brown, C. (ed.), *The International Information Economy Handbook*, p.4, (TDR, Springfield, 1985), states that information accompanying trade accounts for 8% of the value of the invoice.

[53] Bytheway, A., estimates direct cost savings to be around 50p to £2 per transaction; while indirect cost savings are seen as being two to three times greater, in "EDI: Technical opportunity or business necessity", working paper from `EDI: The longer term effects on international trade' research programme, July 1989.

[54] See further Chapter 3, at 3.3.4.2, and Fergus, D., "European EDI in the financial sector", p.105-121, Proceedings of '91 International Conference on EDI, 7-8 Nov., Korea.

submission of regulatory information (eg. customs declarations) and the exchange of CAD/CAM information[55].

A company that wishes to communicate by EDI will also have to decide whether to establish a direct communication link with its trading partner, perhaps through a leased line (eg. from BT or Mercury); or use the facility of a third-party, network provider (eg. IBM or GEISCO)[56].

Within Europe, EDI has tended to grow through the formation of project groups in certain industry sectors, recognising their common data needs and establishing a common system of information interchange: eg. DISH (shipping), Odette (automotive) and CEFIC (chemical). Alternatively, in the US, EDI has tended to develop around large corporations forging EDI links with their traditional suppliers, eg. General Motors[57].

In the future, as developments such as the OSI initiative become implemented globally, it is predicted that the concept of `open-EDI' will emerge:

> "Electronic data interchange among autonomous parties using public and non-proprietary standards aiming towards global interoperability over time, business sectors, information technology systems and data types."[58]

However, the current nature of `generic' message standards requires that the parties need some form of prior agreement regarding the data elements to be exchanged[59].

EDI has made a significant impact over the past five years, as an efficient means of managing business information. There are currently around 12,000 companies using EDI in the US; while in the UK there are some 6,000 users, with the rest of Western Europe catching-up fast[60]. It is estimated that the user base growth of EDI is about 30% per annum, in the UK; while message volume is growing at 100% per year[61].

---

[55] Computer-Aided Design/Manufacturing information; see further McTaggart, B., "Developments in the use of EDI for CAD/CAM interchange", p.581-587, Proceedings of EDI'90, 30 Oct.-1 Nov, 1990; see also Chapter 6, at 6.3.4. Computer-aided Acquisition and Logistics Support (CALS) is a similar form of data communication, where technical information/standards are maintained on a single, shared database. CALS is an initiative from the US Department of Defence, and is designed to reduce the costs associated with the development of equipment; see Evans, Dr S., "CALS", ibid., at p.224-232.

[56] In the US, it is estimated that 80-85% of EDI users communicate via a third-party service provider - John Goetzman, Director of Customer Service, Harbinger EDI Services, December 1990; quoted in Baum, op.cit. supra n.16, at p.108.

[57] See generally, "The rise of `cooperative' systems", p.1-14, EDP Analyzer, Vol.25, No.6, 1987.

[58] quoted in Knoppers, J., "Transforming Cross Industry Practices into EDI: The business case for scenario modelling", p.578, in Proceedings of the 3rd International Congress of EDI Users, 4-6 Sept., 1991.

[59] See section 2.2.3.2 above.

[60] See Tate, Lee, "EDI - a vision of the future", p.165, Proceedings of the 3rd International Congress of EDI Users, 4-6 Sept., 1991, who estimates worldwide use to be between 75-100,000 corporations; while Schuringa, Prof. T.M., ibid., at p.171, states that EDI messaging in Europe was 700 mill. in 1990, although 80% was thought to be internal EDI. See also Tedis `Survey of EDI in all the Member States 1989', XIII/D/5/6-90.

[61] Mandela, Audrey, "EDI trends and directions", Yankee Group Europe Seminar, 6 April 1992. User base growth has been 100% per annum; The Times, Sept. 28, 1990, at p.26. See also Walker, R., "1992: Maintaining the UK's Competitive Edge in EDI", p.8, in Gifkins & Hitchcock, op.cit. supra n.49.

2.2.4 Transborder Data Flows

A transborder data flow (TDF)[62] is the transfer of data across a national border by any one of a variety of medium. The transmission of the data may be carried out electronically and instantaneously via cables or satellite, or it may be effected more slowly by the physical transfer of magnetic tapes, disks, cards or similar media; however, this thesis is primarily concerned with TDFs via telecommunication networks. Such data would also normally be stored or reprocessed in a country other than the originating country[63]. Article 12 of the Council of Europe Convention defines transborder data flows as

> "the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed."[64]

The essence of a transborder data flow is that information is transferred in a machine-readable form[65]. This definition is also limited to transfers from point-to-point, therefore not including mass media broadcasting.[66] Novotny distinguishes TDFs from other forms of international communication, such as fax and telex, by requiring that the " technical process involve: (1) transmission, (2) storage, and (3) computation".[67] Where used for international communications, EDI can be seen, therefore, as the current term to cover much of what was previously described as transborder data flows. However, the majority of TDFs during the 1970s and early 1980s were primarily simple file transfers.

Transborder data flows can generally be classified into the standard four types of information: personal, business, technical and organisational; although, the first use of the term transborder data flow was in connection with the use and abuse of personal data.[68] The four types of TDF are generally used within four major contexts:

- intra-company information, such as parent-subsidiary reporting;

---

[62] Some opinion disgrees with the use of this term: "Another thing that many international business executives agree upon is that the coining of the phrase Transborder Data Flows can, with hindsight, be seen as having been, in some respects, unfortunate and its subsequent misuse as having led to unintended results....use of the term has focused attention on a single form of international communication, i.e., data traffic, giving the false impresssion that data is the dominant form of information transfer and unlike the telephone or ordinary mail it is a source of many problems.", Statement by the Business and Industry Advisory Council of OECD, `Transborder Data Flows In The International Firm', presented at the 2nd Symposium on TDFs, London, 1983.

[63] "data services rendered (exported/imported) across national borders", p.xxi, Sauvant, op.cit. supra n.1.

[64] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, Council of Europe, 1981. (European Treaty Series No 108), Explanatory Report, see also Chapter 4, at 4.3.1.

[65] Edwards, C., & Nigel Savage (Eds.), *Information Technology and the Law*, Macmillan 1986, at p144.

[66] Remote earth sensing by satellite (RES) is also a closely related technology.

[67] Eric J. Novotny, "Transborder Data Flows Regulation: Technical Issues of Legal Concern," *Computer/Law Journal* III (Spring 1982), at p.106.

[68] Briat, Martine, `Personal Data and the Free Flow of Information', in *Freedom of Data Flows and EEC Law*, proceedings of 2nd CELIM Conference [Kluwer, 1988]. She states that only 2-5% of TDFs concern personal data.

- inter-company information;
- transnational pursuit of information resources, such as the use of remote databases and service bureaux;
- governmental information needs.

This thesis is primarily concerned with the use of TDFs for data communications between trading partners within the private sector.

The range of information involved in TDFs is vast and reflects the internationalisation of markets that has occurred over the past few decades. For example, there are an average 29000 messages involved in the departure of a single 747 flight[69]; while SWIFT (the Society for World-wide Interbank Financial Telecommunications) provides electronic funds transfers between around 1200 banks in 50 countries[70].

According to a study undertaken in the US, on the use of transborder data flows by multinational corporations, operations in the following areas have become largely dependent on such transfers:

"a) Production Planning Co-ordination Systems, including production scheduling, material management and inventory record keeping;
b) Financial systems, including budget performances and accounting statements as well as sales and production data;
c) Engineering systems, including large mathematical models and specialised computer equipment;
d) Purchasing and customer systems, including accounts payable and receivable, historical profiles of vendors;
e) Employee systems, including payroll and human resources planning."[71]

Of these, the most frequent reasons given by companies for embarking on TDF are concerned with customer relations and financial management.[72]

In 1983, a survey was carried out by the OECD Secretariat jointly with the Business and

---

[69] Presentation made by Mr W.Monssen, Lufthansa, to `Data Commissioners Conference', Quebec, September 1987.

[70] In July 1990, SWIFT started an EDI pilot project involving 73 member banks; see Nacamuli, A., "The SWIFT Project", p.77-85, Proceeding of the 3rd International Congress of EDI Users, Brussels, 4-6 Sept., 1991.

[71] US National Committee of the International Institute of Communications, 1982. see also the Business International survey in *Transborder Data Flow: Issues, Barriers and Corporate Responses* (New York: BI, 1983).

[72] IBI "IBI World Survey of National Policies and Company Practices Concerning Transborder Data Flows" TDF 110, (Rome, IBI, 1983). For a summary of the results see p26, *Transnational Data Report*, vol.VII, no.1 [Jan/Feb 84].

Industry Advisory Council (BIAC)[73] to ascertain the impact that TDFs have on a company's operations. The following summarises the survey's conclusions:

> "From basic design and research, through production, marketing and distribution to after sales-service, TDF have been used to reduce costs and increase productivity....
> In some cases the improvements in performance allowed by TDF is so great as to make it possible for the firm to reorganize its operating structure in a more efficient way....TDF allow firms to offer entirely new products..."[74]

Another study carried out in 1983, by Business International, found that 85% of the multinational companies surveyed were dependent on TDFs for at least one key aspect of their international operations.[75]

The qualitative survey carried out for this thesis[76], confirmed the findings of these previous reports. All the respondents believed that international data flows were either `essential' or `very important' to the company's operations. The impact TDFs on company management structure was evenly divided among respondents, between greater centralisation and greater decentralisation. One respondent noted that the use of TDFs had led to centralisation of planning, but decentralised decision making[77]. Finally, about half of the respondents stated that they felt the ability to use TDFs had opened up new business opportunities; primarily through the ability to offer customers a better service.

2.3 Data Security[78]

Any discussion on establishing legal security in data communications is irrelevant, unless the types of insecurities that exist in such an environment are examined. One of the most oft-quoted fears expressed by those embarking on the use of such technology is: "what are the liabilities of each party if the sender's message states 500 widgets, but due to the network the recipient receives an order for 50,000 widgets?".

---

73 `Transborder Data Flows in International Enterprises' (OECD Document DSTI/ICCP/83.23). The Report was based on 128 questionnaire responses from 10 countries, and 50 interviews.

74 Kelly, M., "Surveys Show Strategic Importance of TDF", p25, Transnational Data Report, vol.VII, no.1 [Jan/Feb 84]. See also Sauvant, op.cit. supra n.1, who states:

> "TNCs [TransNational Corporations] rely more and more heavily on transnational computer-communications systems. They do this not only to speed up the sending of messages, but also to improve the management of corporate systems and to change the very manner in which corporations actually engage in productions"

75 BI Report, op.cit, supra.n.71.

76 See Appendix A1/A2.

77 Interview with Gunner Reichman, Head of Security, IBM Sweden, 1989.

78 Data security "means providing the users of your data with the data that you intend them to have, and with that data only, at the time you mean them to have it.", p.1, Caelli, W., D. Longley, and M. Shain, Information Security for Managers, Macmillan Stockton Press, 1989. The European Commission states that: "Information Security (IS) is concerned with the protection of information stored, processed or transmitted in electronic form, against deliberate and accidental threats", p.114, fn.1, `Proposal for a Council Decision in the field of Information Security', COM(90) final.

The first critical requirement, before engaging in detailed negotiation to decide on the attribution of liability, is a risk analysis process to provide an assessment of how likely such occurrences are. If it is extremely unlikely that a disturbance on the line would only affect the number of zeros in one part of a message, then the parties might be able to agree to share the resultant costs that arise.

Confidentiality, integrity and availability are the key criteria upon which to judge a data security policy:

> "A security policy defines how the risk to and exposure of assets can be reduced to an acceptable level."[79]

No security policy can be completely effective, therefore companies will need to make an assessment of the risk vis-a-vis the cost of implementing the technical security measures[80].

2.3.1 Security Threats

> "The very complexity of the network can pose security problems through lack of a suitably comprehensive security plan, while each type of service provision is vulnerable to particular threats."[81]

This section will briefly identify the external threats posed to communication networks[82]. Such threats arise from either deliberate interference by persons, or from natural/accidental events. The latter category of threats is potentially endless, comprising earthquakes, flooding and other `acts of god'; as well as the spilling of tea over the back of a monitor (!). However, threats from individuals can be distinguished into five areas:

- Destruction of data by sabotage. The most common example over recent years has been the use of `viruses', `time-bombs' and other devices which can be inserted into the software of a system[83].

---

[79] CCITT, Fascicle 8.7 - Rec. X.402 § 6, para.10.1.

[80] Despite the recognised role of risk analysis in computer security, only 25% of companies are reported to carry out such a process; see Hurford, C., "The 1991 Computer Fraud Survey", p.67-71, Proceedings of Compsec 91, 30 Oct.-1 Nov., 1991. For recent surveys of organisational responses to IT security, see Warman, Dr A., "Organisational Computer Security Policies", L.S.E, London, 1991; and "IT Security Breaches Summary", NCC (in conjunction with the DTI and ICL), 1992.

[81] ICC paper, op.cit. supra n.11, at p.13.

[82] See also Chapter 3, at 3.3.3, for a discussion of the criminal sanctions that can be taken against the perpetrators of such actions.

[83] See the Computer Misuse Act 1990, s.3, at Chapter 3, at 3.3.3.3; see also 3.3.4.3, for a discussion of the inclusion of virus' clauses within software contracts.

- Unauthorised access, `hacking', or line tapping, has become increasingly common, as international networks has spread. It can either occur for the purpose of obtaining confidential information, or in order to manipulate data[84].

- Eavesdropping activities enable a person to find out what data is being communicated, thereby breaching confidentiality; however, the eavesdropper does not directly interact with the data[85].

- Theft does not usually apply to data, since it is usually copied rather than permanently removed[86]; however, the removal of network-related equipment is a continuing issue.

- Unauthorised use occurs when an authorised user makes use of the system for unauthorised purposes, such as running a private business. Such actions can be seen as akin to personal use of the company telephone, and might not be considered a particular threat; however, cases have occurred where substantial unauthorised use accounted for more of the system's processing capacity than legitimate use[87].

2.3.2 Transmission Interference

The previous section focused on security threats created by the actions of persons either within the organisation, or externally. However, the confidentiality, integrity and availability of data can also be compromised by the communication process itself. Such impairments can be broadly defined as random and non-random events; the latter obviously being easier to take preventative measures against. This section gives an overview of such threats.

The major form of random interference on telecommunication lines is `noise'; of which two major forms can be distinguished[88]. `White noise'[89] is the term used to describe the interference created by the natural movement of electrons within the telecommunication channel. The amount of movement, and interference, is directly proportional to the

---

[84] Eg. the `Revlon case', where a company, Logisticon, used its authorised remote access to activate data-scrambling viruses to prevent use of the software it had developed within Revlon's system. See further ACCL, Vol.8, No.1, at p.1-2.

[85] ICC 1990, op.cit. supra n.11, distinguishes between `passive' wire tapping, such as electronic eavesdropping, and `active' wire tapping, where data can be altered.

[86] See further Chapter 3, at 3.3.3, on theft of information.

[87] Hurford, op.cit. supra n.80.

[88] Other random impairments include cross-talk, echoes, intermodulation noise, phase jitter and radio signal fading; see further Black, op.cit. supra n.31, at p.160-168. See also Bender, op.cit. supra n.3, at p.2-108.

[89] Also known as Gaussian noise, background, thermal or hiss; Ibid., at p.160.

temperature. The second form of noise is known as `electrical' or `impulsive' noise, and is interference caused by signals emanating from other, external sources: for example, radio frequency interference stems from microwave or radar transmissions; while electromagnetic interference can be caused by air- conditioning units.

The appearance of such `noise' is not necessarily a significant problem in voice communications, because humans have the ability to make a conversation intelligible by filling in any missing gaps. In data communications, where the data is highly structured, distortions created by noise could create significant problems. However, such problems can be identified through error detection procedures within the communication protocol, manual monitoring or software-auditing procedures, and then the message can be re-transmitted.

The major non-random problem of telecommunications is `attenuation'[90]. This is the fundamental physical fact that a signal will lose power over distance. Such a phenomena is predictable, and therefore communication links are always provided with a series of amplification points, at various intervals, to regenerate the signal. However, an additional problem created by attenuation is the fact that such amplification not only boosts the signal, but also any noise on the line. In digital systems, such a problem does not exist, because the interval-unit simply re-creates the appropriate pulse, rather than amplifies the received sound wave.[91]

The problem of transmission interference during communication is exacerbated because of four additional factors arising out of the process:

- The distance between computers;
- transmission over hostile environments[92];
- number of components involved in the transmission;
- and lack of control over the process[93].

Despite this array of physical transmission impairments, there exist a range of techniques which are able to mitigate, if not remove, such distortions[94]. Indeed, the fact that such data communication impairments have been identified enables the user to take appropriate precautions, not only through technical procedures, but also through internal monitoring of messages received.

---

[90] Other non-random impairments include delay, harmonic distortion, spacing or marking distortion; see further Black, op.cit. supra n.31, p. 168-172.

[91] See NCC, op.cit. supra n.3, at p.15.

[92] Eg. microwave links can be distorted by varying weather conditions.

[93] See Black, op.cit. supra n.31, at p.155.

[94] For a detailed exposition of such error control methods, see Ibid., at pp.172-191.

2.3.3 Data Security Procedures

When establishing a network security policy, companies need to consider two key aspects:

- Procedures to protect the data when in the network[95], and
- procedures to restrict use of the network.

The technology that comprises the data communications channels can obviously have an impact on the security and reliability of a network. Networks can be designed to meet a specified criterion of resilience. The use of fibre optics[96], for example, from a data security aspect, means the absence of electromagnetic interference, they are difficult to tap and they do not emit radiating signals, therefore preventing eavesdropping. In addition, the problem of `noise', identified above, is worse under analogue networks, than digital.

The military origins of packet switching means that the PSDN is designed specifically to achieve disciplined and reliable communications, including error detection, recovery procedures and data flow controls. Packet switching divides a message up, so that in the event of line tapping, only a parts of a message may be picked up by the perpetrator. In addition, the switching nodes have an in-built ability to send transmissions down different routes according to network congestion, or the failure of an individual component.

The means of connection to the network can also impact on the level of security. Leased lines provide for a permanent connection, and therefore can be monitored and `conditioned' for more reliable performance and fewer errors. A dial-up connection to a packet-switched network could lead to the introduction of noise, which could distort the data. From a different perspective, however, dial-up connections give greater flexibility to the user, since a failed circuit only requires the user to redial; while a leased line would require more substantial recovery procedures.

The choice of communication protocol, within which the data is sent, is an important aspect

---

[95] See further Caelli, W., D. Longley, and M. Shain, *Information Security Handbook*, Macmillan Stockton Press, 1991; Davies, D.W., and W.L. Price, *Security for Computer Networks*, John Wiley & Sons, 1984; Slater, Ken, *Information Security in Financial Services*, Touche Ross/Macmillan, 1991; Proceedings of `Managing Network Security in the 90's', Conference, London, 13 Sept., 1991, and Humphreys, E.J., "Open Systems Security, Paperless Trading and the Single European Market", British Telecommunications plc, Feb. 1987.

[96] "the communication of signals by the transmission of light through extremely pure fibres of glass or plastic", Longley & Shain 1989, op,cit. supra n.2. To date, the introduction of fibre optics has primarily been over the long-distance parts of the network, the first transatlantic optical fibre cable was laid in 1988; see further Saxby, op.cit. n.6.

of network security, such as the X.400 message-handling standard[97]. In addition, security procedures are built into messaging standards. Within EDIFACT, for example, each message contains an `Interchange Header Segment' which contains a sender identification field (including an address for reverse routing); a password field (which can be encrypted) and control information[98]. The control information is repeated in the `Interchange Trailer Segment' as a check[99].

In regard to access to the network, in terms of the development of networked systems, the fear of unauthorised access has resulted in the establishment of numerous closed user groups within various trade sectors, operating between long-term trusted trading partners[100].

One of the most secure means of ensuring message authentication, as well as protecting the confidentiality of the message contents, is the use of cryptographic techniques[101]. Such techniques involve transforming the plain text, or authentication code, using a complex algorithm, into `cipher' text. The success of this techniques depends upon two factors:

- The algorithm is too complex to be able to discover by random computational techniques, except over an unreasonably long period of time;

- the encryption key, that transform the data, is kept protected from unauthorised use: key management issues[102].

---

[97] Eg. X.400 includes Message Authentication Codes (MAC), Manipulation Detection Codes (MDC) and CCITT X.401 (security level flags of the message handling system); see Hill, R., op.cit. supra n.35.

[98] The control information contains certain key fields identified by the user. The information in those fields is "combined according to a mathematical procedure (know as an algorithm) and a so-called `checksum' is calculated. This checksum is appended to the data fields in the message. At the receiving end the checksum is recalculated and compared with the received checksum." The checksum information can also be encrypted for higher protection. ICC, op.cit. supra n.11, at p.18.

[99] See further Berge, J., "EDIFACT - a technical introduction", pp.63-78, in Gifkins, op.cit. supra n.49.

[100] Eg. SWIFT in the financial sector. Security techniques and routines are being established for the OSI reference model (eg. IS 7498/2)

[101] "the process of transforming data to an unintelligible form", Dictionary of IT, op.cit. supra n.3. Cryptography "embodies principals, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use", ISO 7498-2-1988(E) § 3.3.20.See Chapter 3, at 3.3.2.4 for a review of regulations restricting the use of encryption.

[102] The need for secure key management has led ISO to adopt an international standard (IS 8732); see Fischer, A.M., "Electronic Document Authorization", 1990; the concept of `Trusted Third Parties' is also being developed; see further Lindberg, Agne, *Electronic Documents and Electronic Signatures*, IRI Papers: The Institute of Legal Informatics, University of Stockholm, Sweden; Goebel, J.W., "The `Trustworthy Third Party' within the Security System", at 3., in *Concepts, Applications and Activities*, a TeleTrust Publication; Andersen, Dr M.B., "The Danish Teletrust Proposal for a Centre-Certifying Authority", p.88, The Computer Law and Security Report, Vol.8, No.2, 1992; and Baum, op.cit. supra n.16, at Chapter 4.

Currently, the two major encryption methods are symmetrical[103] and asymmetrical[104]. The former involves the same secret key being used at both ends of the communication link. This can obviously create serious key management problems in large networks, covering multiple users. In asymmetric encryption, use is made of a matching pair of cryptographic keys, one for encryption, the other for decryption. The decryption key is kept completely secret, while the other is made available to those to whom you wish to communicate. The nature of the algorithms will not enable the private key to be discovered from the public key. This asymmetric method is seen as having particular application as a means of ensuring secure authentication (electronic signatures), which can not be repudiated[105]. Both methods can also be used together, symmetrical encryption for the message and asymmetric for the authentication component[106].

The implementation of audit procedures should also play a critical role in ensuring both technical and legal security[107]. The traditional financial audit inevitably involves information security, whether the accounts are maintained on paper or computer. Therefore, a duty to maintain adequate computer security measures can be implied into a firm's duty to maintain and present proper accounts. System audit techniques are now well established and, if carried out on a periodic basis, can enable users to have considerable confidence in network reliability and performance; although, the extent of the information provided by such an audit can vary considerably[108].

In terms of legal security, audit procedures enables compliance monitoring with both legislative regulations and contractual obligations; for example:

---

[103] Eg. the US Data Encryption Standard (DES), adopted by ANSI and ISO; see "Understanding DES: The Data Encryption Standard", p.200.101-124, *Standards, Policies, & Regulations: Section Guide*, McGraw-Hill, 1989. Within the OSI model there are standards for the incorporation of encryption devices; eg. ANSI X3.105-1983, `Data Link Encryption', for each communication link.

[104] Eg. RSA (Rivest, Shamir and Adleman) and Fiat-Shamir.

[105] "The Non-Repudiation Service...provides proof of the origin or delivery of data in order to protect the sender against the false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent." Introduction, *Working Draft Non-Repudiation Framework*, ISO/IEC JTC1/SC21, Project 97.21.9 Q53 (1989). See further Chapter 5, at 5.3.4. Also Reed, C., "Authenticating Electronic Mail Messages - Some evidential problems", p649-660, Modern Law Review, Vol.52, September 1989; Lindberg, Agne, op.cit supra n.102, at p. 48-52 and Shain, M., "How secure is EDI", p.77-90, Proceedings of EDI and the Law Conference, November, 1990. For additional protection, see also Chaum, D., "Undeniable Signatures", pp.204-209, Proceedings of Compsec 89, London, 11-13 October 1989.

[106] Symmetrical encryption is a much faster process, and is therefore more efficient for long messages.

[107] Hurford, op.cit. supra n.80, states that 67% of respondents make use of internal audit procedures for computer security; however, "more computer-literate auditors are needed to help users and management appreciate the increasing risks which computing presents", at p.71. See also Quest, P., "Computer Fraud - The auditor's approach", pp.19-22, The Computer Law and Security Report, Vol.6, No.3, 1990; Bentley, D.F., "Computer auditing - an aid to fraud investigation", pp.250-256, Computer Law & Practice, Vol.7, No.6, 1991; and Lindup, K.R., "Computer Audit - a threshold", pp.17-21, Computer Audit Update, October 1991.

[108] Eg. INS's Tradanet EDI service offers an audit record of the moment a message is placed in the recipient's mailbox, and moment it was retrieved. See also Brunet, Christophe, "Artificial Intelligence in EDI", pp.93-101, Proceedings of '91International Conference on EDI, 7-8 November, 1991, who discusses the use of `expert systems' to provide users with a network management tool, to enable fault reporting and diagnostic testing etc.

- Data protection audits to monitor the changing uses made of personal data, and therefore maintain relevant registration requirements, as well as the ability to fulfil data subject access requests[109];

- intellectual property/confidentiality audits to ensure that all licence agreements are being complied with, that sufficient documentation is maintained of ownership, and that confidential information is adequately distinguished[110];

- computer crime audits of employee authorisation codes, to enable prosecution for unauthorised access under the Computer Misuse Act 1990[111].

In addition, the submission of administrative data to governmental authorities (eg. Customs and tax returns) can be made electronically in certain countries, and in such situations, the relevant authority may wish to audit a company's computer system to check reliability.

The current state of security technology and consultancy is such that data users have the ability to implement significant safeguards against data corruption etc., based upon a pre-determined requirement for `commercially reasonable security'. However, it is important, when assessing data security requirements, that companies bear in mind the following:

> "...each time a new system or tool is produced, our more or less conscious attachment to tradition leads us to expect guarantees which were previously not only never fulfilled but were not even asked for"[112]

2.3.4 Standardisation

In recent years, in reaction to data user fears regarding data security, there has been a movement towards the creation of national and international standards regarding the security of IT products and systems. The US Department of Defence's, Trusted Computer Systems Security Evaluation Criteria (TCSEC), commonly known as the `Orange book', was the first major attempt to laid down standards regarding the level of security required within an IT environment[113].

---

[109] See further Chapter 4, at 4.4.2.

[110] See further Chapter 3, at 3.3.1.1. Eg. LAN Auditor Software Package.

[111] See further Chapter 3, at 3.3.3.3.

[112] Martino, A.A., "Paperless Trade: Legal and Techincal Standardization Problems", paper presented at COMPAT 88, Hague, Holland, 29 Feb.- 2 Mar. 1988.

[113] DOD 5200.28-STD (26 December 1985).

In the UK, in August 1990, the Department of Trade and Industry issued details of a new national scheme for the security evaluation and certification of IT systems and products. The Scheme initially operated on a pilot basis, becoming fully operational in January 1991.

The Scheme provides for:

- a single standard of security evaluation for both public and private sector IT users[114];
- an internationally recognised certification system.

The certificate is awarded by commercial organisations, Commercial Licensed Evaluation Facilities (CLEFS), under licence from a Certification Body[115].

The criteria used for evaluation, the Information Technology Evaluation Criteria (ITSEC)[116] have been jointly developed by the UK, France, Germany and the Netherlands. It is hoped that such harmonisation will eventually be adopted as a European Community standard[117]. However, the European Security Forum, a 60-member group of large commercial data users, has recently spoken out against the proposal, rejecting "the idea that the same security principles are applicable in the commercial, government and defence sectors"[118].

It would seem, therefore, that the future of such standardisation schemes will depend on their acceptability among commercial data users. Alternatively, such standards could form the basis of a statutory regulation specifying a minimum level of security that data users must ensure[119]. In the US, the Comptroller General of the United States has recently decided that "[Federal] agencies may create valid obligations using EDI systems which meet NIST standards for security and privacy". This decision will obviously have a `filter-down' effect on the use of such standards in the private sector[120].

2.4 Legal Impact

The advantages of a traditional paper-based system of communication can be identified as

---

[114] The evaluation procedure can be applied in a number of ways: system assessment; product certification; service level definition; certification of correct operation of computer based systems, and public interest/regulatory system certification: See Marsh, S., "Application of IT Security Evaluation and Certification", pp.107-115, in Proceedings of the `Data Security and the Law' Conference, London, 8 May, 1992.

[115] The joint certification body is operated by the Communications-Electronics Security Group and the Department of Trade and Industry (DTI). See generally Herson, D., "Security Evaluation and Certification", p.17-24, Proceedings of the `Data Security and the Law' Conference, London, 5 July, 1991; and also ITSEC UK Certified Product List, UKSP06, 1 January 1992.

[116] Publication No.1, UKSP, Issue 1.0, DTI, 1991.

[117] See European Commission document `ITSEC' (version 1.2) issued in June 1991 by DG-XIII.

[118] "Users brand government security draft irrelevant", Computing, 10 October 1991.

[119] See further Applied Computer and Communications Law, p.2, Vol.7, No.2, February 1990 and Rowe, H., "The UK Computers (Compensation for Damage) Bill'", p.6-7, ACCL, Vol.7, No.8, September 1990.

[120] Decision: `Use of Electronic Data Interchange Technology to Create Valid Obligations'; B-245714, December 13, 1991.

stability, dependability and tradition. On the other hand, the use of paper is expensive, slow to use and has a tendency to breed! When companies consider implementing electronic messaging, it is necessary to consider what quasi-legal impact that such data communications can have on the way a business operates:

- Electronic messaging techniques can reduce the chance of certain traditional sources of legal dispute from arising;

- while fear of legal-regulatory restriction can lead a company to reorganise its structure.

With regard to the first point, one of the major benefits of electronic messaging is the speed with which information can be transferred through a trading cycle, both intra-company, inter-company and to the various third parties involved, such as insurers and carriers. The increased speed with which data can be disseminated allows parties to adjust to changing circumstances quicker, with the increased possibility of modifying production schedules. Such speed may mean that fewer cancellation claims are brought.

Trading partners will also be able to receive information at an earlier stage in the transaction process. This will enable early problem recognition, such as delivery, and therefore possible adjustment and resolution at a more acceptable stage for both parties.

EDI linkages will mean fewer transcription errors, and this will inevitably lessen the potential ground for dispute. It can also mean that changes in pricing rates in Company A can be sent automatically to Company B, enabling immediate adjustment and recognition in the buyer's costing system.

In international trade, the absence of the right documentation can cause delays at the port of entry and expose the goods to the risk of deterioration and damage, and may account for high demurrage costs. The ability to send data to the relevant third parties, particularly Customs authorities, can considerably speed up delivery, payment and lower the chance of deterioration and damage[121].

Reorganisation, as a response to potential/actual legal regulation, has been shown in a survey carried out of 152 US Management Information Systems (MIS) managers. The survey suggested that:

- Over 60% of the respondents saw TDF regulation as a potential problem rather than current[122];

---

[121] See Anthony, C.G., p8-9, "Paperless Trading - The Legal Problems of Industry", Proceedings of CELIM Conference, 'Paperless trading & the law in the EEC', Brussels, 17-18 March 1986.

[122] See also Author's survey, at Appendix A, which shows the same result.

- 30% viewed TDF regulation to be a current obstacle to the use of international data communications;
- 53% of the companies had carried out some form of study on the impact of TDF regulation on their operations, and
- 20% of companies had actually implemented policy/procedural changes to deal with TDF regulation[123].

The study then went on to review the organisational strategies adopted by the 20% of respondents that had implemented policies designed to overcome any TDF regulations, actual or perceived. Five strategies were distinguished, although a mixture of them had usually been embraced:

(1) The re-organisation of data processing operations, often involving the decentralisation of certain IT features, such as processing and application development; while centralising control over the communications infrastructure[124].

(2) The duplication of certain types of data and/or systems in the regulating country. Data is often duplicated where it is seen as involving privacy or national security issues. Systems require duplication in countries which require the use of domestically manufactured equipment and software[125].

(3) The use of third-party/remote computing services for processing. The report noted that, based on the experiences of the respondents, the use of the third-parties "may reduce the amount of control over data security, but in return, the corporation is less susceptible to the problems associated with TDF regulation".

(4) A reduction in the company's data requirements, achieved through evaluations of existing corporate information flows. This is an extremely effective and worthwhile strategy, for general company efficiency as well as reducing dependency on TDFs; however, it is also involves a large management time-commitment.

(5) The use of alternate communications channels, such as the distribution of magnetic tapes etc[126].

It was also recognised, however, that the adoption of these strategies were often linked to

---

123 Kane, M.J. and D.A. Ricks, "The Impact of Transborder Data Flow Regulation on Large United States-Based Corporations", p24, The Columbia Journal of World Business, Vol.XXiV, No.2, 1989.

124 See also Greguras, Fred M, and Richard Sizer., "Impact of transborder data flow restrictions on cash-management services", p.22, Information Age, Vol.9, No.1, January 1 1987: companies "restructure data processing operations form a centralized to a decentralized function".

125 Eg. Brazil, see further Chapter 3.4.

126 Ibid., at p.26-28.

wider developments in the use of data communications by companies; for example, the cost of storing data at duplicate facilities has fallen considerably over recent years.

2.5 Comment

Data communications has evolved considerably over the past two decades, from simple bulk file transfers to complex X.400 message-handling systems. These developments can be seen to have had two significant consequences for the legal security aspects of data communications.

On the one hand, the movement towards structured messaging, based upon internationally agreed standards, enable a much greater integration between a company's internal data processing applications and the communication process. With the creation of electronic representations of standard business documents, such as the invoice and purchase order, Company A can place an order directly with the order processing system of Company B, without the need for any human intervention. This can lead to significant improvements in efficiency, but also gives rise to increased risk, in the event that an intervening event occurs, and therefore potential liability.

However, on the other hand, the development of new communication protocols and message standards; as well as the possible introduction of artificial intelligence (ie. expert systems) into the front-end of business applications, can provide for a level of reliability and confidence in the communication process not previously possible. Network performance statistics, for example, do seem to suggest that network reliability is extremely high[127], especially when compared to traditional paper.

The security threats to data communication systems can be expected to multiply as the use of such techniques spread. As electronic messaging becomes adopted by small and medium-sized enterprises, the technological and commercial sophistication of the users is likely to decline; relationships will become increasingly transitory, between greater numbers, for an ever increasing number of purposes. These developments are already leading the trend towards open systems, outlined above. However, such development will pose greater security risks, both technical and legal[128].

Totally secure data communications is neither possible, nor desirable, since in a commercial environment it is important to balance the risks against enabling reasonable access to the facilities and applications. Cost, especially for small-medium sized enterprises, will also be

---

[127] Eg. David Ray, New Zealand Customs, states that their EDI system, CEDI*FIT, run over the GE's network, had experienced 99.98% reliability, quoted at 7-8 November 1991, '91 International Conference on EDI, Seoul, Korea.

[128] See for example, Draper, J., "Open networks and security", pp.330-337, in Proceedings from COMPAT'89, 3-5 April 1989 and "Security in a multi-owver system", proceedings of Tedis Workshop, Brussels, June 20-21, 1989.

an important criteria in implementing data security procedures.

The implementation of data communication techniques into company operations requires close co-operation between technical, commercial and legal staff, to ensure that each individual concern takes appropriate account of the environment with which it interacts. Failure to take a broad view can lead, for example, to legal staff drafting contracts which deter potential trading partners, based on an inadequate knowledge of the technical processes that underlie the system.

Chapter 3 **LEGAL CONTEXT**

The topics reviewed under this section are seen by the author as being associated to the main subject of this thesis, data communications; as well as being linked to the central theme of the work: Legal security. However, this survey is not intended as a comprehensive consideration of the individual topics.

3.1 Public International Law

As noted in the introduction, telematics is the supreme international medium. However, where data communication flows cross national borders, questions of international law can become involved; both public and private. Public international law is "that system of law whose primary function it is to regulate the relations of states with one another"[1], as contained in various international treaties.

---

[1] Wade, E.C.S., and A.W. Bradley, *Constitutional and Administrative Law*, p.10, (10th Ed.) Longman 1986.

Data flows out of a country can potentially have a significant impact on the economic, security and cultural life of a nation, and therefore this issue has led to a desire in certain countries to control such data flow[2]. Other countries, particularly the United States, have been extremely concerned to prevent the spread of such restrictions to the free flow of data. This section reviews the international legal framework covering what has been termed: 'the right to communicate' under public international law[3].

Article 19 of the United Nations Declaration of Human Rights, which was unanimously adopted by the UN General Assembly on 10 December 1948, states:

> "Everyone has the right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers"[4]

In addition, around 69 countries have adhered to the UN International Covenant on Civil and Political Rights[5]; Article 1(3) of which states:

> "Everyone should have the right to freedom of expression; this right shall include the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice"

By adopting the Covenant, states agree to accept the principle of freedom of information as equivalent to a treaty obligation, and therefore the state has a positive obligation to comply with its terms[6].

Both the above instruments do, however, allow for exemptions from the principles. Article 29 of the UN Declaration states that governments have a right to restrict the application of a right "for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic

---

[2] For a review of such controls, Section 3.5 below.

[3] See generally, Feldman, Mark, "Commercial Speech, Transborder Data Flows and the Right to Communicate under International Law", *The International Lawyer*, vol.17 no.1 (winter 1983), pp87-95 and Houston Putnam Lowry, "Transborder Data Flow: Public and Private International Law Aspects", *Houston Journal of International Law*, vol.6 part 2 (1984), pp159-174.

[4] Universal Declaration of Human Rights, G.A.Res.217, UN Doc. A/810 (1948)

[5] International Covenant on Civil and Political Rights, G.A.Res.2200, 21 UN GAOR Supp. (No.16) 52, UN Doc. A/6316 (1966), came into force on 23rd March 1976.

[6] Treaties and Conventions are primary legal instruments (ie. between governments), such that an individual can take action against the state for a breach. For UN treaties, an action is taken to the International Court in The Hague.

society". The Covenant also allows for an exemption on grounds of national security.[7]

It is primarily upon the basis of the UN Declaration and similar international legal instruments, that countries, such as the US, have tried to campaign against the appearance of communication restrictions:

> "Americans tend to be in the vanguard of those urging as little interference as possible in the free flow of data across borders. It is no disrespect to say that this doubtless sincere philosophical conviction also happens, providentially, to accord with the economic interests of the United States."[8]

However, the rapid growth of telecommunications and the changing nature of the technology has led certain developing countries to demand a reformulation of the traditional `free flow' principle to take into account the needs of countries to preserve cultural integrity and protect them from cultural imperialism. For example, particular concern has arisen over the use of satellite technology for Remote Earth Sensing (RES), enabling the industrialised nations access to information, such as a third-world country's crop yield or the existence of certain mineral deposits, unobtainable by the country in question.

In 1978, such concerns resulted in the adoption of resolution by the United Nations General Assembly calling for `A New World Information Order', based on the following principles:

> "(1) Free circulation, and wider and better balanced dissemination of information;
> (2) change LDC's from dependence to interdependence and co-operation; and
> (3) equal dialogue between differing societies."[9]

A similar viewpoint was also adopted by the Intergovernmental Bureau for Informatics (IBI)[10] in 1981:

---

[7] Ibid., at Article 19. The International Telecommunications Convention, Malaga, Torremolinos, Oct.25, 1973 [TIAS 8572], gives State's the right to intercept communications "which may appear dangerous to the security of the state, or contrary to law, public order or decency"; see 3.3.1 below.

[8] Kirby, M., `The Morning Star of Informatics Law and the need for a greater sense of urgency', paper presented at the Intergovernmental Bureau for Informatics, Rome, Italy, 26-29 June, 1984. In the US, the free flow of commercial information has been recognised as falling under the protection of the First Amendment of the Constitution: see *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976).

[9] Lowry, op.cit. supra n.3, at p.165. See also Miller, A.P., "Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age", pp89-144, Columbia Journal of Law and Social Problems, 20:89, 1986

[10] Before achieving independent status within the UN system, the IBI was originally part of the UN Educational, Science and Cultural Orgainsation (UNESCO). It has around 35 members of whom all, except Spain and Italy, are developing countries.

"The right to information such as it is recognised by the Universal Declaration of Human Rights and international treaties has acquired, due to the technological revolution, a scope which is qualitatively and quantitatively different from that which prevailed when they were adopted. The concept of the `right to information' needs to be reinterpreted in the light of changes due to informatics."[11]

Despite these declarations from the Less Developed Countries (LDCs), no significant attempts have subsequently been made to re-issue an amended version of UN Declaration, Article 19.

Within a European context, the 1954 European Convention on Human Rights, drafted by the Council of Europe, is a `primary legal instrument'[12]. In 1970, in *Internationale Handelsgesellschaft v. EVSt*, the European Community Court of Justice stated that the Convention on Human Rights forms an integral part of the general principles of EEC law[13]; a subsequent decision has affirmed that the Convention would form the basis for the development of civil rights with the European Community[14].

With regard to the freedom to communicate, Article 10 of the Convention, states that there is a right to freedom of expression "without the interference by public authorities and regardless of frontiers"[15]. However, the Article is subject to certain exceptions, such as in the interests of public order[16].

Overall, as with other aspects of international law, two answers can be given to the question: does a `right to communicate' exist? The answer is positive, in the sense that the above international instruments are framed widely enough to cover data communications; however, the exceptions provided for would also seem expansive enough to mean that state regulation could in many cases be justified. Significant debate on these issues was heard during the 1970s and early 1980s[17], when significant fears of restrictions existed. As such fears have subsided, and substantial data flow restrictions have failed to materialise, public international law issues have

---

[11] Declaration of Mexico on Informatics, Development and Peace adopted by the IBI, June 23, 1981: para.10.

[12] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950. An individual can take a case to the European Court in Strasbourg; eg. the recent case against the UK government over `Spycatcher' restrictions.

[13] Case 11/70 [1970] E.C.R. 1125.

[14] ECJ, 13.12.1979, Case 44/79. The Convention is also officially recognised by the Council, the Commission and the European Parliament.

[15] See *X and Church of Scientology v Sweden*, 16D and R68, 73 (1979), on Art.10 of the European Convention on Human Rights.

[16] For the extent of such restrictions, see The Sunday Times Case, European Court of Human Rights, 26th April 1979.

[17] Eg. Cocca, A.A., "Human Condition and Communications - the Right to Communicate", p15, Transnational Data and Communications Report, May 1988.

generally disappeared from the policy debate.

3.2 European Community Legal Framework

For the UK, membership of the European Community has the greatest influence on general economic activity, including the development of commercial data communications[18]. Throughout the thesis, the impact of particular policies and initiatives emanating from the European Community will be discussed in detail. This section provides a brief introduction to the scope of European Community activities.

The principal objective of the European Community, established by the `six' in March 1957, is to create an open trading environment, a `common market'. This objective was given a significant boost under the creation of the `Single Market Programme', in 1987[19]. The prime objective of this programme is the "completion of a fully unified internal market" by 1 January 1993[20]. The European Community legal framework, within which the `internal market' will arise, is based on a number of different legal sources: Regulations, Directives, decisions, recommendations and opinions[21].

The European Community operates through both `positive integration', where common policies are established[22]; and `negative integration', where obstacles to trade between Member States are removed. The 1985 `White Paper' identified three forms of obstacles to trade:

- Physical (eg. border controls),
- technical (eg. different regulations and standards),
- and fiscal (eg. administrative formalities).[23]

---

[18] See, for example, Commission Communication, Working Plan for Creating a Community Information Market, COM(85) 658 final, of Nov. 29, 1985.

[19] In 1985, the European Commission published the `White Paper': `Completing the Internal Market', COM (85) 310. This led to the signing of the Single European Act, OJ L 169 (1987), which came into force on 1 July 1987.

[20] SEA, ibid, at Art.8a defines the `internal market' as: "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaty". The EC is currently limted to a membership of 12, until completion of the `Single Market Programme'. After that date, a number of countries, both from the EFTA (eg. Sweden) and Eastern Europe, have applied to join.

[21] Directives bind Member States as to the ends, but not as to the means of implementation; in contrast with Regulations which bind Members in every respect to the letter of the Regulation. In addition, European Court decisions and international treaties to which the EC accedes are also sources of Community law. See generally, Mathijsen, Professor P.S.R.F., *A Guide to European Community Law* (4th edit.), Sweet & Maxwell/London 1985; Wyatt, D. and A. Dashwood, *The Substantive Law of the EEC*, Sweet & Maxwell, 1987, and Wissels, C.M., "European Community Law", pp.10-11, in Meijboom, A.P., and C. Prins (eds.), *The Law of Information Technology in Europe 1992*, No.9 Computer/Law Series, Kluwer, The Netherlands 1991.

[22] Eg. the recent discussions on political union, at the Maarstricht summit.

[23] `White Paper', op.cit. n.19, at paras 11-14.

In terms of removing differences in technical standards and regulations, the EC has moved to a system of "mutual recognition" between the Member States. Where this process proves to be unworkable, the European Commission will then consider the use of legal instruments aimed at the "harmonisation" of regulations.

Certain restrictions to trade can be `justified' by Member States on a number of grounds, including public policy[24] and the `protection of industrial and commercial policy'[25]; however, such restrictions can not be `justified' once a harmonisation measure has been implemented among the Member States.

Within the Treaty of Rome[26], there are five principal freedoms connected to the economic union: Free movement of goods (Arts.9-37)[27]; freedom of movement for workers (Arts. 48-51); freedom of right of establishment (Arts.52-8); freedom to provide services (Arts.59-66) and the free movement of capital (Art.67-73).[28] Based upon these `freedoms', the EC has the power to remove national `measures' that reduce such free movement[29]. With regard to data communications, the freedoms concerning services and capital are of particular interest.

The protection of Article 59, the right to provide services, applies only to firms established within the EEC.[30] However, the EEC Council has tried to expand the scope of the Article. In the 1962 General Programme for the abolition of restrictions on the freedom to provide services, the Council called for the abolition of formal or administrative discriminatory practices that affected foreign nationals.[31]

In 1973, a further directive in this field was issued by the Council, covering the financial institutions sector of the European Community. It applies to all persons, companies and firms

---

[24] Such as data protection legislation, see Chapter 4.

[25] See Case 144/81 Keurkoop v Nancy Kean Gifts (1982) ECR 2853.

[26] EEC Treaty 1957, Cmnd 5179-11, 1972.

[27] Art.9 creates a `Customs Union'; while Art.30-36 prohibit `qualitative restrictions'.

[28] Rudden, B. and Derrick Wyatt, *Basic Community Laws*, Clarendon Press/Oxford 198, at p.24-34, 39-47. See also Moitinho de Almeida, J.C., "Data Flow and Community Law", p.7-22, in Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

[29] Member State `measures' include: "all trading rules enacted by Member States, which are capable of hindering, directly or indirectly, actually or potentially, intracommunity trade.", stated in Case 8/74 *Procureur du Roi v Dassonville* (1974) ECR 837 at 852. However, this general rule has since been qualified in Case 120/78 *Rewe v Bundesmonopolverwaltung fur Branntwein* (`Cassis de Dijon') 1979 ECR 649.

[30] Article 58 states that for a business to be considered established, it must fulfil two criteria:

i) It must be incorporated in accordance with the law of a member state.

ii) It must have its registered office, central administration or principal place of business in the EEC.

[31] The General Programme, 5 J.O.Comm.Eur.32.

that issue commercial information, represent clients before administrative and judicial authorities and advise customers about mergers and general security matters.[32] It calls on Member States to abolish regulations and administrative practices that prevent a company from providing services in a host company under the same conditions as the national of that country. It thus supports Article 7 of the Treaty of Rome, which prohibits all forms of discriminatory manifestations.

Two European Court of Justice cases have also given an indication of how the Court regards the scope and applicability of Article 59. In *Procureur du Roi v Debauve*[33], it was decided by the Court that the intention of Article 59 was to abolish discrimination against providers of services based on nationality or country of establishment. Therefore, a law that applies uniformly against the provision of a service does not violate Article 59.[34]

In *Coditel v Cine Vog Films*[35], it was stated that intellectual property rights were excepted from Article 59 prohibitions, since Article 222 of the Treaty of Rome states that European Community law should:

> "in no way prejudice the rules in Member States governing the system of property ownership".

Therefore, the freedom to provide services could not limit the property interests of an intellectual work, unless such use of a copyright was in fact a disguised restriction on trade[36].

Free movement of capital (Article 67-73), within the EEC, is obviously of relevance to the issue of transborder data flows. In particular, Article 71 calls for the removal of restrictions on capital movements and currency exchange. In a number of recent surveys looking at the extent of TDF, the most common reason for companies to transfer data abroad is associated with financial management.[37]

Unfortunately, there are limitations to the scope of these articles. Capital is normally seen as

---

[32] Activities of Banks and Other Financial Institutions, 16 O.J. Eur.Comm.(No.L 194) 1 (1973), art.2, app.1.

[33] Case 52/79 *Debauve* (1980) E.C.R.857.

[34] See also *Sacchi* [Case 155/73 (1974) E.C.R.409], where the European Court took a broad view of the ambit of Article 59.

[35] *Codital v Cine Vog Films* 1980 E.Comm.Ct.J.Rep 881.

[36] With regard to intellectual property rights, the European Court has distinguished been the existence of rights and their exercise; see Case 24/67 *Parke Davis v Centrafarm* (1968) ECR 55, at 71.

[37] IBI "IBI World Survey of National Policies and Company Practices concerning Transborder Data Flows", TDF 110 (Rome, IBI, 1983). Also, Business International, *Transborder Data Flow: Issues, Barriers and Corporate Responses*, p9 (New York, BI, 1983).

"any asset, good or possessory interest used to accumulate profit or wealth"[38]; however, within the European Community, capital has been given a more limited meaning and scope under Article 67. In *Regina v Thompson*[39], the European Court defined capital simply as a means of payment.

The ECC Council's `First Directive for the Implementation of Article 67' stated that, in order for Article 67 to apply, the capital must belong to a person who is a resident of a member state.[40] It also only covers the movement of capital and not the transfers or payment related to that capital.

Complementary to the economic `freedoms' established under the Treaty of Rome, another important area of EC law is contained within the competition rules of the Treaty, Articles 85-94. The application of these Articles have had a particular influence on the use of data communications, through the opening up the market for telecommunication provision.

3.3 Telecommunications

> "Initially, the debate concerning legal rules for TDF focused mainly upon questions relating to the standardization of communication channels"[41]

The regulation of telecommunications can take two approaches: the form and technical availability of communications technology and the content of the communication[42]. This section gives a brief overview of the regulatory framework concerned with the former question: the technical provision of data communications services.

The distinction between voice and data communications is important for certain regulatory purposes[43]; although, with the movement from analog to digital transmission, and the recent spread of Integrated Services Data Networks (ISDN), such a technical distinction is no longer relevant. In certain circumstances, a regulatory distinction exists between basic and value-added

---

[38] Cole, "New Challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws", *New York University Journal of International Law and Politics*, vol.17, No.4, Summer 1985: 938.

[39] *Regina v Thompson* 1978 E.Comm.Ct.J.Rep. 2247.

[40] 1959-62 O.J. Eur.Comm.49. Residency, necessary for the protection of Article 67, is fixed by the definition of residence contained in a state's exchange control regulations. A corporation is usually resident if it has a local establishment and its capital movements are related to local production (i.e. its data flows must involve EEC residents).

[41] Rankin, T. Murray., "Business secrets across international borders: one aspect of the transborder data flows debate", p.106, Canadian Business Law Journal, 10 (1985).

[42] See generally Markoski, Joseph P., "Telecommunications Regulations as barriers to the transborder flow of information", p287-331, Cornell International Law Journal, vol.14, no.2, Summer 1981; and Schnurr, Lewis, "Conduit-Content Convergence: Its causes and effects", p.157-173, in E.J. Mestmäcker (ed.), *The Law and Economics of Transborder Telecommunications*, Baden-Baden 1987.

[43] Eg. the UK Class Licence for the provision of Value-Added Data Services, see section 3.3.2.

communications services:

> "In regulatory terms an additional service or a deliberate removal of or addition to a message's information content, over and above any act necessary simply to permit or facilitate its conveyance to its destination in an `accurate, reliable and economical manner', is a value added service."[44]

This can obviously be difficult to distinguish in the vast majority of situations, however, the regulatory difference does not tend to be crucial[45].

3.3.1 International Regulation

International telecommunications are governed primarily under the auspices International Telecommunications Union (ITU), based upon the International Telecommunications Convention[46], which is a part of the United Nations system.

The work of the ITU is divided onto a number of different bodies[47]:

(i) The Plenipotentiary Conference, composed of all member states, meets about every five years and is the highest authority in the ITU;

(ii) The Administrative Council;

(iii) The General Secretariat;

(iv) The Administrative Conferences, both world-wide[48] and regional; and

(v) The Consultative Committees, one dealing with International Radio issues (CCIR) and the other with International Telegraph and Telephone (CCITT)[49]

(vi) The International Frequency Registration Board, which co-ordinates international frequencies and satellite position assignments.

---

[44] Long, C., and David Kerr, Chapter 2: The Licences, at s.2.3.1., in Corby, Michael (General Editor), *Telecomms Users Guide to Regulations*, CommEd Books, 1989.

[45] Eg. the use of international private circuits are covered by CCITT recommendations.

[46] ITU Convention, Malaga, Torremolinos, Oct.25, 1973 [TIAS 8572]. The original convention was the International Telegraph Convention, concluded at Paris, May 17, 1865. 56 *British and Foreign State Papers* 294 (1870). This Convention merged with the International Radiotelegraphic Union in December 1932 to form the ITU Convention.

[47] See generally, Millard, C., and Sa'id Mosteshar, "International Telecommunications", p.10003-10043, in Saxby, S., (General Editor) *The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990.

[48] Eg. the World Administrative Radio Conference, see 3.3.3 below.

[49] See Chapter 2, at 2.2.3.

The regulatory role of the ITU is limited to the technical means of telecommunications, such as communication protocols and interconnection standards; although message content can be an issue in certain areas, such as message security and authentication. The regulations, both general and detailed, are contained within the Convention and Administrative Regulations, in the areas of Telegraph, Telephone and Radio.

The international regulatory framework that has been established for the use of satellite technology[50], is similar to that dealing with international data communications, since both are concerned with reconciling the principle of free flow of information against the various rights of both individual persons, such as `privacy' and the protection of intellectual property rights (eg. copyright[51]); and the concerns of nation states for their sovereignty[52].

The use of satellites for data communications is regulated by a series of decisions and agreements arising within the World Administrative Radio Conferences (WARCs)[53]. These Conferences are primarily concerned with the use of the space segment, and the frequency at which the various services are operated, to avoid interference etc.. One of the most significant decisions came at the WARC in 1971, at which it was decided that any allocation of space segment would not be permanent, in order not to restrict the ability of the LDCs to exploit satellite technology at some point in the future[54]. The current set of regulations under which satellite services operate came into force into force on 1st January 1982.

In addition to the WARCs, the International Telecommunications Satellite Organisation (INTELSAT)[55] and regional organisations, such as EUTELSAT[56], also have an important influence on the use of satellites, since, although not controlling the establishment of new services, such services need to be registered to ensure that no technical harm to existing services could result from the new service.

---

[50] Eg. Direct Broadcasting by Satellite (DBS) and Remote Earth Sensing by satellite (RES).

[51] See Pichler, M.H., *Copyright Problems of Satellite and Cable Television in Europe*, Martinus Nijhoff, 1987.

[52] See generally, Groshan, R.M., "Transnational Data Flows: Is the idea of an international legal regime relevant in establishing multilateral controls and legal norms?", Part I: pp1-30, Law/Technology (4th Quarter 1981); Part II: pp1-37, Law/Technology (1st Quarter 1982).

[53] The first was held in 1963.

[54] WARC-ST Final Acts, July 17, 1971, Res. No.Spa.2-1.

[55] Established on the 24 August 1964, with the objective to provide a satellite service "on a global and non-discriminatory basis". It currently includes around 110 Members States.

[56] The European Telecommunications Satellite Organisation was established in May 1977, and membership is limited primarily to members of the European Conference on Posts and Telecommunications (CEPT) or Recognised Private Operating Agencies (RPOA).

The European Community has, over recent years, played an increasingly important role in determining the nature and structure of the European telecommunications industry[57]. In the early 1980s, the European Commission took two companies to court, concerning significant telecommunication provision issues. The cases were taken under Article 86 of the Treaty of Rome, dealing with `abuse of dominant position'.

The first case involved the refusal by British Telecom to allow private message-forwarding agencies in the United Kingdom from relaying telex messages received from and intended for relay to another country[58].

Firstly, it had to be decided if British Telecom, as a public body, was subject to the competition rules of the Treaty of Rome. The Court found that despite its public sector status, BT was essentially a commercial activity. It was also stated that any regulatory powers that had been given to BT were strictly limited, to such areas as the fixing of tariffs; and the content of the schemes was left to be decided by the company itself. Therefore, the Court found that the particular scheme in question to be part of BT's business activity, and that Article 86 "should be applied to regulations fixing the conditions of use in the field of telecommunications".

The Court stated that Article 86 would apply whether the conditions of the contract were that of a private monopolist or regulations of a public telecommunications authority. It would also make no difference if the activity had state encouragement or was clearly alluded to in the legislation of a member state. Finally, Article 86 prevails even when the PTT says that it is implementing a recommendation by one of the Consultative Committees of the ITU.

The final major issue of the BT case concerns 'value-added services', such as electronic fund transfer. It would seem that the European Court will not allow PTT's to restrict the existence of value-added services, or reserve them for themselves. In the recent *Tele-Marketing case*[59], the Court held that the radio station in question was obliged under Article 86 to provide its transmission facilities to the lessee regardless of the fact that the facilities will be used to provide value-added services to a third party. The lessee acts within European law as long as he is

---

[57] See generally Scherer, Professor J., "European Telecommunications Law", pp.225-242, in Meijboom, A.P., and C. Prins (eds.), *The Law of Information Technology in Europe 1992*, No.9 Computer/Law Series, Kluwer, The Netherlands 1991.

[58] Case 41/83 Italy v Commission (1985) CMLR, at p.386. Known as the `British Telecom case', although it was the Italian Government which appealed the Commission's original decision against British Telecom, while the British Government took the side of the Commission. See Schulte-Braucks, Reinhard., "European Telecommunications Law in the light of the British Telecom Judgement", p39-59, Common Market Law Review, vol.23, No.1.

[59] Case 311/84 Tele-Marketing v Compagnie Luxembourgeoise de Telediffusion, 2 Common Market Law Reports, at p.558, 1984.

willing to pay the corresponding charges, including time or volume sensitive tariffs.[60]

With regard to legislative reform, the European Commission outlined its initial position, with regard to the role of telecommunications in the creation of the single market in the 1987 Green Paper[61]. The three main objectives were:

- Furtherance of the constitution of an advanced European infrastructure[62];
- contribution to establishing a community-wide market for services and equipment of communications technology[63];
- contribution to the competitiveness of European industry and service providers.

Under the European Commission's Telecommunications Services Directive[64], Member States are only permitted to retain telecommunications regulation and/or licensing procedures for certain `essential requirements':

- Security of network operation;
- maintenance of network integrity;
- interoperability of services, and
- data protection[65].

---

[60] See SWIFT v CEPT case, in which PTT's drastically raised the charges for leased lines, by adding a volume sensitive tariff, in order to avoid the expected loss in telex revenues. The Commission held it was an abuse under Article 86. See Ramsey, "Europe Responds to the Challenge of the New Information Technologies: A Teleinformatics Strategy for the 1980's", Cornell International Law Journal, Vol.14, No.2, Summer 1981, p279.

[61] Commission, `on the Development of the Common Market for Telecommunications Services and Equipment', COM(87) 290 final of June 30, 1987. See also Commission, `On the Way to a Competitive Community-Wide Telecommunications Market in the Year 1992', COM (88) 48 final of Feb.9, 1988.

[62] Based upon the establishment of ISDN by all Member States by 1993, and Broadband-ISDN by 1995; see Wiebe, Andreas, "EEC Law and Policy in Telecommunications", p.4, paper presented at `Data Security in Computer Networks and the Legal Problems' Conference, Hannover, 23-24 September, 1991. Satellite communications are also seen as an important component in the development of the network infrastructure; see Commission Communication, `On the Way to European-wide Systems and Services - Green Paper on a Common Approach in the Field of Satellite Communications in the European Community', COM(90) 490 final of Nov.28, 1990.

[63] Eg. Commission Directive of May 16, 1988 on Competition in the Market of Telecommunications Terminal Equipment (88/301/EEC), OJ L 131/73 of May 27, 1988; Commission Directive of June 28, 1990 on Competition in the Market of Telecommunications Services (90/388/EEC), OJ L 192/10 of July 24, 1990, and Council Directive of June 28, 1990, on the Establishment of the Internal Market for Telecommunication Services through the Implementation of Open Network Provision (ONP) (90/387/EEC), OJ L 192/1 of July 24, 1990; Article 1 calls for "harmonisation of conditions for open and efficient access to and use of public telecommunications networks and....services". See generally, Cowen, T., "The deregulation of telecommunications in the European Community", p.202-206, Computer Law and Practice, Vol.7, No.5, 1991 and Singleton, S., "Telecommunications and Competition Law: Recent Developments", forthcoming in Computer Law & Practice, 1992.

[64] op.cit. supra n.63, see also the ONP Directive. The `Equipment' directive requires minimum certification to ensure user security; security of employees of network operators; protection of public telecommunication networks against damage. See further, de Cockborne, J-E., "The EC Commission Directive on Competition in the Market for Telecommunications Services", pp.96-115, *Yearbook of Law Computers & Technology*, Vol.5, Butterworths, 1991 and Barrett, D., "Telecommunications and the EEC: Piecing together a fragmented market", pp.94-114, in Proceedings of `Legal, Contractual, Responsibility & Evidential Issues in EDI, EFT, EM, Fax & Telex Communications', London, 20 February 1992.

[65] Ibid., at Article 1(1), sixth indent. `Data protection' extends to the confidentiality of all information, as well as the issue of

Such requirements may be supplemented where necessary, this could include the integration of any future security standards[66]. However, for packet- and circuit-switched data service providers, the Directive also permits Member States to enforce compliance with additional conditions, relating to:

- Regulations regarding the `permanence, availability and quality of service'; and
- any measures designed to protect `a task of general economic interest' carried out by the PTO, which may be threatened by private service provision.

With regard to the commercial availability of data communication techniques, it would seem that the liberalisation of telecommunication service provision has been of particular importance. In certain countries, liberalisation has led to a significant growth in the number of value-added service providers[67]. These companies are now aggressively marketing their services to business, and can be seen to play a critical part in raising awareness among businesses of the potential role of data communications in commercial operations.

3.3.2 National Regulation

> "Efficient telecommunications services play a vital role in the modern economy. Business relies on them for its commercial prosperity and society generally is becoming increasingly dependent on good communications"[68]

Until very recently, the provision of national telecommunication services has been operated by a single telecommunications authority, usually state-owned. These authorities have often been both the regulator and primary provider of communication services within the country[69].

Such a monopoly position inevitably led to the establishment of a restrictive framework of technical regulations, often designed primarily to preserve their dominant position. In particular, such policies have been aimed at restricting the use of private communication networks: For

---

personal data.

[66] See Chapter 2, at 2.3.4.

[67] See Chapter 2, at 2.2.2.

[68] Government's consultative document, "Competition and Choice: Telecommunications Policy for the 1990's", November 1990.

[69] For a general historical perspective, see ICC report, "Toward greater competition in telecommunications: Basic services and network infrastructure", Position Paper No.17, December 1991.

example, differential pricing policies for telecommunication services[70]; the imposition of inconsistent or narrowly interpreted technical standards upon the providers and users of telecommunication services[71]; and network controls, such as restrictions on the availability of private leased lines[72].

During the 1980s, there was a general trend, among the industrialised nations, towards the liberalisation of telecommunications services. This has led to the removal of many of the types of technical restrictions on the use of international data communications that companies experienced in the 1960s and 1970s, mentioned above. The process could be said to have began in the United States in 1982, with the break-up of the monopoly held by AT&T[73]. The US now has the most liberalised telecommunications environment in the world.

In the UK, the Telecommunications Act 1984 opened up the market for telecommunications equipment and allowed Mercury to compete with British Telecom for the provision of public telecommunication services[74]. The Act also established the Office of Telecommunications (OFTEL), headed by a Director-General[75], to monitor and regulate the development of the telecommunications market. The Act removed BT's role in the licensing procedure, which is now carried out by the Secretary of State for Trade and Industry, in consultation with Oftel.

Similar liberalisation is occurring throughout Europe, particularly within the European Community[76], although at a slower pace, since some governments believe that the provision of telecommunications is an area of natural monopoly and should therefore be kept within state control[77].

---

[70] Eg. in West Germany, the Bundespost moved from flat-rate to volume sensitive charging for private networks. The cost of European public communication networks was criticized in the US for being 2.5 - 5 times that of the US: see US, "International Information Flow: Forging a new framework", p13, 32nd Report by the Committee on Government Operations, No.96-1535.

[71] The `interconnect' issue: eg. users can only use equipment supplied by the national PTT.

[72] Eg. Japan kept two US data processing operations out by denying them lines, see US Report op.cit. supra n.70; while the West German Bundespost, at one time, forced companies to lease a minimum of four lines. However, see Commission Directive on the Introduction of an Open Network Provision for Leased Lines, COM(91) 30 final of Feb.14, 1991, OJ 58/10 of Mar.7, 1991; and Commission press release IP(90)67.

[73] See further Kuwahara, S., *The Changing World Information Industry*, at ChapterII, p.28-40, Atlantic Institute, 1985.

[74] The Government has recently announced its plans to extend the liberalisation process, by completely opening up the market for the provision of public telecommunication services: see White Paper, "Competition and Choice: Telecommunications Policy for the 1990s", Cmnd 1461, HMSO 1991; and "The Telecoms Duopoly - the public policy issues", papers in Information Technology & Public Policy, Vol.9, No.2, 1991. Part of this process will involve modifications to the current PTO licence: Eg. New condition 15.3 will require BT to provide any Service Provider with the ability to re-sell services over its telecommunication lines. See further Woods, A., "The Telecommunication Legal and Regulatory Environment", in the proceedings of the `Telecommunications Contracts' Conference, London, 3 December, 1991.

[75] Currently Sir Brian Carlsberg.

[76] See 3.3.1 above.

[77] See Cowen, T., "Judgement in France v Commission", p.3-5, Applied Computer and Communications Law, Vol.8, No.5, 1991.

Statutory regulation of telecommunications in the UK is concerned with four main issues:

- The running of the telecommunication system;
- the connection between telecommunication systems;
- the connection of equipment to the system
- and the provision of telecommunication services[78].

These issues are regulated via licences required to operate various forms of telecommunications systems, the only exceptions to the need to hold a licence are `stand-alone systems' and internal business systems[79]. The two most significant licences currently in use are for the Public Telecommunications Operators (PTOs)[80] and the Branch Systems General Licence (BSGL) for private network providers[81]. In terms of data communications, the latter is of particular concern.

The first version of the BSGL was issued in 1984, following the Telecommunications Act; however, it was extremely restrictive and complex, and therefore few companies operated under it. It was revised again in 1987. The current Branch Systems Licence was published in 1989 and represents a thorough simplification of the licence. All rules on network configuration were removed, as well as almost all the non-technical restrictions. The remaining technical restrictions are designed primarily to ensure the security, integrity and reliability of the national network. The licence covers four main areas:

- general operating and administrative provisions;
- conditions applying to systems connected to Specified Public Telecommunication Systems;
- limitations on private circuit connections[82]
- and conditions regulating or affecting the terms and conditions upon which the

---

[78] Telecommunications Act 1984, s.5. Telecommunication services are further distinguished as either `communication services' or `services involving the maintenance of a telecommunications service', see s.4(3).

[79] Ibid., s.6. These definitions are fairly strictly drawn. See also the new Class Licence for the Running of Self Provided Telecommunications Systems under Section 7 of the Telecommunications Act 1984.

[80] Telecommunications Act 1984, s.7. The three current UK PTOs are British Telecom, Mercury Communications and Kingston-upon-Hull Communications Company. This position will be changing in the near future following the Government's decision to open up the current `duopoly' arrangement, see White Paper, op.cit. supra n.74. Bodies, such as the British Railway, have already made formal applications for a licence. The licence also covers the provision of cellular mobile communication services. For a detailed discussion of the licence conditions, see Long, Colin D., *Telecommunications Law and Practice*, Sweet & Maxwell/London 1988, or Chapter 9, *Encyclopedia of IT Law*, op.cit supra n.47.

[81] The Class Licence for Branch Telecommunication Systems (BSGL), operating for a period of 25 years from November 8, 1989: `Applicable Systems' are specified in Annex A and the permitted telecommunications service are in Schedule 3. There is also a Class Licence authorising the running of Telecommunication Systems providing Value Added and Data Services 1987 (known as the VADS licence). This latter licence is still in operation, although the 1989 BSGL was designed to incorporate most of its terms, and few companies are actually operating under it.

[82] On 28 June 1991, the Secretary of State amended the BSGL to permit the provision of "any services other than International Simple Resale Services" [Condition 14].

telecommunication service is made available[83].

The licence covers the provision of most telecommunication services[84] and makes no distinction between the type of messages being sent, ie. basic or value-added. Amendments to the licence conditions can be made by Oftel, although the subject matter of the licence (ie. `applicable systems') can not be changed.

A breach of the provisions of the licence itself, such as operating outside the definition of an `applicable systems', is a criminal offence[85]. In addition, a civil court action to obtain a mandatory injunction could arise where the network provider fails to comply with an `order' issued by Oftel[86]; alternatively, third parties could take an action for damages for a breach of duty, where a network provider failed to comply with an order. Legal action could arise because the network provider has failed to comply with a licence condition which has been incorporated into the service contract with the data user[87].

Private sector network providers also generally operate under the Network Code of Practice (NCOP)[88]. The Code's purpose is as a recommended `best practice' for the design of private networks, and it ensures that the integrity and performance of the public network, if connected, is not compromised by the functioning of the private network. The NCOP primarily addresses voice communications between the private and public network; however, non-voice communications may need to ensure compliance with the code in certain circumstances[89].

A national licensing regime also exists for satellite operators. Only six licences have been issued so far in the UK, permitting satellite uplinks for one-way point to multi-point transmissions of `specialised satellite services'[90]. To date, such services have focused primarily on providing

---

[83] Eg. Fair trading requirements may be applicable to potential dominant traders: `Major Service Providers' [Conditions 23-27]. See Chapter 9, p.9049, *Encyclopedia*, op.cit. supra n.47.

[84] The exceptions are programme services, which are regulated under the Broadcasting Act 1990, and short-range radio telecommunication services.

[85] TA 1984, s.5(3)-(6); proceedings may only be instituted by or on behalf of the Secretary of State, or the DG Oftel.

[86] Enforcement of licence conditions by OFTEL, through the use of provisional or final orders, is carried out under ss. 16-19 of the Telecommunications Act 1984. Section 18 imposes a statutory duty upon the licensee to comply.

[87] See Chapter 6, at 6.4.

[88] Published by Oftel, Issue No,1, November 1990. The code has a voluntary status.

[89] Eg. in an interface to a digital service on the public network. See generally, Proceedings of BSGL/NCOP Conference, London, 24 May, 1990.

[90] Eg. Electronic Data Systems (EDS), part of General Motors and Maxwell Satellite Communications. See also new Class Licence to run Telecommunications Systems for the Provision of Satellite Telecommunication Services under Section 7 of the Telecommunications Act 1984; ACCL, p.7-8, Vol.8, No.9, 1991.

video or business television.

As a result of this general process of telecommunications liberalisation, restrictions on the use of data communications arising out of technical issues of access to such services have significantly diminished.

3.4 Data Security Law

3.4.1 Introduction

> "the attention of the criminal lawyers will have to shift away from the integrity of the computer, towards the vulnerability of the information and the enforcement of security and regulatory requirements with respect to that information"[91]

Data security should not simply be seen as a technical process. Companies also need to be aware of the complementary legal aspects of data security. Data security law is concerned with three main areas:

- individual privacy, eg. data protection;
- maintaining rights over the use of data, eg. copyright and patent laws; and
- ensuring secrecy, authentication, integrity and availability of information.

Data security legal issues take two main forms: law that allows a business to take action against those that breach data security procedures, therefore acting as both a deterrent and enabling a business to recover damages; and secondly, law that requires of the business that certain data security procedures be implemented, often in order to protect some third party, such as a consumer[92]. As Arkin has stated, to establish legal security, companies need to embrace "three layers of effort which are, of necessity, interrelated: (1) Private preventive measures...(2) Public enforcement measures...(3) Private enforcement measures.."[93].

Legislative sources of data security law can be sub-divided into three:

---

[91] Wasik, M., "The role of the criminal law in the control of misuse of information technology", p.8, Working Paper No.8, University of Manchester, July, 1991.

[92] Eg. consumer EFT systems have come increasingly to the attention of national legislators: for example, under Article 10 of the Denmark Payment Cards Act 1984, if the Ombudsman is dissatisfied with security procedures then changes have to be negotiated with the institution. Failing that, the Ombudsman can issued an order to comply. See also `Banking Services: Law and Practice', Report by the Review Committee (Chair: Professor R.B. Jack), Cm 622, February 1989, at Chapter 9 and 10, p.75-95.

[93] Arkin, S.S., (ed.), *Prevention and Prosecution of Computer and High Technology Crime*, p.1-3, Matthew Bender, 1990.

- Completely new forms of legislation which can have an impact on data security policies, for example, the eighth principle of the Data Protection Act 1984[94];

- legislation which has been extended or amended to take account of information technology and therefore enhances data security, for example, the Copyright, Designs and Patents Act 1988[95]; and

- `sui generis' legislation which directly addresses information security issues; for example, the US Computer Security Act 1987[96].

It should also be noted that data security law covers not only criminal law, but civil and administrative law as well[97]. Indeed, different national-legal cultures may categorise the same offence as a matter of criminal and/or civil law; for example, copyright legislation is designed to safeguard civil rights, but makes use of criminal sanctions.

However, the lag between the pace of change in technology compared to that of the commercial legislative framework has often been noted[98]. In the absence of legislative dictate, businesses therefore have to construct a secure commercial-legal framework for their data communications through the use of either contractual arrangements, both internally (eg. employment contracts[99]) and externally[100]; or via adherence to codes of conduct[101].

The use of contractual means to enforce data security has a number of advantages over legislative protection. Through the use of a contract, the security obligations owed by each party to the contract are clearly specified. As part of this process, the parties will also be required to determine the level of security they expect of each other and the system as a whole.

---

[94] See Chapter 4, at 4.4.2.

[95] See section 3.4.4.

[96] See section 3.4.2.

[97] Eg. US Comptroller General Decision: `Use of Electronic Data Interchange Technology to Create Valid Obligations'; B-245714, December 13, 1991. This states that federal government "agencies may create vaild obligations using EDI systems which meet NIST standards for security and privacy".

[98] Eg. Martino, A.A., notes that the commercial world tends "to go ahead without taking the legal world into consideration in the belief that sooner or later the real world conquers the legal world", in "Paperless Trade: Legal and Techincal Standardization Problems", paper presented at COMPAT 88, Hague, Holland, 29 Feb.- 2 Mar. 1988.

[99] "It is very easy to underestimate the amount of control exercised by junior clerical staff; most of this is not written down in anybody's procedures manuals and is not incorporated in the computer applications", in Morriss, P.W., "Electronic Data Interchange: Security, Control and Audit", p.81-96, COMPSEC 89, London, 11-13 Oct., 1989. A recent survey found that 50% of respondents had included legal obligations within their security policies; see "IT Security Breaches Summary", NCC (in conjunction with the DTI and ICL), 1992. For a general review of recent employment law issues of relevance to the Computer and Communications industry, see Thomas, D., "Employment Law", ACCL, Vol.7, No.3-5, 1991.

[100] See generally, Napier, B., "Information Security: Contractual Issues", pp.83-94, in Proceedings of `Data Security & the Law' Conference, London, July 1991; and Chapter 6.

[101] See, for example, Stuurman, K., "Codes of Conduct", pp.102-113, in *The Legal Aspects of Computer Crime and Security*, document prepared for the European Commission's Legal Advisory Board [LAB], December 1987.

This section reviews the scope of the non-contractual aspect of this newly emerging field of study, data security law, excluding those issues which form a central part of the thesis.

3.4.2 Security Legislation

Over recent years, the increasing dependency of society on computer systems, paralleled with the growing perception of their vulnerability to external interference, has led to consideration among some legislators of the need for measures dealing specifically with the question of data security: For example,

- The Council of Europe, in a recently published report on `*Computer-related crime*', proposes that:

  > "The Member States could....establish a legal framework which would require manufacturers and users to observe at least a minimum of regulations relating to computer security."[102];

- In Canada, governmental bodies operate under regulations issued in 1986: the `Electronic Data Processing Security Standards and Practices for Departments and Agencies of the Government of Canada'[103].

However, the first significant statutory initiative in this area was the US Computer Security Act 1987[104]. It was passed in order to strengthen existing regulations that had been produced by the Office of Management and Budget, and had been in existence since 1978. It was generally felt that these existing regulations had not be paid sufficient attention, at all levels of government.

The scope of the Act is federal government agencies, and it gives the National Institute of Standards and Technology (NIST) the authority to develop standards, guidelines, and associated procedures for computer systems. In addition, each federal agency is required to:

> "• Provide for mandatory periodic training in computer security awareness and accepted computer security practices.

---

[102] Council of Europe, "Computer-related crime", Recommendation No.R (89) 9, adopted by the Committee of Ministers on 13 September 1989 and Report by the European Committee on Crime Problems; at p.75.

[103] GES/NG1.

[104] Public law 100-235, 40 U.S.C.; see generally Vandenberghe, G., "Computer Security", pp.90-95, in LAB report, op.cit. supra n.101; also *Standards, Policies, & Regulations: Section Guide*, p.120.101-109, McGraw-Hill, 1989.

- Identify each federal computer system and system under development which contains sensitive information, and
- Establish a plan for security and privacy of systems"[105].

The Act defines `sensitive information' as "any information, the loss, misuse, or unauthorised access to or modification of which could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled..".

The Act also establishes a new Computer System Security and Privacy Advisory Board to "identify emerging managerial, technical, administrative and physical safeguard issues", and report its findings to various sectors and levels of the federal government.

The potential impact of the Act is significant since the US government represents the largest user of computers in the World. However, to date, it has failed to significantly improve the data security practices of government agencies. Around 29,000 security plans were submitted to the NIST; however, staff shortages has meant that it has only been possible to review 450. Many of those reviewed have been found to inadequately deal with issues, such as data integrity and network security. Indeed, a recent report issued by the General Accounting Office has stated that most government agencies still face a potential catastrophe through failures to implement the Act[106].

Recently, proposals have been put forward in the UK suggesting legislation to force computer users to make adequate computer disaster recovery arrangements and maintain their systems to a pre-defined high standard. The arrangements for disaster recovery would apply to specific areas of an organisation's computer system deemed as being of strategic importance to the business, such as a cash management system[107]. Rules would also be laid down concerning the maintenance and support of the system.

In 1990, the European Commission issued a proposal for action in the field of information security[108]. Within the proposal, various options have been put forward for future action, including the implementation of administrative and regulatory measures.

---

[105] Tomkins.

[106] Foremski, T., "Lax case of security standards", p.10, Computing, 16 August, 1991. See generally Baum, Michael S., and Henry H. Perritt, JR., *Electronic Contracting, Publishing and EDI Law*, Wiley Law Publications, New York, 1991, at § 4.19-4.20.

[107] See Applied Computer and Communications Law, p.2, Vol.7, No.2, February 1990.

[108] Proposal for a Council Resolution in the Field of Information Security, OJ C 277/18 of Nov.5, 1990. See also Chapter 2, at 2.3.4.

Significant objections to these legislative proposals exist among manufacturers and users, who would prefer industry standards to be developed, rather than the possibility of restrictive legislation[109]. A second obstacle to such legislation is being able to provide a legislative definition of `adequate' security arrangements, that is not too expensive to implement, particularly for small and medium sized enterprises; or so lax that the rules are ignored.

3.4.3 Computer Misuse

In a comprehensive study on computer-related crime carried out under the auspices of the US Department of Justice, this area was given the following definition:

> "Computer-related crime is the same in name as other familiar types of crime, including fraud, larceny, embezzlement, theft, sabotage, espionage, vandalism, burglary, extortion, and conspiracy. However, relative to the occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales and geography, many computer-related crimes differ significantly from traditional crime. The nature of business, economic, and white collar crimes is changing rapidly as computers pervade the activities and environments in which these crimes occur. Computers are therefore engendering a new kind of crime in which they play four roles as objects, subjects, instruments, and symbols of deception."[110]

As the quote notes, computer crime can be defined to cover a wide range of activities. This section, however, is concerned with recent legislation which has been drafted to address the novel issues arising out of computer crime.

3.4.3.1 Traditional Criminal Sanctions[111]

The following is a brief overview of some major criminal offences and the areas of inadequacy in traditional statute law that have given rise to the need for either modifications to existing law, or

---

[109] However, see Warman, Dr A., "Organisational Computer Security Policies", L.S.E, London, 1991, which reports that 41% of respondents thought that legislation was appropriate to data security; but, the majority felt that existing legislation was not comprehensive enough.

[110] SRI International.

[111] See generally, Arkin, S.S., (ed.), *Prevention and Prosecution of Computer and High Technology Crime*, Matthew Bender, 1990; Sieber, U., *The International Handbook on Computer Crime*, John Wiley & Sons, 1986; Tapper, C., *Computer Law* (4th edition), Longman 1989; and Wasik, M., *Crime and the Computer*, Clarendon/Oxford 1991.

the drafting of `sui generis' legislation.

Fraud

Fraudulent activity is not substantially altered by the use of data communications[112]; although a person's ability to cover his tracks may be enhanced. Computers may be involved in any aspect of the fraudulent process: eg. alteration of the input of certain information; alteration of the operation of the computer through manipulation of certain programs, and/or the output could be varied by computer. The computer is simply a modern tool by which the actions have been carried out.

In the majority of cases involving computer-related fraud, existing legislation is a perfectly adequate instrument under which to prosecute. However, as with other areas of legislation[113], in certain cases the terminology used in the drafting of fraud legislation can give rise to problems of definition, not anticipated before computers appeared. In certain national jurisdictions, for example, for a fraud to be deemed to have occurred, it is a necessary requirement to prove that a `person has been deceived'[114].

Under English law, section 15 of the Theft Act 1968 states:

> "(1) A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it,....
>
> (4) For purposes of this section "deception" means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person."

Case law has further defined `deception' to mean "to induce a man to believe a thing which is false, and which the person practising the deceit knows or believes to be false"[115]. Where innocent persons have been involved at some moment in the fraud, such as the processing of

---

[112] However, see Cook, W., "Paying the bill for hostile technology: PBX Fraud in 1991", pp.174-177, Computer Law and Security Report, Vol.7, No.4, 1991; which discusses a new form of fraud being committed against the telecom network itself.

[113] See Chapter 5, at 5.1.2.

[114] Eg. Denmark, Austria, Greece, Italy, Switzerland. See Sieber, U., "The Comprehension of Computer Crime by Substantive Law", p10, in *The Legal Aspects of Computer Crime and Security*, document prepared for the European Commission's Legal Advisory Board, December 1987.

[115] in the words of Buckley J in *Re London and Globe Finance Corpn Ltd* [1903] 1 Ch 728 at 732.

computer output, there does not appear to be any problem with prosecuting under Section 15[116]. However, where the process is completely automated, the courts have suggested that an offence can not be deemed to have taken place[117]. This could cause particular legal insecurity in an data communications environment, where electronic invoices, purchase orders etc. are generated automatically by the user's computer system, upon receipt of a particular, triggering, electronic message.

Theft

> "information as such is not the subject of the legal norm, but something else - a physical object like a book or a document, which is closely associated with the information"[118]

The general presumption in international law has been that information cannot be owned. This presumption is based on the principle of the `free access to information', as enshrined in Article 19 of the UN Universal Bill of Human Rights and subsequent international treaties[119]. Case law and statute challenging this presumption is scarce. The major exception to the principle are `intellectual property' rights, covering patent, copyright, trade secrets and confidentiality law[120].

As quoted above, the law generally provides rights over a particular physical object rather than the information contained within; therefore information can only be protected under traditional theft statutes where the physical object is stolen. However, the major problem with computer technology is the ease with which data can be copied onto a different medium or, indeed, removed via remote access across a data communications network. Such actions do not fall easily within `theft' legislation since, firstly, it is difficult to establish what exactly has been lost by the victim, since there is no loss of possession, just exclusivity; secondly, most statutes define `theft' in terms of property (ie. something tangible), and to extend theft to include intangibles could over-extend the rule of law.

In English law, the principle that information is not `tangible property' was decisively upheld in

---

116 Eg. *R v Thompson* [1984] 3 All ER 565.

117 Eg. *R v Moritz*, unreported 17-19 June 1981, Acton Crown Court; quoted in Wasik, M., *Crime and the Computer*, Clarendon/Oxford 1991.

118 Bing, Jon, "Information Law?", p219, Media Law & Practice, Vol.2, No.3, 1981.

119 See Section 3.1, above.

120 See Section 3.4.4, below.

Oxford v Moss[121], when an undergraduate was acquitted of theft after obtaining an examination paper, copying it and returning the paper. It was held that, under the Theft Act 1968, information could not be classified as property, and therefore could not be stolen. The Court also recognised that the University had not been permanently deprived of their property. This position was reaffirmed in *R. v Absolom*[122], when a geologist was found not guilty of the theft of information relating to a company's oil exploration, which he had tried to sell to a rival company[123]. In certain European civil law jurisdictions, however, `information' has been seen as an object, in particular circumstances, capable of being stolen[124].

An alternative offence which could be brought against a person accessing a computer and removing data, would be for theft of electricity:

> "A person who dishonestly uses without due authority, or dishonestly causes to be wasted or diverted, any electricity..."[125]

Although any sanctions would obviously bear no relation to the value of the information.

The unauthorised use of computer facilities, the so-called `theft of services', is not classified as a criminal offence in most jurisdictions[126]. Such an offence usually involves employees running their own business on the company system. It is often, therefore, a disciplinary term within the employment contract.

Interception of Communications/Eavesdropping

Criminal measures have been enacted against the interception of communications, both voice and data; as well as electronic `eavesdropping'. In the UK, the Interception of Communications

---

121 [1979] 68 Cr App. R 183.

122 Times, 14 Sept.1983. See also *The Attorney-General v Guardian Newspapers Limited & Others* [1987] 1 W.L.R. pp.1248, 1264; where Sir Nicolas Browne-Wilkinson V.C. stated: "Information as such is not property in any sense, it is available to the whole world...".

123 Similar decisions can be found in common law jurisdictions, such as the US (eg. Ward v Superior Court, 3 C.L.S.R. 206 (Cal., 1972) and Canada (eg. R v Stewart (1983) 5 CCC (3d) 481 (CA); rvsd (1988) 1 SCR 963 (SC)).

124 Eg. France: Crim. 8-1-1979, D 1979, IR 182, on Art. 379 CP; The Netherlands: Hof van Beroep Arnhem, Oct.27 1983, NJ 1984, 80; Belgium: Hof van Beroep Brussels, Dec.5, 1986, Computerrecht 1987, pp.36-40. Quoted in Kaspersen, H.W.K., "Standards for Computer Crime Legislation: A Comparative Analysis" in Vandenberghe, Prof. G.P.V., (ed.), *Advanced Topics of Law and Information Technology*, No.3 Computer/Law Series, Kluwer/The Netherlands 1989.

125 Section 13, Theft Act 1968.

126 The Canadian Criminal Code s.301.2 was passed to cover `theft of services' scenarios, as well as certain US States, eg. Virginia.

Act 1985 makes it illegal to intercept any transmission on a public telecommunications system without approval from the Secretary of State at the Home Office[127]; while the Telecommunications Act 1984 makes it an offence to intentionally modify or interfere with the contents of a messages sent by means of a public telecommunications system, where it occurs otherwise than in the course of that person's duty[128]. In the US, similar provisions are provided for under the Electronic Communications Privacy Act 1986[129]. However, such legislation does not usually extend protection to private data communications networks.

A new security threat that has recently come to light is the monitoring of electrical signals and emissions from VDU screens, which are then reconstituted for viewing on external equipment: `electronic eavesdropping'. Under UK law, it is possible that such activities could fall under the terms of the Wireless Telegraphy Act 1949, which makes it an offence "...the receiving...of electro-magnetic energy....which....(b) is used...for the gaining of information..." without a licence. However, the legislation was not intended to cover such an activity and therefore the courts might not be willing to accept such an extension[130].

In many legal jurisdictions, traditional wire-tapping statutes only refer to the interception of oral communications, and do not necessarily provide effective protection for private communication networks[131].

Forgery

Under the UK Forgery and Counterfeiting Act 1981, Section 1 states:

> "A person is guilty of forgery if he makes a false instrument with the intention that he or another shall use it to induce somebody to accept it as genuine..."[132]

The leading English case involving computers was *R v Gold*[133]. In this case, the defendants

---

127 IC 1985, s.1(2). See *R v Effick*, CA March 19, 1992 (Independent, 31.03.92); reported in New Law Journal, April 10, 1992.

128 TA 1984, s.44.

129 18 U.S.C. 2510-21. See also US federal wire and mail fraud statutes, 18 U.S.C. 1343, 1344.

130 See Dumbill, E.A., "Other criminal offences", p.36-48, Proceedings of `Data Security and the Law' Conference, London, 5 July, 1991 and Lewis, O., "Information Security & Electronic Eavesdropping - a perspective", pp.165-168, Computer Law and Security Report, Vol.7, No.4, 1991.

131 See Sieber, op.cit. supra n.114, at p.21.

132 Under s.8(d), an `instrument' is defined as "any disc, tape, sound-track or other device on or in which information is recorded or stored by mechanical, electronic or other means".

133 [1987] 3 WLR 803. For a detailed discussion of this case, see Wasik, op.cit. supra n.117, at p.70-74.

gained unauthorised access to BT's Prestel service; and then discovered the password codes of various private mailboxes. The defendants were prosecuted under the Forgery Act, for creating a `false instrument' by entering the customer's authorisation code to enter the system.

However, the Court of Appeal decided that the electronic signals, that composed the identification code, could not be considered `tangible', in the sense that a disc or tape were; and that they were held in the system for such a fleeting moment, that they could not be considered to have been `recorded or stored'.

It is also interesting to note, that the courts were critical of the application of the Act to such a set of circumstances:

> "The...attempt to force these facts into the language of an Act not designed to fit them produced difficulties...which we would not wish to see repeated."[134]

Such explicit recognition by the court system of the need to draft new legislation, as opposed to trying to bend traditional interpretations to fit computer technology, lent significant pressure to the calls for reform of the criminal law.

3.4.3.2 **Computer Misuse Legislation**

As illustrated in the review above, the problems of applying traditional criminal law to the use of computers are three-fold:

- The legislation uses terminology that can not be comfortably stretched to cover computer/communications technology (eg. `deception')[135];
- the nature of data makes it difficult to extend legal protection without interfering with other rights (eg. free access), and
- novel threats and activities are possible, which are unique to computers (eg. hacking and viruses), and therefore requires new legislative provisions.

---

[134] [1988] AC 1063, at p.1069.

[135] See also Chapter 5, at 5.2.

This section reviews the introduction of computer misuse-specific legislation, designed to fill the identified gaps in legal protection.

3.4.3.3.1 Unauthorised Access

Perhaps the most well-known issue in the area of computer misuse concerns unauthorised access: `hacking'. Unauthorised access, in data security terms, is linked to the need to ensure the integrity and confidentiality of information. Access can occur either through direct access to the computer system (ie. by employees gaining access to unauthorised applications) or through a remote terminal.

In a legal action against `hacking', the burden of proof is generally upon the prosecution to show that the access is unauthorised. This is obviously much more difficult in the case of internal employees. Companies, therefore, need to establish clear lines of authority for every employee (and keep them regularly audited), or it may prove difficult to prove that an employee knowingly or intentionally exceeded his authority[136].

Some national law has criminalized `mere' access to the computer, while others require that the culprit can be proven to intend damage; or has accessed confidential information; or has modified the data[137]. The OECD Report[138] states that `hacking' requires `intent' on behalf of the perpetrator, or violation of `security measures'. The meaning of `security measures' is identical to that contained within the International Telecommunications Convention of 1973, covering technical and organisational techniques (ie. no reference is made to the quality of the techniques used!).

3.4.3.3.2 International efforts

Computer crime has an obvious international dimension. It has been seen as necessary, therefore, to ensure that legal protection is harmonised internationally. Over recent years, attempts have been made through international organisations to achieve a harmonised approach

---

[136] See Chapter, 2, at 2.3.3, regarding the need for `access audits'. The London Metropolitan Police Computer Crime Unit suggest the use of a front end `banner' message to warn users against unauthorised access; see Applied Computer and Communications Law, p.6, Vol.8, No.5, 1991. One recent survey suggests that 10% of users have adopted this technique; see "IT Security Breaches Summary", NCC (in conjunction with the DTI and ICL), 1992.

[137] See *Germany*, Second Act on Economic Criminality (1986); Par.202a StGB; and *France*, Computer Crime Act of 5 Jan. 1988.

[138] `Computer-related crime: Analysis of legal policy', OECD, Paris 1986.

to legislating against computer crime, and prevent the appearance of `computer crime havens'.

From 1983 to 1985, an ad hoc committee of the OECD discussed the need for international harmonisation of criminal laws with respect to computer-related economic crime. After further joint work with the Working Party on Information, Computers and Communications Policy (ICCP), a final report was published in 1986[139]. The Report lists five categories of offences which it believes should constitute a common approach to computer crime.

The Council of Europe has also considered this field. A select committee of experts, the European Committee on Crime Problems, was established in December 1985 to consider the legal issues raised by computer crime. The final report was published in September 1989[140]. As part of the Committee's work, it produced guidelines for national legislatures on a `Minimum List of Offences Necessary for a Uniform Criminal Policy'. The list was made up of the eight following offences: Computer fraud; computer forgery; damage to computer data or computer programmes; computer sabotage; unauthorised access; unauthorised interception; unauthorised reproduction of a computer programme; unauthorised reproduction of a topography.

These eight offences were seen by all Member States to be the critical areas of computer misuse that required provisions in criminal law. In addition, the Report put forward an `optional list' of four offences that failed to achieve consensus among Members, but were thought to be worthy of consideration: alteration of computer data or computer programmes; computer espionage; unauthorised use of a computer and unauthorised use of a protected computer programme.

The importance and success of the Report was emphasised by the Council of Ministers (the ruling body of the COE), when on 13 September 1989, Recommendation No.R(89)9 was adopted, urging governments to take account of the Report when reviewing and initiating legislation in this field

3.4.3.3.3 The UK Computer Misuse Act 1990[141]

---

139 Ibid.

140 `Computer-related crime', Report by the European Committee on Crime Problems, Strasbourg 1990. See also Draft ICC-UK Position Paper on `Cross-border and reciprocity aspects of computer crime'.

141 Halsbury's Statutes Service: Issue 35, 12 Criminal Law, pp.25-41. See generally Wasik, op.cit. supra n.117, at Appendix 4; Dumbill, E.A., "Computer Crime", p.5, Applied Computer and Communications Law, Vol.7, No.4, 1990; Wotherspoon, K., "Computer Misuse Act 1990", p.391, Lloyd's Maritime and Commercial Law Quarterly, 1991, and Jones, M., "The Computer Misuse Act 1990", pp.125-136, in Proceedings of the Data Security and the Law Conference, 8 May 1992.

In the UK, the Computer Misuse Act 1990 became law on 29th August 1990. The direct origins of the Act are found in the Law Commission report on `Computer Misuse'[142], published in October 1989; although the Scottish and English Law Commission's had published previous reports and working papers[143], as well as a Private Members Bill during the previous parliamentary session. In December 1989, Michael Colvin MP introduced a Private Members' Bill, with the tacit support of the government, and closely following the Law Commission's recommendations.

The primary motivation for governmental support was probably a belief that if the UK did not follow the example of many of its European partners, then the UK's position in the European information market could suffer. This is similar to the reason given by the government when it introduced the Data Protection Act (DPA) into Parliament in 1983, when the Under-Secretary of State at the Home Office stated that the DPA will "enable our own data processing industry to participate freely in the European market"[144]. The fear is that if the UK does not have adequate legal protection for both systems and data, then it will restrict the growth of the UK IT industry.

The Act introduces three new categories of offence:

S.1: Unauthorised access to computer material: "..causes a computer to perform any function with intent to secure access to any program or data held in any computer;"

The `Interpretation' section of the Act states that `any function' covers "copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held"[145]. The `intent' component does not need to be directed at any particular computer/program and/or data. This is the basic hacking offence, and is punishable by a fine of up to £2000 or six months in jail.

S.2 Unauthorised access with intent to commit or facilitate commission of further offences

This covers further `serious' offences such as fraud or blackmail; offences for which either the sentence is fixed by law, or where imprisonment may be for a term over five years. The access and the further offence do not have to be carried out at the same time.

---

142 Report No. 186, Cm.819, London: HMSO, 1989.

143 Scottish Law Commission, `Report on Computer Crime', Cm.174, Edinburgh, HMSO, 1987 and Law Commission, Working Paper No.110, `Computer Misuse', London, HMSO, 1988.

144 Statement of Lord Eton: 443 Parl. Deb., HL (5th ser.) 509 (1983).

145 Section 17(2).

S.3 Unauthorised modification of computer material: "..any act which causes an unauthorised modification of the contents of the computer;"[146]

Modifications include actions "to impair the operation of any computer..to prevent or hinder access to any program or data...to impair the operation of any such program or the reliability of any such data". This clause was principally promoted by the recent spate of publicity and fear surrounding the use of computer viruses[147].

The latter two offences are viewed as the more serious, and can therefore be punished by a jail sentence of up to five years, and an unlimited fine.

During passage of the Bill attempts were made to add a provision whereby hackers would be able to offer a defence if computer users had not implemented security measures. The amendment failed. However, subsequently, Michael Colvin, the Act's proposer, has stated:

> "If companies do not invest in their own computer security strategy, then they cannot expect the sympathy of the courts when people are charged under the provisions"

Obviously, computer crime has an international dimension, and therefore the Act includes provisions to offer extended protection. In basic terms, prosecutions will be possible where either the accused or the target computer was located within the UK at the time of the offence, or if the `further offences' intended by the accused were to be carried out in the UK[148].

The principle of `double criminality' is also introduced into the Act[149]. This means, in regard to the second unauthorised access offence, that a person will not be guilty of committing such an offence unless the `further offence' is an offence under the law of that other country.

The Act gives the police the power to obtain a warrant from a circuit judge if it can be shown that there are "reasonable grounds for believing" that unauthorised access, under Section 1, has, or

---

146 This provision removes the need to take an action under s.1(1) of the Criminal Damage Act 1971, as occurred in Cox v Riley, 83 Cr. App. R. 54, Q.B.D. (1986); see further Tapper, op.cit. supra n.111, at p.295.

147 In the US, a "Computer Virus Eradication Act" has been proposed to cover such instances.

148 CMA, at ss.4-9.

149 Ibid., at s.8(1).

is about to be committed[150]. During its passage through the Commons there were attempts to give wider powers to the police to monitor communications during investigations into suspected hackers. This would have involved alterations to the Interception of Communications Act 1985, which currently requires Home Office approval. The amendment failed to be adopted, despite support from the police, since it would have raised significant civil liberties issues.

This section has focused on the formulation of substantive criminal law provisions to deal with computer crime. However, the effectiveness of such provisions depend primarily on whether an adequate procedural legal framework exists, both nationally and internationally. In order for crime to be prosecuted, sufficient resources must be available for investigations, eg. law enforcement agencies with specific training in the IT field[151].

Another significant issue is how to apply the traditional powers of investigation, search and seizure into a computer environment: for example, what powers should the police have to access network/multi-user systems, since such access might damage the interests of third parties users? Such issues remain currently unresolved[152].

The most significant case, to date, under the new Act, potentially seriously undermined the effectiveness of the Act. In *R v Sean Cropp*[153], the judge accepted the arguments of the defence counsel, who stated that the language of the Section 1 offence, required that the `unauthorised access' had to be from one computer into another. If such an interpretation was to have survived, it would have prevented companies from taking legal action against employees who internally `hack' systems. The case illustrates an additional problem when prosecuting computer crime: a failure by the judiciary to understand the nature of how the technology functions.

3.4.4 Intellectual Property Rights[154]

---

150 Ibid., at s.14.

151 The DTI is currently funding a study by Coopers & Lybrand Deloitte and Cameron Markby Hewitt into whether sufficient expertise and information are available to discover and deal with computer misuse.

152 See generally, Kelman, Alister, "Legal implications of emerging technology and applications", Proceedings of Managing Network Security in the 90's, Conference, London, 13 Sept., 1991; Dumbill, op.cit. supra n.130, at p.46-47, and Tapper, op.cit. supra n.111, at Chapter 10. See *R v McMahon*, Isleworth Crown Court 1987, where the police failed, at the time of arrest, to seize the relevant computer disks; quoted in Sizer, R., S. Chalton, and S.J. Gaskill, "Data Protection", p.16020/2, in *Encyclopedia*, op.cit. supra n.47.

153 Transcript from Crown Court, Snaresbrook, 4 July, 1991; see also Dedman, R., case report in The Computer Law and Security Report, p.168, Vol.7, No.4, 1991 and Collins, S., case report in Computer Law & Practice, p.270, Vol.7, No.6, July-August 1991. The Court of Appeal has since overturned the decision, stating the need to plug this "suprising and unlikely" gap in the legislation (Lord Taylor); The Times, 11 June, 1992.

154 See generally Bainbridge, D.I., *Computers and the Law*, Longman, 1990; Dommering, E.J., and P. Bernt Hugenholtz (eds.), *Protecting Works of Fact*, Kluwer, 1991; Keustermans, J.A. & Ingrid Arckens, *International Computer Law*, Matthew Bender/New York 1988; Millard, Christopher J., *Legal Protection of Computer Programs and Data*, p171, Sweet &

Information, stored in all forms, is more vulnerable to copying rather than straightforward theft. This tendency has been particularly extended by the use of information technology, which makes it easy to produce perfect copies in a very short time and very cheaply. In addition, data communication techniques enable such copies to be distributed extremely widely, very quickly. Intellectual property laws are intended to restrict the use of certain types of information, in the same way that data protection legislation controls the use of personal data.

The particular benefit of intellectual property rights, as a means of legal protection, is based in the fact that unlike contractual restrictions, which can only be enforced against parties to the contract, intellectual property rights are generally applicable against all persons within the jurisdiction of the right[155]. In terms of data security, however, users also need to be aware of the impact the loss of availability of specific information (or product/service) could have in the event that the owner of the right withdrew your right to use that information[156].

This section will be divided in three: the first part will review the scope of copyright legislation; the second part will review the enforcement of copyright in a cross-border communications environment. The third part will consider the area of trade secret law and confidentiality.

3.4.4.1 **Copyright Law**

Copyright law protects the tangible expression of ideas, not the idea itself[157], therefore such legislation usually requires that the copyrightable material be `fixed' in some tangible medium. This is defined under the US Copyright Act of 1976 as:

> "A work is "fixed" in a tangible medium of expression when its embodiment in a copy....., by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."[158]

Maxwell/London 1985; Pearson, H., and Clifford Miller, *Commercial Exploitation of Intellectual Property*, Blackstone Press, 1990; Robertson, R., *Legal Protection of Computer Software*, Longman, 1990, and Bainbridge, D.I., *Intellectual Property*, Pitman Publishing, 1992.

155 Contracts do, however, usually play an important role in the protection of intellectual property rights, since a party's right to use (eg. copy) the relevant information is usually detailed within some contractual document (eg. a software licence).

156 Eg. Where a third party asserts their copyright to prevent one party from supplying the contracted service. This has arisen recently with respect to facilities management contracts, where a software supplier (Computer Associates) has objected to the FM company (Hoskyns) using software licenced to the party intending to use the FM service; see Singleton, S., "Facilities Management - Part 1", pp.6-8, Applied Computer and Communications Law, Vol.9, No.4, April 1992.

157 Patent law protects the `device or process' for carrying out an idea.

158 17 U.S.C. 101

This differs from English copyright legislation[159], by distinguishing where the fixation period is considered to be only transitory. In practice, this could mean that under US law, communication of copyrightable material might not be considered to amount to an infringement[160]. Under English law, the degree of permanence of the copy is irrelevant to the commission of an offence[161]; while:

> "Copyright in work is infringed by a person who without the licence of the copyright owner transmits the work by means of a telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service), knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission..."[162]

Where copyright exists, it confers upon the copyright holder the exclusive right to copy, adapt, distribute and perform the material. The material must be the original expression of the author although, unlike patent law, the right is not exclusive; therefore copyright in a `work' can exist with two different people if it can be proved that each version of the work was developed independently.

Computer software has been recognised as copyrightable in the vast majority of countries, either through express incorporation into statute, or through acceptance by the courts in case law. Computer software has generally been categorised as a form of `literary work'[163].

In the US, there has been a number of cases that have extended the protection that software receives under copyright law from the simple expression of an idea, to the `look and feel' of the whole functioning program. Copyright infringement can, therefore, occur even when the particular expression (ie. programming language) is different, if the overall `structure sequence and organisation' is the same[164]. To date, this trend has not been followed outside of the US[165],

---

159 The Copyright Designs and Patents Act 1988, s.3(2); hereinafter referred to as the CDP 88.

160 Baum, op.cit. supra n.106, at p.431, does not see this as a problem in data communications; see *Secure Servs. Technology, Inc. v Time & Space Processing, Inc.*, 722 F.Supp.1354, 1364 (E.D. Va. 1989).

161 CDP 88, at s.17(6).

162 Ibid., at s.24(2). This is a secondary infringement of copyright.

163 Ibid., at s.3(1)(b).

164 The leading case in this area is *Whelan Associates v Jaslow Dental Laboratory*, 797 F.2d 1222 (3rd Cir., 1986). See Sieber, V., "The development of the law in the United States", p.139-151, Proceedings of `Copyright Protection of Computer Software' Conference, Hungary, 14-18 Oct., 1991.

165 However, in the UK, see *MS Associates Limited v Power* [1988] FSR 242 and *Computer Aided Systems (UK) Ltd v Bolwell*, IPD, April 1990 at 15. See also, the EC Council Directive of May 14, 1991, on the legal protection of computer programs, O.J. 1991 L 91/250, which failed to adopt this approach, and indeed gives software developers significant rights to carry out reverse analysis (Art.5(3)) and `decompilation' (Art.6). See generally, Dumbill, E.A., "EC Directive on computer software protection", p.210-213, Computer Law and Practice, Vol.5, No.5, 1991.

and indeed within the US the scope of such a concept is not yet been clarified.

Unlike patent protection, copyright generally arises with no need for formal acceptance, although notices of authorship on all published works are required in some jurisdictions. In some countries, such as the US Copyright Act 1976[166], registration of copyright is required before an action for infringement can be taken. Where copyrighted data is being sent to such countries, users therefore need to ensure that any necessary procedural requirements have been complied with.

Remedies for copyright infringement tend to be of four main forms:

- an injunction to stop the production of further copies
- a demand that all copies are surrendered to the copyright owner
- damages for losses suffered by copyright owner
- an account of profits made by the infringer

The ability to bring a successful civil action[167] for software copyright infringement requires, among other things, that the plaintiff's ownership of the copyright be established[168]. Practically, this can be extremely difficult; for example there may have been no documentary evidence kept of the authorship of the software, such as draft plans and flow charts.

Data users who are developing bespoke software, need to ensure that adequate documentation is maintained of all the stages involved in the development of the software and that such documentation is appropriately marked with the authors signature and a time/date stamp[169]. Regular intellectual property audits also ensure that adequate evidence can be produced in the event of the need to take legal action against the infringement of the company's copyright. The inclusion of redundant code in software development can be a useful means by which copying

---

166 op.cit. supra n.158.

167 Under UK law, copyright infringement also gives rise to criminal offences: CDP 88, at s.107(1): a person can be guilty of copyright infringement where he, without licence from the copyright holder:

> "(a) makes for sale or hire, or
> (b) imports into the United Kingdom....
> (c) possesses in the course of business...
> (d) in the course of business -
> (i) sell or lets for hire, or
> (ii) offers or exposs for sale or hire, or
> (iii) exhibits in public, or
> (iv) distributes, or
> (e) distributes otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright,
> an article which is, and which he knows or has reason to believe is, an infringing copy of a copyright work".

168 The CDP 88 contains provisions which effectively shift the burden of proof onto a defendent, see s.105(3).

169 See Tapper, op.cit. supra n.111, at p.156.

can be proved, by acting as a form of `signature'.

The creation and use of computerised databases has become a key feature of the international information economy. Such databases are being used in a wide range of contexts; for example, as an international library service (eg. Reuters textline and Butterworth's Lexis); or as a store of specialised technical information within multinational companies, industry groupings or specialised customer/supplier relationships (eg. the CALs initiative of the US Department of Defence[170]). The accessing of such international databases can be a critical aspect of a company's data communication activities, and indeed its commercial operations[171].

Under the Copyright Designs and Patents Act 1988, databases can be classified as either `literary works', in the form of a `table or compilation'[172]; or as a `cable programme service'[173], depending on whether the nature of the service is interactive[174]. The scope of the copyright protection, however, is not always clear[175]. Although copyright will exist in the database as a whole, a separate copyright can also exist in the individual components that make up the database; therefore, an infringement could occur in either or both persons rights. In addition, the copyright monopoly is only given for a certain period of time[176], but databases are usually continuously updated with new information, therefore does the protection period keep changing? Due to the legal uncertainty created by databases, the European Commission has recently published a proposed directive asserting and harmonising copyright protection of databases[177].

In the US, the copyright protection of databases is even more uncertain. A recent US Supreme Court case, *Feist Publications Inc v Rural Telephone Service Company*[178], has ruled that a database would only be able to gain copyright protection if it met the copyright standard of

---

170 See "Report on the potential legal issues arising from the implementation of CALS by the DoD", Prepared by the US Legal Issues Committee of the Acquisition Task Group, CALS/CE Industry Steering Group, 10 November 1991.

171 See for example the Dresser Case, see section 3.5.2, below, where loss of access to a database meant lost business.

172 CDP 88, at s.3(1).

173 CDP 88, at s.7(1): "a service which consists wholly or mainly in sending visuail images, sounds or other information by means of a telecommunications system....for reception - (a) at two or more places (whether for simultaneous reception or at different times in response to requests by different users), or (b) for presentation to members of the public."

174 Interactive services would not fall under the definition of a `cable programme service' [CDP 88, s.7(2)(a)]; however, the scope of this distinction is onclear; see Millard, C., "Copyright", p.84, Chapter 4 of Reed, C., (ed) Computer Law, Blackstone, 1990.

175 See further Tapper, op.cit. supra n.111, at p.50-61.

176 Eg. 50 years from the end of the year in which the author dies [CDP 88, at s.12(1)].

177 "Proposal for a Council Directive on the legal protection of databases", 29 January 1992. See Barrett, B. and Coulter, C., "Proposed Council Directive on the legal protection of databases", pp.34-37, Computer Law and Practice, Vol.8, No.2, 1992; and Singleton, S., "The EC Database Directive", pp.2-4, Applied Computer and Communications Law, Vol.9, No.5, May 1992.

178 See Pearson, H., "A blow to computer data base protection", p6-7, Applied Computer and Communications Law, Vol.8, No.5, 1991.

'originality' in its mode of functioning; copyright protection would not simply be extended to include items which took effort on the part of the owner to compile[179]. This case means that the collection of information in many types of US-based databases can not be protected, except through contractual arrangements.

As discussed in Chapter 2, data communications depend on the use of technical standards, a common language between the parties. In this respect, the ISO and the CCITT have a dominant role in the creation and promotion of international communication standards. Such public standards do not raise significant copyright issues. However, higher level communication protocols, such as EDI messaging standards, tend to have been developed in a more piecemeal fashion. In the UK, for example, although the UN/EDIFACT standard is freely available, many current users are participants in closed sectoral user groups (eg. Odette) that have developed proprietary message formats. Restrictions on the use of such non-public standards, by asserting copyright ownership, could have serious implications for a user who, although a member of a closed user group, wishes to extend the use of such communications to a wider range of its customers and suppliers. Within a European context, such copyright restrictions could be struck down on competition law grounds[180].

3.4.4.2 International regulation

In terms of copyright protection, there are two primary concerns when communicating data:

- Does copyright exist in relation to the data being included in the communication?;
- and will the copyright protection extend to the legal jurisdiction in which the communication is received?

One obvious example of copyrighted material being transmitted over communication links is in connection with the broadcasting of television programmes via satellite and cable links.

International protection of copyright is provided for either through bi-lateral agreements, or international treaty. Such international agreements either provide for a minimum level of rights

---

[179] This differs from the situation in the UK, where the level of originality can be very low, based on the use of some labour and skill [see *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 All E.R. 465, H.L.]. German copyright legislation requires a high level of originality, and therefore does not cover much computer software.

[180] Eg. European Court of First Instance case, *Magill TV Guide v ITP, BBC and RTE*, July 10, 1991, IP/91/668. See also Prins, Corien, "Standardisation of EDI Technology - A Trojan Horse?", pp.138-145, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992. For the US perspective, see Tener, Ralph M., "Copyright Issues relating to the development and maintenance of EDI standards", paper in proceedings of EDI and the Law '91, Conference, Washington, February, 1991.

which each signatory to the agreement guarantees; or contracting state A guarantees that a person from contracting state B will be given national treatment, ie. will be treated as if they were residents of state A.

The two most significant international copyright agreements are the Berne Convention[181] and the Universal Copyright Convention (UCC)[182]. The Berne Convention provides for certain minimum rights for authors; while the UCC requires that "adequate and effective protection" be given to authors from another contracting state[183]. Together these treaties provide for a significant minimum degree of harmonised protection.

Recently, there have been moves within the current round of negotiations under the General Agreement on Tariffs and Trade (GATT)[184] to extend protection for copyright and other intellectual property rights; although distinct differences exist with regard to the perceived scope of protection. In 1988, the European Commission published a Directive on software copyright, which was adopted on 14th May 1991[185], the Directive creates a common standard of protection and rights throughout the Member States of the European Community[186].

Companies making use of international data communications, therefore, need to check certain issues to ensure legal security:

- where the transmission includes the copyrighted information of a third-party, has the appropriate permission been given;
- will the rights be adequately protected in the recipients jurisdiction, and
- when receiving information, does the company have the right to make further use of the copyrighted information, ie. make further copies[187].

---

[181] The Berne Convention for the Protection of Literary and Artistic Works was created on September 9, 1886; the most recent revision was in Paris, 24 July, 1971.

[182] revised in Paris, 24 July, 1971.

[183] UCC, article 1.

[184] See *General Agreement on Tariffs and Trade: Ministerial Declaration on the Uruguay Round of Multilateral Trade Negotiations*, Sept. 20, 1986, 25 I.L.M. 1623, 1627.

[185] Council Directive on the legal protection of computer programs, op.cit. supra n.165. See also Wilkin, R.P., "The EC Directive on the Legal Protection of Computer Programs", p.2-4, Applied Computer and Communications Law, Vol.8, No.3, 1991; Vinje, T.C., "The EC Software Directive and Interoperability", p.175-201, Hungary Conference, op.cit. supra n.164, and Czarnota, B., and R. Hart, *Legal Protection of Computer Programs in Europe*, Butterworths, 1991.

[186] Within Europe, the `CITED project' (Copyright In Transmitted Electronic Documents) has recently been established. Its aim is to protect the "needs of the information industries to safeguard copyright material which is stored and transmitted in digital form, and thus overcome the reluctance of copyright holders to commit their works to a form which is capable of rapid and accurate copying and thus highly susceptible to piracy."; see XIII Magazine, p.5, No.2/92.

[187] See Pool, I & R.J. Solomon, "Intellectual Property and Transborder Data Flows", pp113-139, Stanford Journal of International Law, vol.16, 1980.

3.4.4.3 Trade Secrets Law/Confidentiality[188]

Trade secret law is an extremely widely used form of protection for business information. It is more widely used in the US than in the UK, primarily due to the fact that it tends to be enshrined in statute in the US, which provides for greater certainty. It is often used for the protection of software, and in an employment context. Obviously, in terms of data communications, confidentiality is a critical security requirement, particularly where the communication occurs via a third party network[189].

Trade secret law is often used in preference to other forms of intellectual property right. Unlike patent and copyright, there are no restrictions with regard to the protection of underlying ideas and principles; an extremely wide range of information could be classified as trade secret. Protection is also available immediately, without the need for formal procedures, such as registration. The length of protection is not limited to a certain number of years, it simply depends on the information remaining a `secret'. Another advantage of trade secrets law is that an action can be taken against all forms of misappropriation, including in certain situations, the use of memory alone.[190]

Confidentiality protection primarily arises within contractual relationships, such as with employees and trading partners. In the US, trade secrets law is enacted at the state level[191]. In the UK, a `breach of confidence' is a common law offence based in `equity'. However, in both jurisdictions, an action for breach of confidence requires three conditions to exist:

> "First, the information itself...must have the `necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligations of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it."[192]

As indicated above, the critical first step in any action is for the courts to decide if the information involved can be categorised as a trade secret/confidential. The following factors have been held

---

188 See generally, Poullet, Professor Yves, "The Information Contract - contractual aspects: confidentiality clauses", pp.119-156, in ICC, *International contracts for sale of information services*, ICC/Paris 1988; and Chapter 2, pp. 2097-2116, in *Encyclopedia*, op.cit. supra n.47. See also Lane, David, "EDI: Can Equity cope?", pp.95-98, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

189 See further, Chapter 6, at 6.4.1.

190 Eg. *Faccenda Chicken Ltd v Fowler* (1987) Ch.117.

191 A Uniform Trade Secrets Act was drafted at federal level in 1979, and has been adopted by at least ten states; see "Introduction to Uniform Trade Secrets Act", 14 U.L.A. 541 (1989 Supp.). The Act was amended in 1985.

192 *Coco v Clark* [1969] R.P.C. 41; see also *Lansing Linde Ltd v Kerr* (1991) IRLR 80.

to be relevant:

> "(1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others."[193]

It is clear that secrecy does not have to be absolute, rather it is a question of objective fact: for example, at what point does trade secret information sent to a number of trading partners, via a communications network, enter the public domain?

As can be seen by points (3) and (6) above, the implementation of security procedures, both technical and legal, are likely to be critical considerations in a courts evaluation. Although the courts will consider all forms of misappropriation of trade secrets, an action will only succeed if the plaintiff can show that adequate precautions were taken to protect the secret nature of the information. Such security procedures, as stated by the court in *Amoco Production Co. v Lindley*[194]:

> "often entails establishing that affirmative and elaborate steps were taken to insure that the secret claimed would remain so."

Such `affirmative' steps inevitably extend to the contractual provisions established between all the relevant parties.

In some legal jurisdictions, trade secrets have been classified as `property' and therefore criminal sanctions, such as fines, are applicable in addition to civil sanctions. In the United States, around twenty-seven states have criminal offences expressly covering the use of trade secrets. The US Uniform Trade Secrets Act creates two major offences: unauthorised use or disclosure, and improper acquisition of a trade secret[195]. In Germany, Article 17 of the German Unfair Competition Law of 1909 states that an employee who abuses trade secrets can be fined and placed in jail for up to three years. Such provisions also exist in Article 418 of the French penal

---

193 US Restatement of Torts (1939).

194 609 P.2d 733 at 745 (S.Ct.Okla.,1980). See also Baum, M., "The linkage between security and electronic commerce law", p.86, fn.6, Proceedings of the EDI and the Law Conference, 7 May 1992.

195 See generally Arkin, op.cit. supra n.111, at Chapter 4.

code. The introduction of a tort of unauthorised use or disclosure of a trade secret has been advocated in the UK by the English Law Commission[196].

The major disadvantage in the application of trade secret/confidentiality law is within an cross-border communications environment. Unlike patents and copyright, trade secret protection is not subject to international treaty, extending jurisdiction. As was seen in the *Spycatcher* case, the publication of confidential information abroad can circumvent and render the `right' ineffective domestically[197]. Protection can usually only be enforced internationally where the confidentiality is contractually based[198].

3.4.5 Encryption Regulation

Initially the development and use of cryptographic techniques[199] for communications was restricted to governments and the military. The spread of such techniques to the commercial sector is comparatively recent and, therefore, a number of countries still try to control the use of such techniques[200]. The primary justification behind such restrictions would seem to be for reasons of national security. Such a fear is the stated basis for the regulations issued by the US National Security Agency. The Agency has stated that "unrestrained non-governmental cryptologic activity poses a threat to national security". However, probably more importantly, unrestricted private cryptography would also "hamper the Agency's own international communications monitoring activity"[201]!

The intervention of international telecommunications for reasons of national security is already sanctioned under the International Telecommunications Convention of Malaga Torremolinos. The Convention gives broad rights to intercept, monitor and stop international communications in the name of national security[202]. A state is also permitted under the International

---

196 Report No.110, `Breach of Confidence', Cmnd.8388, 1981. See also Chapter 4, on data protection legislation.

197 [1988] 3 All ER 545. Indeed, in response to the situation that arose, Lord Keith of Kinkel stated that "consideration should be given to the possibility of some international agreement aimed at reducing the risks to collective security involved in the present state of affairs."; at 646.

An additional issue raised by the *Spycatcher* case, centred on the defendent newspapers reference to their right to freedom of expression' as stated in Article 10 of the European Convention on Human Rights (see section 3.1 above). The courts explicitly recognised the need to balance such basic rights against the right to confidentiality: see *Encyclopedia*, op.cit. supra n.47, at p.2113.

198 Eg. in *Business Intelligence Services Inc v Hudson* (580 F Supp 1068 (SDNY 1984)), a US court recognised that the nature of the computer industry may make the contractual imposition of a worldwide restraint-of-trade clause reasonable and enforceable.

199 See Chapter 2, at 2.3.3.

200 See Lindsay, D., "Encryption and Regulatory Controls in Europe", p.28-30, The Computer Law and Security Report, Vol.7, No.1, 1991.

201 Rankin, op.cit. supra n.?, at p.41.

202 ITU Convention, Malaga, Torremolinos, Oct.25, 1973 [TIAS 8572], at Article 19. In the UK, the Protection of Trading

Telecommunications Convention to require the disclosure of cryptographic keys[203], although this is justified primarily on the basis of enabling the national PTTs to ensure compatibility with the public network.

A survey carried out in 1983, found that the encryption of international data transmissions was permitted in only around 37% of the respondent countries[204]. However, out of the multinational respondents to the thesis survey[205], only one stated that they had experienced encryption regulation[206].

Within Europe, France has the most stringent controls. Under a 1939 statute, the national PTT has a duty to regulate the import, manufacture, use and export of any encryption technique. A licence has to be obtained by both the supplier and the user[207].

In the UK, the current stated position of the government is that no statutory encryption regulations exist[208]. However, it the widely held view within the commercial data user community that restrictions do exist, although, primarily in the form of subtle governmental pressure.

3.5 Quasi-Legal restrictions on international data communications

> "Since distance, time of day, and the crossing of national boundaries are no longer issues for today's advanced technology, it is apparent that access to and dissemination, collection and control of information...can become a major national and international policy issue."[209]

International data communications are restricted for a variety of motivations which depend primarily on the nature of the data involved. There are also a number of conflicting policy issues that are relevant, including:

Interests Act 1980, at s.2, enables the Secretary of State to impose restrictions on the transfer of "documents and information required by overseas courts and authorities". The export of military information can be restricted under the Import, Export and Customs Powers (Defence) Act 1939 and various statutory instruments.

203 Ibid., at Article 22.

204 IBI Survey, op.cit. supra n.37, at p.8.

205 Appendix A1/A2.

206 Interview with H G Fielding, Head of Data Processing Security, Barclays Bank, March 1989. Regulations had been experienced in Switzerland, Singapore and South Korea.

207 A new law is currently being debated in the French Parliament, which would restrict the need for a licence to encryption suppliers; see Lindsay, D., "Encryption Regulatory Controls", p.3-6, Applied Computer and Communications Law, Vol.9, No.1, 1992.

208 Letter from D. Locke, Government Communications Headquarters to D. Marsh, Needham & Grant, 14.1.1991.

209 Wigand, Rolf T., "Transborder data flow: its impact on business and government", p57, Information Management Review 1(2), Fall 1985.

- the need for uninterrupted flows of information between countries;
- the need for security safeguards against the misuse of personal or company information;
- the need to recognise the economic value of information and protect trade in it by accepted rules of fair competition;
- the legitimate interest of countries to prevent transfers of information that are dangerous to national security or contravene citizens' rights[210].

Issues of data protection are obviously one of these concerns and are discussed in detail in Chapter 4. Restrictions have also often been imposed by the national telecommunications authorities, as outlined in section 3.3 above. However, this section will review the other motivations upon which countries justify restrictions on the international flow of data.

Consideration of these issues has been divided between regulations that are primarily motivated on economic grounds, and those motivated by socio-political concerns. Such categorisation, in certain cases, is an area of controversy in itself, dependent on the interest group being represented. For example, European data protection legislation has been seen by much of US business as a economic protectionist measure, rather than being motivated by privacy concerns:

> "the EC has taken direct aim at the capture of a large share of the global teleinformatics market while noticing privacy as only a secondary concern."[211].

3.5.1 Economic motivated

Some countries have attempted to regulate data flows because of a concern about their increasing dependence on the activities of multinational corporations that hold sensitive data outside their borders: they see it as undermining national sovereignty, ie. through the erosion of

---

[210] See generally, Gotlieb, A., C. Dalfen and K. Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", pp227-257, The American Journal of International Law, Vol.68, 1974; Fishman, "Introduction to Transborder Data Flows", 16 Stamford Journal of International Law 1, 1980; Bach, Gabriel, "Law and Politics in Transborder Data Flow", p1-24, Law/Technology, 2nd Quarter 1981; Ploman, E.W., "Transborder Data Flows: The International Legal Framework", pp551-562, Computer/Law Journal, Vol.III, 1982; Spero, J.E., "Barriers to International Information Flows: more than a war of words", p67-69, Telecommunications, , Vol.17, No.11, November 1983; Wigand, Rolf T., Carrie Shipley and Dwayne Shipley, "Transborder Data Flow, Informatics, and National Policies", pp.153-175, Journal of Communications, Winter 1984; Robinson, P., "Legal Issues Raised by Transborder Data Flow", 295, 11 Can.-U.S. Law Journal, 1986; Sauvant, K P, *International Transactions in Services: The Politics of Transborder Data Flows*, The Atwater Series on the World Information Economy No 1, Westview Press/London 1986; Millard, C.J., "Transborder Data Flows: The European Perspective", paper presented at the Computer Law Association's Conference on 'Distribution, Access & Communications', Amsterdam, 1-3 June 1988; Hoyle, C., "Transborder Data Flows", paper presented at 'Legal, Contractual, Responsibility and Evidential Issues in EDI, EFT Email and communications by fax or telex', London, 20 February 1992.

[211] See Eger, "The Global Phenomenon of Teleinformatics: An Introduction", pp.216, 14 Cornell International Law Journal, 1981. See also Evans, A.C., "Emerging Restrictions on Transnational Data Flow: Privacy Protection or Non-Tariff Barriers?", p1055-1103, 10 Law & Policy in International Business; Pinegar, Kevin R. "Privacy Protection Acts: Privacy Protection or Economic Protectionism?", p183-88, The International Business Lawyer, April 1984.

a nation's decision-making capacities; as well as leading to potentially massive national economic loss.

In Canada, the Clyne Committee[212] reported that the increasing levels of data flowing from Canada to the US, for processing and storage, was likely to lead to a loss of sovereignty. It also meant an estimated loss in foreign exchange to the US for data services of $300 million; as well as a predicted loss of some 23,000 directly-related jobs. In addition to these dismal economic statistics, as one report has noted:

> "Canada feels some national embarrassment and resentment over increasing quantities of sensitive data about Canadians being stored in a foreign country"[213]

In the international information economy, information that is used within decision-making processes tends to flow from the less developed countries (LDCs) to the richer nations; while, conversely, the information that flows towards the less developed countries is usually that contained within decisions that have already been taken. This has created a fear within LDCs that the information revolution may simply serve to widen the gap between rich and poor nations[214]. Alternatively, however, transborder data flows have also been seen as a crucial part in an LDCs development:

> "bridging the gaps between nations by contributing to a transfer of such data resources as computer hardware, databases and information jobs."[215]

The position of data-processing operations can have considerable economic consequences for nations, since high paying technical jobs are generally concentrated in the state which carries out the processing, while low paying, key punch operations are carried out in the data exporting state. Countries can, and have, become concerned about the impact that TDFs can have on national economic indicators, such as employment and the balance of trade. Such concerns have led to the imposition of requirements that `domestic' information and transactions be processed in the home country[216].

---

[212] Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty: "Telecommunications and Canada" (Ottawa: Minister of Supply and Services, 1979)

[213] Turn Rein (ed), "TDF: Concerns in Privacy Protection and the Free Flow of Information", Report of the AFIPS Panel on TDF, vol.1 (Arlington, VA, 1979).

[214] See Bortnik, Jane, "International information flow: The developing world perspective", p333-353, 14 Cornell International Law Journal, 1981; Ennison Jr., Thomas, "Sovereignty Considerations in TDF - developing country perspective", p175-181, Transnational Data and Communications Report, Vol.VII, No.3, 1984.

[215] UNESCO, E/C.10/1986/16, 1986.

[216] Eg. West German Bundespost regulations, 1 January 1982, require that private leased lines with international access, carry

Brazil is the classic example of a developing state implementing a stringent `informatics' policy in order to encourage the growth of a domestic data processing industry. It has declared its commitment to the following objectives, and has created a maze of regulations accordingly:

> "To maximise the information resources located in Brazil, both imported and locally produced;
> To acquire and maintain national control over the decisions and technologies related to the Brazilian data industries;
> To enable Brazilian society to have universal access to information; and
> To administrate information resources in such a manner that they contribute to the enhancement of Brazil's cultural and political environment."[217]

Overall, it would appear that the degree to which less developed countries wish to regulate TDFs usually depends on the tone of their relationships with multinational corporations[218].

In addition to such existing restrictions, as value-added data processing has become an increasingly valuable sector of the economy, it is inevitable that governments have become interested in the possibility of applying taxes to transborder data flows; both as a means to raise revenue, and to improve their balance of trade. The 1983 IBI survey on national policies for TDFs stated that, although taxation on such intangible products and services does not yet exist, 64% of the respondent nations stated that it was still an open issue[219].

In France, the Customs Authorities have already tried to impose a scheme for the taxation of software, based on its development costs; while in 1982, a French intergovernmental report on `Transborder Data Flows'[220] suggested the development of a scheme by which TDFs could be

---

out `substantial' local processing before transmission; while the 1980 Canadian Bank Act requires all `basic' financial data to be processed and maintained in Canada (s.157(4)). Such actions have also been justified on the grounds of protecting national sovereignty.

217 Brizida, "Transborder Data Flows in Brazil" (1982) 13 CTC Reporter (UN Centre on Transnational Corporations). See also Brown, R.W., "Economic and Trade Related Aspects of Transborder Data Flow: Elements of a Code for Transnational Commerce", p.22, Northwestern Journal of International Law and Business, Spring 1984, Vol.6, No.1.

218 Groshan, R.M., "Transnational Data Flows: Is the idea of an international legal regime relevant in establishing multilateral controls and legal norms?", Part I: p6, Law/Technology (4th Quarter 1981)

219 op.cit. supra n.37, at p.8. See also USTR Ambassador, William E Brock, "Global Competition: What impact on US industry?", 52 Antitrust Law Journal, 147 (1983) at 153: "We're beginning to hear now of governments which are seriously discussing taxing the exchange of information..". See generally, Williams, D.W, (ed.) *Tax on the International Transfer of Information*, Longman, 1991; and Kelley, P.L., "The impact of customs and taxation on data flows in the EEC", pp.115-126, in Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

220 known as the Madec Report, after its chairman. The classification system distinguished data flows into four categories: (a) legal: public or confidential; (b) commercial: capable of being sold (c) functional: information carriers as distributors, a conduit for two-way communication, central nervous system; (d) economic: contribution to the creation of a final product, value-added.

accurately measured, to enable the possibility for future taxation. Such ideas have yet to be put into practice by governments, yet the prospect remains significant.

3.5.2 Non-economic motivated

> "Information is power and economic information is economic power....This in turn leads to a loss of national sovereignty through international flows"[221]

> "The concern over national computer vulnerability mirrors the concern over the need for greater privacy protection for the individual"[222]

Countries may conclude that excessive use and reliance on TDFs creates economic, and indeed political, vulnerability. Regulations may therefore be introduced to ensure that a `critical mass' of national data is not held outside the state. Without such action, the fear is that access to essential national/economic information, processed within another state, may be withheld during a period of political confrontation. A survey carried out in 1983, stated that the highest percentage of policies restricting the export of data were related to national security concerns[223].

During the dispute over the Siberian gas pipeline, President Reagan ordered a halt to technical communication between the Dallas-based Dresser Industries and its French subsidiary, a compressor manufacturer for the project. This action resulted in the loss of a $3.5 million order from an Australian company, since the French company no longer had access to the technical database of the parent company[224].

The alternative explanation for this fear is that nationally sensitive information may be removed from the country without permission.

3.4.3 Comment

During the late 1970s and early 80s, there has been a significant amount of concern voiced by

---

[221] Louis Joinet, Secretary-General of the French Commission on Data Processing and Liberties; quoted in Pipe, Russel G., "National Policies, International Debates", p118, Journal of Communication, vol.29, Summer 1979.

[222] Eger, "Transborder Data Flow", p.50, 24 Datamation, Nov.15, 1978.

[223] IBI World Survey of National Policies and Company Practices Concerning Transborder Data Flows, p5, TDF 110, November 1983.

[224] See also the SARK Report (Swedish Ministry of Defence: "The Vulnerability of the Computerised Society", Stockholm, March 1980), which concluded that the vulnerability of Swedish society was "unacceptably high".

companies, particularly multinationals, over a perceived trend towards governmental regulation of data flows[225]. The reality of these fears seems difficult to accurately assess, since only a few, oft- repeated, examples appear in the literature on this topic.

It would appear, however, that as developments in telematics gave greater prominence to the commercial potential of international data communications, governmental bodies did turn their attention to the issues involved. This in turn inevitably led to expressions of concern regarding the extent to which such technological developments could impact on a national economy; and therefore, various control mechanisms were promoted[226].

> "It is almost impossible to control an entire nation's inflow and outflow of data and information transmitted via conventional telephone lines and to identify which data and information are subject to control, duty and taxes"[227]

However, as the above quote illustrates, as the technology has progressed further, governments have also recognised the technical difficulties involved in any significant regulatory initiatives, and would therefore seem, at the present time, to have decided against such action.

---

[225] See Bushkin, Arthur A., "The threat to International Data Flows" Business Week (3 August 1981); Hickmott, G.T., "Data Restrictions: Users' Concerns", p25-27, Transnational Data and Communications Report, Vol. IX, No.12, 1986; Greguras, Fred M, and Richard Sizer., "Impact of transborder data flow restrictions on cash-management services", pp17-22, Information Age, Vol.9, No.1, January 1 1987; Kane, M.J. and D.A. Ricks, "The Impact of Transborder Data Flow Regulation on Large United States-Based Corporations", p23-29, The Columbia Journal of World Business, Vol.XXiV, No.2, 1989, and Herman and Halvey, *International Flow of Data is threatened*, American Banker, Sept. 25, 1990.

[226] Eg. a model code for transnational commerce in the area of transborder data flow; Brown, op.cit. supra n.217.

[227] Wigand, op.cit. supra n.209, at p.63.

Chapter 4 **DATA PROTECTION**

4.1 Definitions

Data protection legislation has currently been enacted in seventeen West European countries[1], as well as other industrialised nations, such as Japan[2] and Canada[3]. Nearly all other West European countries have put forward proposals, at various stages, towards legislation[4]; while of the seventeen countries with legislation, a number have already revised or amended their original legislation.

---

[1] Austria, Denmark, Finland, France, Germany, Guernsey, Iceland, Ireland, Isle of Man, Israel, Jersey, Luxembourg, The Netherlands, Norway, Portugal, Sweden and the UK.

[2] 'A Bill to Protect Computer Processed Personal Data held in Administrative Organs' was enacted on 16 Decemeber 1988, and came into force on 1 October, 1989. It covers computer data held in government departments.

[3] Eg. The Privacy Act 1982, [S.C., 1980-81-82-83, c.111], passed on 7 July, 1982. It covers federal government and agencies. The provinces of Québec and Ontario have their own legislation.

[4] Belgium, Greece, Hungary, Italy, Spain and Switzerland all currently have data protection bills. Hungary, now a Member State of the Council of Europe, is the first Eastern European country to try and pass a data protection bill.

However, such widespread implementation of data protection legislation does not necessarily indicate a common perception of the scope of such legislation. Indeed, the definition of `data protection' can vary considerably between each legal jurisdiction.

One of the most straightforward definitions of data protection is given in the British Government's explanatory report, appended to the draft of the Council of Europe Convention on Data Protection:

> "...the legal protection of individuals with regard to automatic processing of personal information relating to them."[5]

However, an expanded definition of data protection has been put forward by a number of Less Developed Countries. They have promoted the concept of data protection as a legal regime that should also be applied to information pertaining to states, as well as individuals. Resolutions at Latin American and African conferences proposed that "information and knowledge affecting national sovereignty, security, economic well being and socio-cultural interests should be brought within the ambit of data protection."[6]

Indeed, our initial definition is not even sufficient to cover the variations of data protection legislation between industrialised nations, or even within Western Europe. Some countries, such as Denmark and Austria, extend protection to legal persons, such as companies and trade unions. Other countries, including France and the Netherlands, have legislation that extends to manual records, as well as computer data. Protection is limited primarily to public sector data processing in countries such as the United States[7] and New Zealand[8].

It is also necessary to distinguish data protection from the related, but distinct, areas of `privacy' and `data security'. A simple distinction between data protection and `privacy' is made in the Lindop Report[9], when it gives an example that the use of inaccurate or incomplete information when decision-making, although within the proper scope of data protection, is not necessarily a

---

[5] Explanatory Report, p5, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981 (Cmnd 8341); hereinafter referred to as the Convention.

[6] quoted in Intergovernmental Bureau for Informatics, TDF 270, p55.

[7] US Privacy Act 1974 (5 U.S.C., s.552a). Certain sectoral legislation exists covering the private sector, eg. Fair Credit Reporting Act 1970 and Electronic Funds Transfer Act 1978. See generally, Reidenberg, Professor J.R., "United States Data Protection in the Private Sector: Between a Fortress for Individual Rights and the Wild West", Proceedings of Privacy Laws & Business, 4th Annual Conference, Cambridge, 2-4 July, 1991.

[8] Official Information Act 1983. The government tabled `The Privacy of Information Bill', which would cover the private sector, on the 10 August, 1991.

[9] Report of the Committee on Data Protection, (Chairman: Sir Norman Lindop) Cmnd 7341 (1978), para 2.03.

privacy issue. Data security is more closely linked with data protection, being a part of the requirements of adequate data protection, but it also covers issues of computer crime, as well as ensuring that company computer systems are protected from physical disasters.

Data protection legislation is generally concerned that individuals, upon whom data is held, are able to discover the existence of the information, as well as the motives behind such possession. In addition, the focus is less on the type of data held, than with the conditions under which it is held.

An alternative, less legalistic, definition of data protection legislation has been suggested by the UK Office of the Data Protection Registrar. At a conference, the Deputy Registrar defined data protection as `fairness legislation', not requiring a balance between data users and data subjects, but simply being fair to an individual.[10]

Within Western Europe, the 1981 Council of Europe Convention on data protection forms the basis of all national data protection legislation. Behind the Convention, two distinct motives exist: the threat for individual privacy posed by data processing and other new technologies; as well as maintaining a free flow of information in an international market. The Council of Europe Convention on data protection was initially seen as an extension of Article 8 of the European Human Rights Convention, concerning an individual's right to privacy. However, the explanatory memorandum to the Convention also states that it is necessary to reconcile this with the principle of free flow of information, which is enshrined in Article 10 of the Human Rights Convention[11].

Indeed, in the course of the Parliamentary debates on the United Kingdom Data Protection Act 1984, the Under-Secretary of State at the Home Office, clearly put forward these two objectives:

> "[T]he Bill is drafted to fulfil two purposes. The first is to protect private individuals from the threat of the use of erroneous information about them - or indeed, the misuse of correct information about them - held on computers. The second is to provide that protection in a form that will enable us to satisfy the Council of Europe Convention on Data Processing so as to enable our own data processing industry to participate freely in the European market."[12]

---

[10] CBI Conference, London, 4th March 1988.

[11] Convention, op.cit. supra n.5, at p.10-11.

[12] 443 Parl.Deb.,H.L. (5th ser.) 509 (1983) (statement of Lord Eton); see also Hansard, Vol.53, (January 1, 1984), p.31.

The UK Data Protection Registrar echoes this statement in his `Third Annual Report', when he states that data protection legislation is based "in concerns for both privacy of the individual and the need for efficient international trade"[13]. However, he goes on to stress the prominence of the former, and the bonus nature of the latter!

4.2 The scope of data protection legislation[14]

> "There no longer exists the freedom to refuse public information concerning personal data, but rather the freedom resides in the ability to control the use made of personal data inserted in a computer program..... Therefore, the right of access to data banks, the right to check their exactness, the right to bring them up-to- date and to correct them, the right to the secrecy of sensitive data, the right to authorize their dissemination: all these rights together today constitute the new right to privacy."[15]

Since the Warren and Brandeis definition of privacy as the `right to be let alone'[16], a great amount of time has been devoted to defining an exhaustive list of the constituent components of the term `privacy', a problem we have considered above with respect to data protection. For example, the United Nations Declaration of Human Rights, Article 12, states that every individual has a right to privacy, yet fails to define the term. However, what does seem to be agreed upon is the extent to which the meaning of `privacy' is dependant on a nations culture.

The classic contrast to the British attitude to privacy is Sweden. On the one hand, Sweden has had a freedom of information Act since 1776, but they also have a social system based on the existence of a mandatory, unique personal identifier for each citizen, something which would not be acceptable in this country at the present time. While in France, since Napoleonic times each citizen is legally required to deposit his or her personal file with the local police station on moving residence, in the UK this would be seen as a great infringement of privacy[17].

---

[13] The Third Report of the Data Protection Registrar, p.2, June 1987, HMSO.

[14] This Chapter will not consider the impact of data protection legislation on developments in telecommunications services, ie. voice telephony; see further Bradgate, R., "Privacy and Telecommunications", p.5-7, Applied Computer and Communications Law, Vol.8, No.7, 1991.

[15] Frosini V., 'The European Convention on data protection', Computer Law and Practice, January/February 1987, pp84-90.

[16] "The Right to Privacy", 4 Harvard Law Review, 193, 1890.

[17] See Sizer, R., S. Chalton, and S.J. Gaskill, "Data Protection", p.16006, in Saxby, S., (General Editor) *The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990.

However, what is the difference between the principles upon which data protection legislation is based and justified, and those that lie behind the `right to privacy'? The 1978 Lindop Report on Data Protection acknowledged the following distinction:

> "a data protection law should be different from that of a law on privacy: rather than establishing rights, it should provide a framework for finding a balance between the interests of the individual, the data user and the community at large."[18]

Such a balancing act can be easily recognised in the two motives behind the Council of Europe Convention. Also, as mentioned earlier, data protection legislation generally recognises that data users can have a legitimate purpose for holding certain data, irrelevant of the subjects wishes[19].

Despite this stated difference between the concept of data protection and that of privacy, developing data protection case law can extend the scope of the legislation to wider questions regarding an individual's `right to privacy'. In Germany, a Constitutional Court decision declared unconstitutional an act which had authorised the Government to undertake a comprehensive population census. The Court declared that each data subject has a right to "determine in general the release and use of his or her personal data"[20]; therefore recognising a right of individual self-determination (Recht auf informationelle Selbstbestimmung) and raising data protection to a constitutional level. The decision also led to a fundamental review of the Federal Data Protection Act.

In the UK, which does not have a constitutional or statutory right to privacy, data protection case law could extend its boundaries through judicial precedent, or through the decisions of the Data Protection Registrar, to the creation of a more thorough `right of privacy'. It has been noted that some judicial opinion within the European Court of Human Rights has begun to use the Council of Europe Convention on data protection to enliven and strengthen Article 8 of the Human Rights Charter.[21]

---

[18] op.cit.supra n.9, pxix. Sizer, ibid., at p.16003, comments that data protection legislation is "essentially a compromise between altruism and pragmatism".

[19] The concept of a balance, between data user and subjects, would seem to complement the use of contracts to secure international data protection equivalency; see further Chapter 6, at 6.2.

[20] Judgement of December 15, 1983, Bundesverfassungsgericht [BVerfG], 65 Entscheidungen des Bundesverfassungsgericht [BVerfGE] 1, at p43; *translated in* 5 Human Rights Law Journal, 94, 1984. See also "New Technologies: a challenge to privacy protection?", Council of Europe, Strasbourg 1989, p.34, which defines `informational self-determination' as "the right of the individual to control the amount of data collected on him, to follow up the use made of the data, to remain at all stages aware of the different operations carried out on his data, etc."

[21] Mr P.Hustinx, `The role of the Council of Europe', Privacy, Laws and Business Conference on Data Protection in Ireland, The Netherlands and Switzerland, 19th Oct. 1988.

A related question which arises in this area concerns the issue of freedom of information. How does the right to `freedom of information' relate to data protection? The Council of Europe has currently got a committee considering the potentially conflicting interests of data protection and `freedom of information'. The Committee is looking into problems concerning access rights, often into public archives, that may lead to an infringement an individual's privacy. This would seem particularly relevant for countries such as Sweden, which have a strong legislative tradition in both spheres, with freedom of information legislation since 1776 and the first data protection law in 1973. Indeed, in the UK, it has been claimed that data protection has been used as an excuse by some government authorities to refuse to disclose legitimate public documents and maintain greater secrecy![22]

However, data protection can also be seen as functioning as a supplement to freedom of information legislation, by increasing the transparency of an authority's decision-making process. For instance, individuals are able to ascertain, through use of their `data protection' access rights, the extent of personal information that public authorities hold, and can therefore be presumed to use in their decision-making processes. Indeed, in Quebec, Canada, 1982 legislation deals with both access to documents held by public bodies and the protection of personal information under the same statute[23].

Within the English legal system, data protection must also be distinguished from an action in civil law for breach of confidence[24]. An overlap exists between the action for breach of confidence and the Data Protection Act 1984 concerning the control of information. However, there are also a number of significant differences between the common law and statutory legal remedies.

Breach of confidence applies to all types of information, regardless of the medium involved, whereas the UK Data Protection Act applies only to information that has been automatically processed. The Act does, nevertheless, cover all categories of information, whereas, an action for breach of confidence can only arise if the information is perceived to be of a confidential nature. The Act is also primarily intended to prevent abuses from arising, while for an action for breach of confidence to succeed, there has to have been either a breach, or an anticipated breach.

---

22 Campbell, Duncan and Steve Connor, *On the Record: Surveillance, Computers and Privacy*, Michael Joseph/London 1986, at p.35.

23 `Access to documents held by public bodies and the Protection of personal information' Act 1982; see also *The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990, Chapter 16, and Flaherty, D.H., *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press 1989.

24 See Chapter 3, at 3.4.4.2.

4.3 International Law

The data processing industry has a very international character. Large amounts of data cross national borders every day, either electronically, via cables or satellites, or through the manual transfer of media, such as magnetic tapes. The former can usually be transferred without significant control or supervision by any form of governmental authority. Such transfers thus pose a threat to individual privacy, since national laws can be circumvented by transferring data to a so-called `data havens', which lack such legislation. The data processing industry therefore has the ability to act with a degree of independence from national legislation.

In order to prevent data users from avoiding data protection controls, and therefore guaranteeing a free flow of information, international governmental organisations have become involved in attempting to obtain harmonisation of data protection legislation. The European Community is currently debating a draft Directive on data protection; while the United Nations Commission on Human Rights has proposed draft guidelines on `computerised personal data files', which have yet to be finalised[25]. To date, the two primary international legal instruments dealing with data protection have originated from the Council of Europe and the O.E.C.D..

This section reviews the data protection activities of the four major international institutions.

4.3.1 The Council of Europe

The Council of Europe has been the major international force in the field of data protection since the 1981 Convention `for the Protection of Individuals with regard to Automatic Processing of Personal Data' was adopted[26]. Currently 19 of the 26 Council of Europe Members have signed the Convention, and have therefore accepted an obligation to incorporate certain data protection principles into national law. The Convention came into force on October 1st 1985 when five countries had ratified it: Sweden, Norway, France, The Federal Republic of Germany and Spain.

---

[25] E/CN.4/1990/72, 20 February, 1990. Such guidelines, to be considered by the UN General Assembly, would provide for minimum standards of protection: see Privacy Laws & Business, p2-3, no.11, September 1989.

[26] The Convention, op.cit. supra n.5. However, even in 1984, one commentator was able to state that the Convention "is likely to be of lesser importance that the [OECD] Guidelines because of its failure to arrive at a consensus that might be supported...by the United States"; see Cooper, David M., "Transborder Data Flow and the Protection of Privacy: The Harmonisation of Data Protection Law", p349, The Fletcher Forum, Vol.8, Prt 2, 1984.

The Council of Europe has been involved in this area since 1968, when the Parliamentary Assembly passed a Recommendation[27] asking the Council of Ministers to look at the Human Rights Convention to see if domestic laws gave adequate protection for personal privacy in the light of modern scientific and technical developments. The Council of Ministers asked the Committee of Experts on Human Rights to study the issue, and they reported that insufficient protection existed.

A specialist Committee of Experts on the Protection of Privacy was, therefore, asked to draft appropriate resolutions for the Committee of Ministers to adopt. Resolution 22 (1973) covered the 'ground rules' for data protection in the private sector; while Resolution 29 (1974) focused on the public sector[28].

However, further initiatives were considered necessary. In 1976, the Committee of Experts on Data Protection was established. Its terms of reference were defined in 1977 as:

-to prepare a Convention on the protection of privacy in relation to data processing abroad and transfrontier data processing;
-to carry out a study on data bank regulations, particularly for medical data banks;
-to examine problems relating to the professional ethics of computer experts.

The text of the Convention was finalised in April 1980, and opened for signature on 28 January 1981[29].

The Convention is based around a number of basic principles of data protection, upon which each country is expected to draft appropriate legislation. Such legislative provision is intended to provide for a minimum degree of harmonisation between signatories and was intended to prevent restrictions on transborder data flows for reasons of `privacy' protection[30].

Since 1981, the Committee of Experts on Data Protection has been primarily involved in the drafting of sectoral rules on data protection. These form part of an on-going series of

---

[27] Recommendation 509 (68), "On Human Rights and Modern Scientific and Technological Developments", Annuaire Européen, 6 (1968), p.363.

[28] "On the Protection of the Privacy of Individuals via-a-vis Electronic Data Banks in the Private Sector", Resolutions 1973, p.73-74; "On the Protection of the Privacy of Individuals via-a-vis Electronic Data Banks in the Public Sector", Resolutions 1973, p.87-89.

[29] op.cit. supra n.5.

[30] Ibid., Article 12(2).

recommendations issued by the Committee of Ministers designed to supplement the provisions of the Convention[31]. There are currently Council of Europe working parties looking into the particular sectoral issues raised within the telecommunications[32] and media sectors; and the data protection issues created by the use of Personal Identification Numbers and genetic data.

The major weakness of the Council of Europe Convention is its lack of enforceability against countries that fail to uphold the basic principles. No enforcement machinery was created under the Convention and therefore any disputes would have to be resolved at the diplomatic level.

One particular issue concerns the nature of `equivalent' data protection legislation. Under Article 12(3a) of the Convention, a member can prevent the transfer of data to another member where:

> "a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
> b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party..."[33]

The first point is intended to cover situations where one Contracting State's legislation provides additional protection to certain types of data, such as legal persons or classifies different data as sensitive[34]. However, does `equivalent' mean identical or similar, and who decides in the event of a dispute? Such uncertainty, creates legal insecurity for companies wishing to establish international data communications.

4.3.2 The Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development was established in 1961, and currently comprises 24 of the leading industrial nations. The nature of the organisation has

---

[31] Recommendations have already been produced to cover the areas of personal data in `medical data banks'(81); `scientific research and statistics' (R(83) 10); `direct marketing'(R(85) 20); `social security records' (R(86) 1); `the police sector' (R(87) 15); `employment records' (R(89) 2); `used for payment and other related operations' (R(90) 19) and `the communication to third parties of personal data held by public bodies' (R(91) 10).

[32] `Draft recommendation on the protection of personal data in the area of telecommunications services, with particular reference to telephone services', final activity report of Working Party No.9, February 1991 (CJ-PD (91) 2). Currently, this recommendation covers `voice, text, image and data transmission' by both public and private service providers.

[33] Ibid., Article 12(3).

[34] See Sections 4.4.2 and 4.4.3.

meant that interest in data protection has centred primarily on the promotion of trade and economic advancement of member states, rather than `privacy' concerns.

In 1963, a Computer Utilisation Group was set up by the 3rd Ministerial Meeting. Aspects of the Group's work concerned with privacy went to a subgroup, the Data Bank Panel. This body issued a set of principles in 1977. In the same year, the Working Party on Information Computers and Communications Policy (ICCP), was created out of the Computer Utilization and Scientific and Technical policy groups. Within this body, the Data Bank Panel became the `Group of Government Experts on Transborder Data Barriers and the Protection of Privacy'. Its remit was:

> "to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonisation of national legislation, without this precluding at a later date the establishment of an international convention".

The OECD Guidelines were drafted by 1979, adopted September 1980, and endorsed by UK government in 1981.[35]

The Guidelines are simply a recommendation to countries to adopt good data protection practices in order to prevent unnecessary restrictions on transborder data flows, they have no formal authority. However, some companies and trade associations, particularly in the United States, Japan and Canada, have formally supported the Guidelines.

With regard to the issue of transborder data flows, the Guidelines state:

> "A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection."[36]

---

[35] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981) [hereinafter referred to as the `Guidelines']. The Republic of Ireland became the last member country to sign the Guidelines, in January 1987.

[36] Ibid., Paragraph 17.

This is extremely similar to the provisions provided under the Convention.

4.3.3 The United Nations

The United Nations has focused on the human rights aspects of the use of computer technology comparatively recently. In 1989, the General Assembly of the Commission on Human Rights adopted a set of draft "Guidelines for the regulation of computerized personal data files"[37].

These draft guidelines were subsequently referred to the Commission on Human Rights Special Rapporteur, Mr Louis Joinet for re-drafting, based on the comments and suggestions received from the member governments and other interested international organisations. A revised version of the `Guidelines' were presented in February 1990[38]. Since then, however, no significant further action has taken place.

The Guidelines are divided into two sections. The first section covers Principles concerning the minimum guarantees that should be provided in national legislations, and are based upon those principles discussed in Section 4.3.5. below. However, three additional terms have been put forward:

- 5. Principle of non-discrimination - sensitive data, such as racial or ethnic origin, should not be compiled[39];

- 6. Power to make exceptions - only for reasons of national security, public order, public health or morality; and

- 8. Supervision and sanctions - the authority `shall offer guarantees of impartiality, independence via-à-vis persons or agencies responsible for processing...and technical competence'.

The transborder data flow principle, number 9, states that:

---

[37] UN General Assembly, forty-fourth session, Resolution 44/132, on 15 December, 1989.

[38] UN Economic and Social Council, `Human Rights and Scientific and Technological Developments', E/CN.4/1990/72, 20 February 1990.

[39] See also Section 4.4.2. below.

"When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards...information should be able to circulate freely as inside each of the territories concerned..."

This current draft would suggest, therefore, that contractual means of achieving equivalent international data protection would not be acceptable[40].

The second section considers the Application of the guidelines to personal data files kept by governmental international organisations. This requires that international organisations designate a particular supervisory authority to oversee their compliance. In addition, it includes a `humanitarian clause', which states that:

"a derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance"

Such a clause is intended to cover such organisations as Amnesty International, who hold large amounts of personal data, but would be wary of sending information out to a data subject on the basis of an access request made while the person was still imprisoned.

4.3.4 The European Community

4.3.4.1 Background

Despite interest and involvement in data protection and privacy issues for nearly two decades, from both the European Parliament and the Commission, the emergence of a `Directive' (the Community equivalent to United Kingdom Law) concerning this area, only appeared in July 1990. The `Directive', when adopted will oblige member states to undertake appropriate measures to fulfil the objectives of that Directive[41].

The European Parliament's involvement in data protection issues has primarily been through its Legal Affairs Committee, though the issue has been subject to parliamentary questions and debates for the past ten years. In February 1975, Lord Mansfield, the presenter of a report on

[40] See Chapter 6, at 6.2.1.

[41] `Directives' bind member states as to the ends, but not as to the means of implementation; in contrast with `Regulations' from the Commission which bind members in every respect to the letter of the Regulation.

behalf of the Legal Affairs Committee on the protection of individual rights, stated in Parliamentary debate, that this subject was:

> "an exciting opportunity for the European Parliament to broaden its influence and powers...a full-hearted response will go far to widen the influence of the Parliament and at the same time to disarm those critics who complain it is a powerless talking shop."[42]

Parliament adopted a resolution calling for a directive to ensure that "Community citizens enjoy maximum protection against abuses or failures of data processing" as well as "to avoid the development of conflicting legislation."[43]

In 1977 the Legal Affairs Committee established the Sub- Committee on Data Processing and the Rights of the Individual. The Sub-Committee, produced the `Bayerl Report' in May 1979.[44] The resultant debate in the European Parliament led to recommendations being made to the Commission and the Council of Ministers concerning the principles that should form the basis of the Community's attitude to data protection[45].

These recommendations called on the European Commission to draft a directive to complement a common communications system; to harmonise the data protection laws and to secure the privacy of information on individuals in computer files. It advocated independent EEC action, since no other international organisation had yet established its own rules. It recognised that OECD guidelines would not be binding and expressed reservations about waiting for the Council of Europe, since it would take a long time for 26 nations to pass appropriate legislation. Any Community data protection law, as envisaged by the Sub-Committee, would be derived from the Swedish system of prior license and control, and adopted in whole or part by Denmark and France, rather than the Federal Republic of Germany's system of self-regulation in a statutory framework.

In July 1981, soon after the Council of Europe Convention had opened for signature, the European Commission recommended all members to sign it and seek to ratify it by the end of

---

[42] E.P.Debates No.186/254, 21 Feb.1975.

[43] Resolution on the protection of the rights of individuals in connection with data processing; OJ 1976, C100, p.27, 3.5.1976.

[44] Named after the rapporteur. Report on the Protection of the Individual in the face of the technical developments in data processing, 1979-1980 Eur.Parl.Doc. (No.100) 13 (1979).

[45] OJ 1979, C140, p.34, 5.6.1979.

1982[46]. However, as yet only seven out of the twelve member states have passed data protection legislation.

A second parliamentary report, the `Sieglerschidt' Report, was published in 1982.[47] The report noted "that data transmission in general should be placed on a legal footing and not be determined merely by technical reasons"[48]. It recommended the establishment of a "European Zone" of members in the EEC and Council of Europe, within which authorisation before the export of data would not be needed. It also indicated that initiatives, such as a Directive, was still necessary "as urgently needed as ever before to provide the highest possible level of protection"[49]. Following the report, a resolution was adopted by the European Parliament, on 9 March 1982, calling for a directive if the Convention proves inadequate[50].

However, in the context of 1992 and the `single market', the European Commission has, over recent years become interested in data protection legislation again, to ensure that divergent national legislation does not constitute an obstacle to the creation of the `single market'. Indeed, data protection issues have been referred to within a number of other European Community initiatives[51]. In August 1989, at the 11th International Conference of Data Protection Commissioners, the final resolution called upon the European Community to take direct action in this area[52].

4.3.4.2 The draft directives

"If the fundamental rights of citizens, in particular their right to privacy are not safeguarded at Community level, the cross-border flow of data might be impeded just when it is becoming

---

[46] Commission Recommendation of 29 July 1981, relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, OJ No. L 246/31, 29.8.1979, 81/679/EEC.

[47] Second Report on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing, E.P.Doc.1-548/81, 12 Oct.1981.

[48] Ibid., at p.7.

[49] It also gave four other reasons why European Community action was necessary: 1. The OECD decisions have no binding force; 2. the Council of Europe Convention is optional; 3. the Convention falls short of the European Parliament's ideas to date; 4. Community rules are necessary for intra-Community data flows. Ibid., at p.31-32.

[50] OJ No. C87, p.39, 5.4.1982.

[51] Eg. the Open Network Provision (ONP) draft Council directive and the European Commission Recommendation of 17 November 1988 `concerning payment systems, and in particular the relationship between cardholder and card-issuer'.

[52] `Berlin Resolution of the International Conference of Data Protection Commissioners of 30th August 1989'. An additional statement was issued by the Data Protection Commissioners of the European Community Nations. See Privacy Law & Business, p.19-21, No.11, September 1989.

essential to the activities of business enterprises and research bodies and to collaboration between Member States' authorities in an area without frontiers"[53]

This statement was delivered by the European Commission in July 1990, when the proposed directive on data protection was published. The Directive, when adopted, is likely to require significant changes in the UK's Data Protection Act 1984 (DPA), and impose new burdens on businesses with regard to the processing of personal data.

As outlined above, finally, after years of discussion, the Commission decided that a Community initiative was necessary in the area of data protection. The Commission therefore put forward a package of six proposals dealing with data protection:

1. A draft framework directive on data protection, based upon a number of principles[54], the first supra-national law on data protection;

2. a recommendation that the European Community, as a supra-national governmental institution, adheres to the 1981 Council of Europe Convention on data protection. It is within the framework of this international agreement that the EEC intends to ensure the protection of personal data transferred to third countries, in particular Eastern Europe[55];

3. a resolution to extend the protection offered by the directive (1) to all personal data held in the public sector, that do not fall under the scope of European Community law (eg. crime and defence);

4. a declaration extending the data protection principles to all the personal data held by Community institutions and bodies;

5. a draft directive for the telecommunications sector, especially the Integrated Services Digital Network (ISDN)[56];

---

[53] "Draft proposal for a Council Directive approximating certain laws, regulations and administrative provisions of the Member States concerning the protection of individuals in relation to the processing of personal data", p.4, para.6, COM(90) 314 final SYN 287, 13.8.1990; O.J. No.C277, 5 Nov. 1990 (hereinafter referred to as the 'general directive'.

[54] Ibid.

[55] This action is possible due to Article 210 of the Treaty of Rome, which gives the Community an independant legal personality, and thus the ability to enter into international legal committments; see also Nugter, A.C.M., *Transborder Flow of Personal Data within the EEC*, p.297, No.6 Computer/Law Series, Kluwer/The Netherlands 1990.

[56] "Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and public digital mobile networks" SYN 288 (hereinafter referred to as the 'Telecoms directive').

6. a draft Council decision to adopt a two-year plan in the area of security for information systems. This could lead to minimum European standards/guidelines being developed and imposed on businesses[57].

The proposals arose from the work of DG-3 (Internal Market) and DG-13 (Telecommunications, Information Industries and Innovation) of the Commission.

The Commission has put forward a number of reasons to justify the need for data protection activity. The primary purpose, as illustrated in the introductory quote, is to ensure the free flow of data as part of the programme to establish the `Single Market' under Article 100a of the EEC Treaty. Since the 1981 Commission recommendation, calling on Member States to sign and ratify the Council of Europe Convention on data protection (No.108) by the end of 1982, only seven of the twelve Member States have passed data protection legislation: the UK, the Republic of Ireland, France, Germany, the Netherlands, Denmark and Luxembourg. Even between these seven Member States `remarkable divergences' exist in the form of legislation, in particular the Commission notes six key differences:

- Coverage of manual data;
- protection for legal persons (eg. companies);
- the extent of a data user's duty to inform the data protection authority of what personal data is held (eg. the registration requirement);
- the giving of information to the data subject at the point of data collection;
- additional protection for categories of `sensitive' data;
- and, restrictions on the export of personal data[58].

However, the Commission also asserts the need to protect an individual's right to privacy. The different levels of data protection in the Community are seen as a potential obstacle to the development of the Community's data processing industry, in particular the growth of the new telecoms services. The existence of `data havens', countries with no data protection, are also seen as potentially distorting competition within the Community, since businesses might move to such countries to avoid the processing restrictions that exist in other Member States. Overall, the

[57] The proposal, at Article 6, establishes a Senior Officials Group on Information Security (SOGIS) to advise the Commission in this area. Article 2 proposes six `lines of action', including an analysis of user security requirements and the "integration of certain security functions in information systems".

[58] op.cit. supra n.53, at p.15.

intention of the Directive is to establish `a high level of protection throughout the Community'[59], rather than the `minimum approach' of the Council of Europe and OECD.

The draft directive is ambitious in seeking to cover "every situation in which the processing of personal data involves the risk to the data subject". The text therefore covers both manual and automated files[60], both public and private sectors. The movement of data from the public to the private sector is seen as posing the greatest threat to individuals. The Directive does not extend protection to `legal persons' (eg. companies and trade unions), that are currently protected under the data protection legislation of two Member States; Denmark and Luxembourg.

It is intended that the Commission will issue further sectoral data protection directives (the first covering the telecommunications sector) as appropriate; or alternatively will encourage the use of codes of conduct.

The following provisions of the Directive, if they remain unchanged, could have a significant impact on the use of data communications, particularly when compared to the current situation in the UK, under the 1984 Data Protection Act:

Article 9:

> (1)....at the time of first communication or of the affording of an opportunity for on-line consultation the controller of the file shall inform the data subject accordingly...

In addition, the data subject has the right to veto any such communication (Art.9(3)).These procedures for notification on first use of a person's data are "designed to ensure the transparency essential to the exercise by the data subject of the right of access". However, they could also create a substantial bureaucratic obstacle to data communications. Currently, under the UK Act, companies are allowed to transmit data to any third-party simply included in the registration details[61].

Article 18:

---

[59] Ibid., at p.5.

[60] Ibid., Article 2.

[61] The UK Data Protection Act of 1984 [hereinafter referred to as DPA'84], 1 Halsbury's Statutes of England, Current Statutes Service (Butterworths) 1189 (1984), s.4(3)(d). See generally Savage, R.N., and C. Edwards, *A Guide to the Data Protection Act*[2nd ed.], Financial Training, 1985.

Data Security -

"(1).....Such measures shall ensure in respect of automated files an appropriate level of security having regard to the state of the art in this field, the cost of taking the measures, the nature of the data to be protected and the assessment of the potential risks. To that end, the controller of the file shall take into consideration any recommendations on data security and network interoperability formulated by the Commission...

(2) Methods guaranteeing adequate security shall be chosen for the transmission of personal data in a network."

In addition, under Article 11 (2), data users will be required to provide the national `supervisory authority' (ie. the Data Protection Registrar) with a `general description' of the security measures that have been taken in compliance with Article 18 (2). Drawing the line between the provision of a description of such a general nature that it would be pointless and a description of security measures that could threaten their effectiveness is likely to be the subject of substantial debate.

Although the general requirement is the same as that contained in the UK Act[62], the reference to the role of the European Commission suggests that there could be a movement towards the harmonisation of security procedures. Indeed, there are already certain technical standards and evaluation criteria for data security being promoted within Europe[63]. Data users are not, however, obliged to follow any such recommendations.

Article 24:

"Transfer of personal data to third countries -

(1).....may take place only if that country ensures an adequate level of protection.

(2) The Member States shall inform the Commission of cases in which an importing third country does not ensure an adequate level of protection.

(3) Where the Commission finds.....that a third country does not have an adequate level of protection and that the resulting situation is likely to harm the interests of the Community or of a Member State, it may enter into negotiations with a view to remedying the situation."

---

[62] See section 4.4.2 below.

[63] See European Commission document `ITSEC' (version 1.2) issued in June 1991 by DG-XIII; and Chapter 2, at 2.3.4. The Telecoms directive, at art.8(1), requires `telecommunications organisations' to provide "adequate, state-of-the-art protection".

Unlike the Council of Europe Convention and the OECD Guidelines, the Directive has chosen to use the term `adequate' as opposed to `equivalent' protection[64]. Such a term would perhaps seem to be a less strict requirement. It could, however, be easily argued that the US, with little private sector data protection legislation, fails to meet either term!

The role the Directive gives to the Commission goes beyond that which it normally carries out. Indeed, the Commission is not even placed under any obligation to negotiate within a particular period, therefore enabling the process to be extremely long. However, Article 25 allows derogation from Article 24; it states:

> "(1) A Member State may derogate from Article 24(1) in respect of a given export on submission by the controller of the file of sufficient proof that an adequate level of protection will be provided. The Member State may grant a derogation only after it has informed the Commission and the Member States thereof and in the absence of notice of opposition given by a Member State or the Commission within a period of ten days."

The reference to `a given export' would suggest that the procedure would be a complex and time-consuming activity, for each individual data user. Such a provision could severely restrict international data flows[65].

The general directive has recently completed consideration by five committees within the European Parliament[66]. The Economic and Social Committee (a parallel advisory body to the Parliament, composed of representatives from employers, trade unions and other interest groups) has also been consulted to advise on the draft. The Directive has now returned to the Council for the drafting of a new composite Directive, which reflects the various interests and amendments that have been suggested. However, it is intended to be in force by 1st January 1993, in line with the establishment of the `Single Market'. Once passed, countries have two years in which to implement the Directive in national legislation.

---

[64] However, in the Report of the Committee on Legal Affairs and Citizen's Rights (The Geoffrey Hoon Report), dated 15 January 1992 (ICC Document No.373-22/Int.106), the term `equivalent' has been substituted for `adequate' in the suggested amendment to Article 4(1)(b). This change has not been followed, however, in the suggested amendments to Article 24 and 25.

[65] Ibid. The Report has suggested amending this clause to state: "a given export or type of export of personal data". This would enable precedents to be set for categories of data, and thereby remove the need for a case-by-case bureaucratic process..

[66] Ibid. The Report proposes a new provision, Article 16(1a), which would require data users to maintain an audit trail of all data sources to enable inaccuracies to be corrected all the way back to the orignal source. Such a provision could impose serious limitations upon the ability of data users to make computational alterations (eg. segmentation, aggregation etc.) to the data they have received.

It can be anticipated that there will be considerable lobbying from interest groups, representing the views of data users, data subjects and existing national data protection authorities, before the final text is agreed[67]. Within the governments of the Member States, the UK's Home Office has declared the current opinions to be as follows:

> "The French, German and Luxembourg representatives have declared themselves broadly in favour of the Directive's approach. Ireland, the United Kingdom, the Netherlands and Denmark have expressed reservations about a number of the requirements which go beyond the Council of Europe Convention; and the other states, which do not yet have data protection laws in operation, have not expressed firm views."[68]

The other major legislative initiative in the area of data protection is the sectoral directive covering telecommunications[69]. In the area of telecommunications, it is the appearance of the Integrated Services Digital Network (ISDN)[70] and mobile networks[71], in particular, that have given rise to privacy concerns. The directive is limited to `public telecommunication services'[72], and therefore does not cover private networks; however, the directive will impact on data communications when sent over the public network[73].

The following provisions within the Telecoms directive could impact on the use of data communications involving personal data:

- Article 5(2) - "the contents of the information transmitted must not be stored by the telecommunications organisation after the end of the transmission". This could cause difficulties for store and forward communication systems, or when messages are retained within the network for data security purposes[74].

---

[67] See Ihnen, U., "Battle for EC draft directive continues, but revised version on horizon", p.3-5, Privacy Laws & Business, No.18, October 1991; Chace, C., "Big split on data laws", The Guardian, January 8, 1991 and Pounder, C., "EC sharpens the claws of data protection law", p.24-25, Computing, 18 October, 1990.

[68] Presentation by Philip Stevens, Principal, Data Protection Policy, The Home Office, at Privacy Laws & Business 4th Annual Conference, Cambridge, July 2-4, 1991.

[69] The Telecoms directive, op.cit. supra n.56.

[70] Voice, text, image and data can all be passed over the same communications lines.

[71] This includes mobile data networks, eg. Hutchison Mobile Data Network Ltd..

[72] Article 2 and 3.

[73] See further Chapter 2. Article 20 gives the Commission the power to extend the directive to cover private networks. The Hoon Report, op.cit. supra n.64, at p.40, suggests amending the scope of the proposed Directive to cover "public and private digital mobile networks and public and private value added services".

[74] See Chapter 6, at 6.3. The Hoon Report, ibid., at p.41, suggests amending this provision to allow for the contents to be stored "where the telecommunications organisation has contracted with a service provider to store such information".

- Article 7(2) - information may not be disclosed externally, unless authorised by law or with the subscribers consent. Such a provision has been described as "unworkable in the context of interconnect agreements and for network planning and fraud prevention"[75].

- Article 8(2) - imposes a duty upon `telecommunication organisations' to inform subscribers to `mobile radio telephony' services, such as a mobile data network, of the security risks involved, and "offer them an end-to-end encryption service". This latter requirement could create particular problems for service providers.

The Telecoms directive has been greeted with a significant amount of opposition from the industry, and there is a strong move to limit the scope of the directive to voice telephony[76]. Substantive discussions on amending the text are being delayed until the future structure of the general directive has been clarified.

The primary aim of the draft directives is to enhance harmonisation, removing restrictions on the flow of data between Member States; however, alternatively, current developments could result in the creation of a `fortress Europe' with respect to data protection[77].

4.3.5 The Data Protection Principles

> "One constantly witnesses the rapid obsolescence of legal solutions which have been brought to bear on one single technical matter or on one single problem. In this way, one realizes the need to determine principles and to relate them to long-term tendencies."[78]

The UK Data Protection Act 1984, is based around eight general principles[79]. These principles are intended to be good practices that data users should comply with in order to protect the data

---

[75] Durie, R., "Problems with data protection legislation", p.164, in Proceedings of `Legal, Contractual, Responsibility & Evidential Issues in EDI, EFT, EM, Fax & Telex Communications', London, 20 February 1992.

[76] Ibid., at p.169.

[77] As expected, the draft directive has generated significant criticism from business. The draft is currently undergoing signifcant re-drafting and a new version is expected to be issued in April/May 1992. According to recent comments made by members of the European Commission, the three key areas are: (a) coverage of manual records will remain; (b) a separate directive will be drafted for the direct marketing industry and (c) the distinction between public and private sector data processing will be removed. See Dresner, S., "International Data Protection Up-date", Applied Computer and Communications Law, Vol.9, No.3, 1992.

[78] Rodota, Professor Stefano, `Policies and Perspectives for Data Protection', p.13,Proceedings of the Fourteenth Colloquy on European Law - Beyond 1984: The Law and Information Technology in Tommorrow's Society, p13-41, Council of Europe Conference, Lisbon, 26-28 September 1984. See also Clariana, who states that "a declaration of principles....provides greater flexibility and adaptability to technological change...", in "The Legal Framework of International Data Flows", I.B.I., "Proceedings of the Second World Conference on Transborder Data Flow Policies", Rome, 26-29 June 1984, TDF 260, at p.40..

[79] DPA 84, op.cit. supra n.61, at Schedule 1.

they hold, in both their interests and those of their data subjects. These principles are fundamental to an understanding of the basis of data protection legislation in Western Europe.

The principles were originally developed in the 1972 Younger Report[80], which argued that the government should ensure that private sector data users comply with ten principles of good data processing. These principles, reduced down to eight (!), were considered central to the recommendations of the 1978 Lindop Report[81].

Internationally, the data protection principles were adopted as the basis for the 1980 OECD Guidelines[82]. Indeed, the general concern over transborder data flow restrictions within the OECD, led to the drafting of separate principles to safeguard the flow of non-technical data, although they were never adopted[83]. The principles contained within the 1984 Act are designed to comply with the principles as stated in the Council of Europe Convention on Data Protection[84].

Under the UK Act, the Principles are expressed in very general terms and are therefore not directly enforceable through the courts, but only through the actions of the UK Data Protection Registrar. Where a data user breaches one of the principles, the Registrar can issue an `enforcement notice'[85], specifying the nature of the breach and outlining the measures that will need to be taken in order to correct the breach. If the data user fails to comply with the notice, then the Registrar can issue a `deregistration notice'[86]. This notice orders a data user to cease processing personal data immediately. The Principles are also intended to act as a basis for sectoral codes of practice[87].

The first principle states:

---

[80] Report of the Committee on Privacy (Chairman: Kenneth Younger), Cmnd 5012, HMSO, London, 1972.

[81] op.cit. supra n.9.

[82] The Guidelines, op.cit supra n.35, are based upon eight, self-explanatory, principles of good data protection practice: `Collection limitation', `data quality', `purpose specification', `use limitation', `security safeguards', `openness', `individual participation' and `accountability'. In the US, these principles are usually referred to as `fair information practices'; see for example Reidenberg, J., "Personal Information and Global Interconnection: The Challenge of Regulatory Convergence", pp.27-36, The Economic Integration Frontier, Project Promethee Perspectives n.18-19, December 1991.

[83] Bing, J., P. Forsberg, and E. Nygaard, *Legal Issues related to transborder data flows*, DSTI/ICCP/81.9; Appendix II: `Tentative Outline of Principles for the Free Transnational Flow of Non-Personal Data'. The document outlined eight principles, eg. national authorities "should not routinely sample or supervise the contenst of transnational data flows". See also "Second World Conference on Transborder Data Flow Policies: Working Document", Rome, 1984, p.47-48, which outlines eight basic principles for TDFs; including, `preservation of culture and language' and `availability of information on data transmission research' (quoted in Sauvant, K P, *International Transactions in Services: The Politics of Transborder Data Flows*, The Atwater Series on the World Information Economy No 1, Westview Press/London, at p.248-249).

[84] The Convention, op.cit. supra n.5, at Chapter II - `Basic principles of data protection'.

[85] DPA'84, op.cit. supra n.61, at s.10.

[86] Ibid., at s.11.

[87] Ibid., at s.36(4); See further section 4.6.2 below.

"Information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully"

It would be a breach of the first principle if the data subject, or data provider, were deceived or misled about the purpose for which the data were obtained, held, used or disclosed[88].

Data protection principle number two specifies that:

"Personal data shall be held for one or more specified and lawful purposes".

For example, a contravention of this principle would occur if an organisation were to register the holding of personal data for purposes of personnel management, and use it additionally for marketing purposes. This principle does not limit the processing of data, it merely requires such activities to be registered, in accordance with the requirements of the Data Protection Act 1984.

The third principle states that:

"Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or purposes"

Disclosure is therefore not restricted as long as the details are made public, within the requirements of the Register. This principle would be breached if an organisation sold information to a third party after collecting the information purely on the registered basis of an internal purpose of the organisation.

Principle four relates the need to only hold personal data that is "adequate, relevant and not excessive in relation to that purpose or those purposes". This principle is concerned with the collection of data, often a manual operation carried out separate from the computer process. It also implies that data users need to continually monitor/audit the data held, to assess changes in relevance etc., a complex and time-consuming process for modern databases, unless accounted for when designing the system.

---

[88] See further Walden, I., "The First Principle and Direct Marketing", p.3-4, Applied Computer and Communications Law, Vol.8, No.1, 1991.

The fifth principle requires that all personal data "shall be accurate and, where necessary, kept up to date". If, for example, an organisation purports to keep a list of undischarged bankrupts, but makes no effort to seek information on persons discharging themselves from bankruptcy, it will be contravening this principle.

Opinions that do not claim to be a statement of fact are therefore not covered by this principle. If information has been obtained from a third party it has to be recorded as such, as well as any challenge to the accuracy of the information by the data subject to which it refers. If these conditions are met, then the inaccurate data does not breach this principle.

The Registrar has put forward the issues that he may consider when dealing with a potential breach of this principle. These include, the significance of the inaccuracy; whether reasonable steps where taken by the data user to check the accuracy of information held and what procedures were followed by the data user once the inaccuracy was brought to light.[89]

Data users will also need to focus on the specific security concerns relating to the identifying data element, "which relates the stored data to a certain individual"[90]. This component can be viewed as the means of authenticating the data[91]. The accuracy requirement and degree of protection attached to this element should therefore reflect its unique role. For example, if identification of an individual is made via an address, then it is critical that this data element is detailed enough to reflect the fact that the location may be divided into separate units.

With regard to keeping information `up-to-date', the nature of the information and its purpose, will be relevant to compliance. For information acting as a historical record, it may not be necessary to carry out periodic examinations to determine if the data require updating[92].

Principle six states that personal data "shall not be kept for longer than is necessary for that purpose or those purposes". This principle seems to imply that data should be destroyed when

---

[89] Guideline 4, `The Data Protection Principles', p16. The Guideline series is available free from the Office of the Data Protection Registrar, Wilmslow.

[90] Bing, J., "Reflections on a Data Protection Policy for 1992", p.171, *Yearbook of Law Computers & Technology*, Vol.5, Butterworths, 1991 (Paper presented at the Conference, `Access to public sector information, data protection and computer crime', held by the Commission of the European Communities and the Council of Europe, Luxembourg, 27-28 March, 1990).

[91] See Chapter 5, at 5.3.3.

[92] Eg. where an evidential/security `log' of all messages sent and received by an electronic messaging system is being maintained; see Chapter 6, at 6.3.3.

the specified purpose for which they were collected has been achieved. Such a process will require the same form of periodic review mentioned with regard to Principle 5.

The seventh principle relates to a data subject's right to know `at reasonable intervals' if personal data is held on him and to have access to such data. The data subject is also given the right to have such data corrected or erased, `where appropriate'.

A data subject has an `appropriate' right to correction or erasure of personal data only where it is necessary to comply with the other Data Protection Principles, such as when data is irrelevant or inaccurate. However, a data subject does not have a right to get personal data removed simply because he does not want particular data users to have data about him.

An individual's access rights are central to data protection legislation, although Article 8 of the Council of Europe Convention states that such rights are `[a]dditional safeguards for the data subject'![93] The first necessary stage in the exercise of the `right of access' is to discover the existence of the files, since `access' is not a meaningful term unless combined with a knowledge of where the files are.

Two main procedures have been adopted, within European data protection legislation, to achieve the objective of discovering the existence of a file: a public register or a notification procedure. This former is that contained in the UK Data Protection Act. The Register[94] is a record of the range of files held by the data user, but does not tell an individual if he/she is included. Alternatively, a `notification' procedure usually involves the data user informing the subject when a file is created on them[95], or upon communication to a third party[96]. This is very bureaucratic in terms of an organisations administration, but does establish the positive `right to be informed', which is more meaningful than mere `access' rights.

The last principle concerns data security, and requires that `appropriate security measures' are installed by data users against `unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data'[97].

---

[93] op.cit. supra n.5, p32.

[94] DPA'84, op.cit. supra n.61, at s.4.

[95] Eg. The Netherlands, Wet Persoonregistraties [Rules for the protection of privacy in connection with personal data files, January 6, 1989, Staatsblad 1989, 665; hereinafter referred to as "The Netherlands"], at s.28(1): the data user must give written notification within one month of file creation.

[96] Eg. the EC draft directive, op.cit. supra n.53, at Article 9.

[97] See further at Section 4.4.2 below.

4.4 National Data Protection Legislation

Data protection legislation lays down rules and regulations designed to prevent personal information from being misused. Such legislation can be viewed as being concerned with issues related to information possession, as well as information communication. However, this thesis is primarily concerned with the impact on the latter.

The following sections will consider three specific aspects of data protection regulation, within West European legislation:

- Regulations controlling the transfer of personal data outside the national jurisdiction are designed to prevent the legislation from being circumvented;
- requirements upon the sender and recipient to enact an adequate data security policy are intended to protect data from loss, unauthorised access, etc.,
- and data protection legislation which covers legal persons (ie. companies), thereby significantly extending the scope of protection to much of the trade data that is communicated.

4.4.1 International Data Transfers

This section gives an overview of the provisions regulating the international communication of personal data in European data protection legislation. Such regulation of transborder data flows is obviously necessary in each country to ensure that data users cannot evade national data protection rules by processing abroad.

The Austrian legislation[98] contains the most strict and elaborate provisions concerning the transfer of data. Such transmissions are permitted provided that:

> "1. the data subject has expressly and in writing agreed to the transmission, which consent may be revoked in writing or
> 2. the transmission is part of the legitimate tasks of the person[99], or

[98] Bundesgesetz vom 18.Oktober 1978 uber den Schutz personenbezogener Daten; Bundesgesetzblatt 1978, pp.3619 ff (as amended July 1, 1987); hereinafter referred to as "Austrian".

[99] In 1988, the Data Protection Commission refused permission for a credit reference agency to transfer data concerning family status abroad. The Commission concluded that such information was not covered by the legitimate purpose of the agency; see Privacy Law & Business, p2, no.8, November 1988.

3. the transmission is necessary for the safeguarding of prevailing justified interests of third persons"[100]

In addition, data users are required to obtain a licence from the Data Protection Commission for certain international data transmissions[101]. Exemptions from the licensing requirement exist if the transmission is to a country designated as having `equivalent' legislation; or

"1. they take place according to national or international legal provisions which explicitly mention the classes of...data and the recipients, or
2. if the data subject asked for the transmission in writing, which request may be revoked in writing, or
3. if the data have been published legally in Austria, or
4. if the transmissions..are exempted from licensing by an Order of the Federal Chancellor after consultation of the Data Protection Council, because they are performed by a great number of data controllers and the contents of which are defined by law or by a contract with the data subject and if no privacy interests of the data subjects need protection.."[102]

Where a licence is issued, then the foreign data processing entity has to agree to comply with certain obligations[103], usually evidenced in contract[104].

Under the Danish private sector data protection legislation[105], a distinction is made between sensitive data, such as race and criminal matters, which can be processed and transferred only where provided by law or with the consent of the data subject; and other personal data, which can be transferred only "to the extent that this is a natural part of the normal operation of any business enterprise of the type in question"[106]. This last point could presumably limit the adoption of innovative data processing arrangements.

A licence must be obtained from the Data Surveillance Authority prior to the transmission of data in two circumstances:

---

[100] Austrian, op.cit. supra n.98, at s.18(1).

[101] Ibid., at s.33 & 34.

[102] Ibid. at s.32(1) & (2).

[103] Ibid., at s.34(2), the requirements are specified in s.19.

[104] See further Chapter 6, at 6.2.

[105] Lov om private registre m.v., Lov nr.293 af 8.juni 1978 (private sector, as amended on 1st April, 1988); hereinafter referred to as "Denmark".

[106] Bent Ove Jespersen, "International Data Transfers Experience", p48, Proceedings of the International Data Protection Commissioners Conference, Paris 1990.

(1) if the data are collected in Denmark for inclusion in a system subject to licence (eg. credit reporting agencies, black-listing), or sensitive data are collected for inclusion in a foreign register;
(2) export of a data for processing abroad, where the data includes sensitive data"[107]

Data users who want to export data to a foreign third-party are required to obtain contractual warranties, or similar controls, from the third-party that the system processing the personal data in the foreign jurisdiction will operate under the substantial provisions outlined in the Danish Act[108].

Under the Finnish Act, data users must notify the Data Protection Ombudsman when transferring data abroad. The notification must include details of source, recipient and the `time and manner of transferring'[109]. In addition, the consent of the data subject must be obtained, or the permission of the Data Protection Board, for any intended transborder data flows to countries other than those specifically exempted[110]. Only a few such applications have been made since the Act[111].

The Act also contains an extended provision regarding the transmission of data abroad, stating that such a transfer must not:

> "endanger the protection of the privacy, interests and rights of the data subject or the security of the State"[112]

The inclusion of the reference to the protection of the State imposes an obligation on data users of a fundamentally different nature to the protection of a data subject's personal data, and reflects concern shown in some countries that the increased use of international data communications by companies can threaten a State's sovereignty[113].

---

107 Denmark, op.cit. supra n.105, at s.21(1).

108 Jespersen, op.cit. supra n.106, at p49.

109 Partanen, H., "Finnish Regulation of International Data Transfers and Some Experience", p51, Proceedings of the International Data Protection Commissioners Conference, Paris 1990. About 25 such notices are made annually.

110 Personal Data File Act 1987, s.30, and Personal Data File Decree 1987, s.16 (unofficial translation published by the Ministry of Justice, Helsinki 1988; hereinafter referred to as "Finland"). The countries exempted comprises those with existing data protection legislation.

111 Partanen, op.cit. supra n109, at p52. The number quoted in 1990 was four.

112 Finland, op.cit. supra n.110, at s.22.

113 See Chapter 3, at 3.5.2.

In France, the transmission of data internationally is governed by Article 24 of the data protection Act[114], which states:

> "On the proposal or as advised by the Commission, the transmission between France and another country in any form of personal data subjected to automatic processing....may call for prior authorization or be regulated by decree made in the Conseil d'Etat, to ensure compliance with the principles laid down in this Act."

To date, no such specific regulations have been issued by the Conseil d'Etat; although CNIL[115], the French data protection authority, has made a number of `deliberations' concerning individual cases involving the export of data[116].

In Germany[117], there are no explicit provisions applying to TDFs in the private sector[118]. International data transfers are simply classified as a `third-person' ("Dritter") disclosure, and have to comply with the relevant requirements for all such disclosures.

If the personal data is being traded with a `third person', then the disclosure is only lawful in two cases:

- Where the data subject has given written consent; or
- the disclosure has been expressly authorised by legislation[119].

Where the transfer is intended for the data users own purpose (a non `third-person' disclosure), it has to be justified under one of three grounds:

- the transfer serves the purpose of the contractual relationship with the data subject[120];

---

114 Loi No.78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertiés, J.O. du 7 Janvier 1978 et rectificatif au J.O du 25 Janvier 1978; hereinafter referred to as "France".

115 The Commission Nationale Informatique et libertés.

116 See Section 4.5.1 below.

117 Gesetz zum Schutz vor Missbruach personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) vom 27 January 1977, BGB1. I 1977 S.201. On June 1, 1991, a new Federal Data Protection Act came into force, covering the united Germanies: Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesgesetzblatt 1990 I, p.2954 [hereinafter referred to as "German"].

118 TDFs by state authorities are regulated, under § 17.

119 German, op.cit. n.117, at Article 4(1).

120 Eg. the German subsidiary of a European airline wanted all employee information processed at the parent company's location. This was seen by the data protection athority to fall within the scope of the employment contract - quoted in Nugter, op.cit. supra n.55, p198.

- it serves the purpose of a quasi-contractual relationship of trust with the data subject; or
- it is necessary in order to safeguard the justified interests of the disclosing person or of a third party or of the general interest.

Where either the first or second condition applies, then the transfer is permitted. Where the third justification forms the basis upon which the transfer is to be made, then it is necessary to examine whether the recipient jurisdiction has an `equivalent' level of protection[121]. One company interviewed, stated that it would not allow the transfer of personal data to the US, since it lacks `equivalent' legislation[122].

A transfer by the data user to a computer bureau is not considered to be a `third-person' disclosure[123], unless the bureau is situated within a foreign jurisdiction.

The private sector data protection authorities (`Der Regierungspräsident') have, where the recipient state lacks `equivalent' protection, allowed the use of contractual agreements, whereby the recipient will ensure that the data subjects have the same protection as they would in Germany[124].

Under the new legislation in The Netherlands[125], section 49 states:

> "1. Any person having access from the Netherlands to a personal data file located outside The Netherlands and to which this Act does not apply shall ensure the security of that access and of the personal data obtained by that means.
> 2. Data shall not be supplied from The Netherlands to....any personal data file in another country to which this Act does not apply where it has been declared by General Administrative Order that such a transfer of data would have a serious adverse effect on the privacy of the persons concerned"

---

121 referred to as `Äquivalentzprinzip'.

122 Interview with Werner Vaupel, Datenschutzbeauftragter, Hoechst AG; 07/04/89. Thomas Hoeren believes that it "is very doubtful whether the English data protection law is equivalent to the German law", stated in "EDI and Transborder Flow of Personal Data: The perspectives of private international law and data protection", p.85, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992

123 German, op.cit. n.117, at Article 2 (9).

124 Interview with Hans Küchenhoff, Regierungsrat, 6/4/1989. See also Poullet, Y., "Privacy Protection and Transborder Data Flow: Recent Legal Issues", p32, in Vandenberghe, Prof. G.P.V., (ed.), *Advanced Topics of Law and Information Technology*, No.3 Computer/Law Series, Kluwer/The Netherlands 1989: p29-41. A Manchester Business School survey quotes an example of a Dutch company wanting to exchange data with its German subsidiary, the Dutch parent signed a declaration stating that it would abide by the German law; "Government and Business relations project: The Data Protection Act 1984", Manchester Business School, 8th April 1987.

125 The Netherlands, op.cit, supra n.95.

No such regulatory Order currently exists.

In Norway, the legislation[126] requires that the exporting data user must notify the Data Inspectorate of any such transfers. The notification should include details of where the data is to be sent, why and the method of transfer. The Inspectorate may then refuse such a transfer, or simply lay down certain conditions, such as requiring that the foreign data processing company contractually agrees to comply with the Norway data protection legislation[127]. The number of such notifications since 1980 is around 400[128].

The Data Inspectorate has noted that, in relation to the export of data, "..the way we have been practising the rules seem to avoid complaints and problems. The number of cases of dispute is extremely limited..."[129]

In Sweden, the data protection legislation requires that data users wishing to transmit data to a country which has not ratified the Council of Europe Convention must seek express authorisation from the Data Inspectorate:

> "..If there is reason to assume that personal data will be used for automatic data processing abroad, the data may be disclosed only after permission from the Data Inspection Board.....Permission is not required, however, if personal data are to be used for automatic data processing solely in a State which has acceded to the Council of Europe's Convention"[130]

Since 1982, when Sweden ratified the Council of Europe Convention, the Data Inspectorate has had fewer than one hundred such applications for permission, covering five major categories of personal data: employee files; customer files; direct marketing files; data for pharmaceutical testing and files on persons with a specific education or work area[131].

---

[126] Lov om personregistre m.m av 9.juni 1978 no.48 (as amended on 1st October 1987); hereinafter referred to as "Norway".

[127] See Citibank case, quoted in Privacy Laws & Business, p22, no.3, August 1987.

[128] Apenes, G., "International Data Transfers Experience", p53, Proceedings of the International Data Protection Commissioners Conference, Paris 1990.

[129] letter from Helge Seip, the Norwegian Data Inspectorate [3/11/87].

[130] The Data Act 1973 (SFS: Swedish Code of Statutes 1982: 446), as amended with effect from April 1, 1988, s.11 [hereinafter referred to as "Sweden"].

[131] Wahlstrom, S., "International Data Transfers Experience", p55, Proceedings of the International Data Protection Commissioners Conference, Paris 1990. Other types of data include international payment systems and debt collection and credit information.

The decision to allow such international transfers is based upon four primary considerations:

- the sensitiveness of the personal data;
- if liability could be demanded in the recipient State;
- if persons concerned have expressed their consent, and
- the national data protection legislation in the recipient State[132].

Permission is not required where the disclosure of personal data to a third country does not involve further `automatic processing' in that third country, such as the use of a Swedish on-line database service. In such circumstances, the recipient is not able to alter the data and is not considered to be a threat[133]. However, the Act does extend to the systematic collection of manual data in Sweden for ultimate processing in a foreign country.

The Data Inspectorate is not permitted by the Act to examine data being transferred to a country that has ratified the Convention; however, this can severely limit the Inspectorate's ability to monitor compliance with the legislation, especially possible further transfers outside of the Contracting Parties[134].

The United Kingdom Act[135], provides the Data Protection Registrar with the power to issue a `transfer prohibition notice' to an organisation processing personal data:

> "prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question."[136]

This notice prevents the organisation from transferring any such data to a third country.

Where the transfer of data is to a country that is a signatory to the Council of Europe Convention, the Registrar only has the power to restrict the transfer of data if he is satisfied that either of two conditions exist:

---

132 Ibid., at p55.

133 Ibid., at p54.

134 Ibid., at p56.

135 DPA'84, op.cit. supra n.61.

136 Ibid., s.12(1). This provision has been described as "elaborate provisions to regulate TBDF"! in Rankin, T. Murray., "Business secrets across international borders: one aspect of the transborder data flows debate", Canadian Business Law Journal, 10 (1985).

- There is likely to be a <u>further</u> transfer to a country, not a signatory to the Convention, and likely to contravene the data protection principles; or

- where the data is considered sensitive (under section 2(3)), with additional safeguards under the Act[137].

This provision has been seen as creating a potential problem when the intended transfer is to Spain. To date, although Spain has ratified the Convention, it has failed to pass any legislation enforcing the Convention in domestic law[138].

Criminal sanctions arise under the Data Protection Act 1984 in two categories: those of strict liability, and those requiring recklessness or actual knowledge. Offences giving rise to strict liability would include contravention of a transfer prohibition notice[139]. However, the Data User could also be guilty of an offence for knowingly or recklessly transferring data overseas other than described in the registered entry[140].

Prosecutions under the Act can only be brought by the Data Protection Registrar, with the approval of the Director of Public Prosecutions. The penalties for an offence involving an international data transfer are:

> "(a) on conviction on indictment, to a fine; or
> (b) on summary conviction, to a fine not exceeding the statutory maximum (as defined in section 74 of the Criminal Justice Act 1982"[141]

However, the enforcement of such provisions has rarely occurred[142], and not at all with regard to international data transfers.

---

[137] Ibid., s.12(3).

[138] See Aldhouse, F., "UK Data Protection - Where are we in 1991?", p.187, 5 Yearbook of Law Computers and Technology, Butterworths, 1991.

[139] Section 12(10).

[140] Section 5(2)(e).

[141] Section 19(2), the maximum is currently £2000. For offences under Section 6, the fine shall not exceed the fifth level on the standard scale (s.19(3)).

[142] See Halifax Building Society case, under s.5(2), in Gaskill, S.J., "Data Protection: Recent Court and Tribunal Cases", Proceedings of Privacy Laws & Business, 4th Annual Conference, Cambridge, 2-4 July, 1991.

4.4.2 Data Security

A critical element of effective data protection and communication is the need for data security[143]. The eighth principle of the UK Act directs that data users should ensure that they have `appropriate security measures' against possible loss, destruction, unauthorised disclosure or alteration[144]. Therefore, data users are required to maintain the confidentiality of the data, the accuracy of the data, and be able to satisfy the right to access the data and correct it if necessary. Although a failure to comply with the principle is not directly an offence, it could result in an `enforcement notice' being issued by the Registrar.

The Act quite clearly outlines the range of issues that should be considered when implementing `appropriate' data security. It states:

> "6. Regard shall be had -
>
> (a) to the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and
> (b) to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data."[145]

Data users are therefore expected to consider the sensitivity of the personal data they hold, and implement suitable security procedures. Such measures involve different aspects: Physical security, such as the security of disk storage facilities, from flood as well as unauthorised access; software security, such as maintaining a log of all failed access requests; and, operational security, for example with regard to work data being taken home by employees, and periodic data protection audits of the computer systems[146].

The Data Protection Registrar has also commented that the mere fact a breach of security has occurred will not be proof that the data user has been negligent, provided the data user has "done everything which could reasonably be expected"[147].

---

[143] See generally, Barber, B., "Data Protection, Computer Security, Standards and Safety", NHS Information Management Centre, July 1990.

[144] See also the Convention, op.cit. supra n.5, at Article 7 and the Guidelines, op.cit. supra n.35, at Paragraph 11.

[145] DPA'84, op.cit. supra n.61, at Schedule 1, Part II. See also *Security and the 1984 Data Protection Act*, NCC, 1987.

[146] See further Chapter 2, at 2.3.3.

[147] Guideline 4, op.cit. supra n.89, p.28.

There has recently been an attempt to extend the impact of the security provisions of the Data Protection Act. In 1990, a private member's bill was presented to the House of Commons which was designed to:

> "provide entitlement to compensation, in certain circumstances, to an individual who suffers damage...by reason of the unreliability or lack of security, of a computer, data or program.."[148]

Although the bill failed to get parliamentary support, it does illustrate the possible nature of future legislation, under a government of a different political persuasion, which might be introduced.

Other European data protection legislation has also made explicit reference to the need for data security measures, although varying in the degree of detail and direct intervention by the data protection authority. For example,

- In the Austrian Act, the legislation states seven specific security procedures for companies to implement, including checks on the effective implementation of the security measures and authentication protocols[149];

- Under the Danish Act, the Data Inspectorate reserves the right to "prescribe the precautions considered necessary to achieve the proper security"; as well as a specific prohibition on the use of a person's national registration number on the external surface of mail[150] (although it is not clear if this would apply to the use of an electronic mail service). If data users neglect to implement proper security measures, it is a criminal offence[151]

- In France, the CNIL has the right to establish security standards[152];

- The German private sector is required to appoint a Data Protection Controller[153], whose general duties extend to the implementation of internal data security procedures. In this

[148] Rowe, H., "The UK `Computers (Compensation for Damage) Bill", p.6, Applied Computer and Communications Law, Vol.7, No.8, September 1990.

[149] Austrian, op.cit. supra n.98, at s.10(2).

[150] Denmark, op.cit. supra n.105, at s.2-1(4).

[151] See also Luxembourg Loi dun 31 mars 1979 reglementant l'utilisation des donnees nominative dans les traitements informatiques, Journal Officiel du Grand-Duche du Luxembourg A No.29 11 avril 1979 (Personal Data (Automatic Processing) Act, Council of Europe Info.Doc. CJ-PD (79) 3; hereinafter referred to as "Luxembourg".

[152] France, op.cit. supra n.114, at s.21(3).

respect, the Act includes an annex which specifies ten aspects of data security which must be taken into account[154]: `admission control', `leakage control', `memory control', `user control', `access control', `dissemination control', `input control', `control of processing on behalf of other parties', `transport control' and `organisation control'.

Companies which either sell, disclose or act as data processing enterprises for other companies are required to register with the `Rigierungspräsident' of their Lande[155], and are regularly inspected to check on the transmission of data and the security arrangements[156].

- The Icelandic Act contains an unusual and extremely vague clause stating that "for data which is considered likely to be useful for foreign states, security measures shall be applied to facilitate the destruction of records without delay in case of the outbreak of war or fear of eventual hostilities"[157]

- Under the Norwegian Act, data security rules can be introduced by the government. A working group appointed by the Ministry of Justice, and chaired by a member of the Data Inspectorate, has drafted a detailed set of `Personal Data Files Security Regulations' for data users[158].

The Council of Europe Convention, at Article 7 requires that:

> "There should be specific security measures for every file.....They should be based on the current state of the art of data security methods and techniques".

In addition, under Article 6, it states that "special categories of data" may need to be given additional safeguards. Indeed, most European data protection legislation, including France, Norway and Sweden, have provisions which explicitly address the question of `sensitive' data. However, different national traditions make it impossible to offer general rules to categorise `sensitive' data. For example, under Norwegian law, data concerning a persons sexual life is

---

153 German, op.cit. supra n.117, at s.28.

154 Ibid., Annex to s.6(1).

155 Ibid., at Part IV: `Commercial data processing by private bodies for other parties in the normal course of business', ss.31-40.

156 Interview with Hans Küchenhoff, Der Regierungspräsident in Darmstadt - 06/04/89.

157 Act No.39/1985 with regard to the Systematic Recording of Personal Data (English Translation: Council of Europe Info.Doc. CJ-PD (86) 15) [hereinafter referred to as "Iceland"]; at Art.9.

158 `Proposal for Regulations for Security Regarding Personal Registers', unauthorized translation presented by Datatilsynet at the International Data Protection Commissioners Conference, Oslo, 1988.

considered `sensitive', while it is not mentioned in French law. However, under French law, trade union affiliation is considered `sensitive', while not in Norway.

Within the UK Act the Secretary of State has the power to provide additional safeguards for information relating to:

> "(a) the racial origin of the data subject;
> (b) his political opinions or religious or other beliefs;
> (c) his physical or mental health or his sexual life; or
> (d) his criminal convictions"[159]

To date, no such supplementary provisions have been made.

Some national data protection legislation has been widely drafted to cover certain types of computer misuse, in particular `unauthorised access', which may require the breach of security measures in order for an offence to be committed. In Finland, the Personal Data Files Act states that a person commits an offence of unauthorised access a person:

> "through the use of a user code that does not belong to him or through other fraudulent means passes a control or identity or a corresponding security system and thus without authorization gains access to a personal data file"[160].

4.4.3 Legal Persons

One particularly important debate in the field of data protection concerns the extension of data protection legislation to cover organisations, or `legal persons'. The debate focuses on two issues. First, the narrower issue based on the argument that legislation should extend to organisations, particularly smaller enterprises, because information about the organisation may implicitly be information about the organisations owners and controllers. Second, the wider issue, that organisations have legitimate rights in respect of information about them held by others in the same way that individuals have. However, the extension of data protection legislation to legal

---

[159] DPA'84, op.cit supra n.61, at s.2(3).

[160] See Finland, op.cit supra n.110, at, s.45. See also section 145 of the Norwegian Penal Code (amended 1987) which covers persons "breaking security measures to gain access to data/programs"; and the Sweden, op.cit. supra n.130, at s. 21, which creates the offence of `data trespass'. See generally Chapter 3, at 3.4.3.

persons could seriously affect the use of electronic messaging systems for the communication of commercial data.

Five Western European nations currently include both physical and non-physical persons in the `data subject' sections of their data protection legislation, while of six European countries currently considering legislation, three are intending to include protection for non-physical persons[161].

Five major European nations have enacted data protection legislation that covers both natural and artificial persons, Norway[162], Austria[163], Iceland[164], Luxembourg[165] and Denmark[166]; while the French CNIL extended the scope of the national legislation, to cover legal persons, by an administrative decision[167].

Most international organisations have refrained from considering in-depth the non-physical persons issue, possibly because of the considerable political and economic arguments that such an investigation would engender. The two international agreements on data protection that do mention the issue, the OECD Guidelines and the Council of Europe Convention, do not call for national legislation to include corporate persons as data subjects. However, they exhibit different attitudes to the possibility of such an inclusion, which reflects their differing origins and priorities.

The OECD, an organisation designed to promote economic development among the major Western nations, asserts:

> "the notions of individual integrity and privacy are in many respects particular and should not be treated in the same way as the integrity of a group of persons, or corporate security and

---

[161] Switzerland, Hungary and Italy are currently considering bills on data protection which would include artificial persons. Belgium, Greece and Spain's proposed legislation would not.

[162] Norway, op.cit. supra n.126, at Para.1: "The term `personal information' shall mean information and assessments which are, directly or indirectly, traceable to identifiable individuals, associations or foundations."

[163] Austrian, op.cit supra n.98, at s.3.2: "natural and legal persons or associations of persons under commercial law whether specifically identified or likely to be identifiable".

[164] Iceland, op.cit. supra n.157, at Art.1: "The present Act applies to any systematic recording of data concerning private affairs of individuals as well as financial affairs of individuals, establishments, concerns or other legal persons which should reasonably and normally be kept secret."

[165] Luxembourg, op.cit. supra n.151, at Art.2: "Person means any natural person, public or private corporate body or group of persons."

[166] Denmark, op.cit. supra n.105, at s.1(1): "..comprising private or financial data on any individual, institution, association or business enterprise..".

[167] On July 3rd 1984.

confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another."[168]

This seems to suggest that existing business and commercial law contains protective measures that can be relied upon to serve the interests of the artificial person, such as copyright laws, credit-rating legislation and the law of tort, including the action for breach of confidence[169].

The Council of Europe, on the other hand, is an organisation specifically dedicated to safeguarding human rights. In 1971, the International Association of Lawyers submitted to the Council of Europe two proposals for the protection of privacy that assumed the interests of individuals and companies were similar[170]. They were an attempt to combine into one law protection of the personal sphere against intrusions, personal data against unauthorised operations of electronic data banks and industrial and commercial data against illicit appropriation. The Council took no further action on these drafts, deciding that too many questions has been placed together[171].

The Council of Europe does not include artificial persons in the main body its the 1980 Convention on data protection, however, it states that legislation can be extended to include information relating to:

> "groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality"[172].

It continues by saying that states that include such categories in their data protection legislation may then invoke the rule of reciprocity with regard to states who have not made such extensions (Article 3(4)).

In addition to the possibility of protection under the Council of Europe Convention, under Article 25 of the European Convention on Human Rights, any person, including any `non-governmental

---

168 Guidelines, op.cit. supra n.35, at Appendix, para.3.

169 See Chapter 3, at 3.4.4.2.

170 "Draft Articles for an International Convention for the Protection of Personal and Industrial Privacy" and "International Agreement for the Protection of the Personal and Industrial Sphere"

171 See Hondius, F.W., *Emerging data protection in Europe*, North Holland, Amsterdam, 1975, at p.97.

172 The Convention, op.cit. supra n.5, at Art.3(2b).

organisation or group of individuals' may claim to be a victim of a human rights violation, including the right to privacy, and thus petition the support of the Human Rights Commission[173].

The European Community considered the issue in the `Bayerl' report, which investigated whether an EEC Directive should be issued on data protection[174]. The Report concluded that giving access to corporate files might facilitate companies gaining access to propriety information of their competitors.

In the United States, privacy protection tends to concentrate on the interests of the individual, guarding against unwarranted intrusions or disclosure by the Federal government and other public entities. Controls on the disclosure of personal information by federal agencies was introduced in the Privacy Act of 1974[175]. No omnibus Privacy Act exists for the private sector, even at state level; however, specific regulations have been enacted dealing with financial information[176].

As far as the issue of non-physical persons is concerned, the 1974 Privacy Act only gives protection to individuals as citizens of the United States, or an alien lawfully admitted for permanent residence, not to non-physical persons. More generally, case has suggested that the creation of a right of privacy for legal entities identical to natural persons is unacceptable to American law. In *U.S. v Morton Salt Co.* (1949), the United States Supreme Court stated that:

> "while they [corporations] may and should have protection from unlawful demands made in the name of public investigation...corporations can claim no equality with individuals in the enjoyment of a right of privacy"[177].

Indeed, the free flow of commercial information has been recognised as falling under the protection of the First Amendment of the Constitution[178].

---

[173] European Convention on Human Rights 1950, Cmnd.8969, Art.25.

[174] op.cit. supra n.44.

[175] 5 U.S.C., s.552a (Supp.1976).

[176] Eg. Fair Credit Reporting Act 1970 (15 U.S.C.,s.1681); Right to Financial Privacy Act (12 U.S.C.,s.340); Fair Credit Billing Act (15 U.S.C., s.1666).

[177] 338 U.S.632, 652 (1950), quoted in Kevin R. Pinegar, "Privacy Protection Acts: Prvacy Protection or Economic Protectionism?", The International Business Lawyer, April 1984, pp.183-188.

[178] See *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976).

It is argued that `groups of individuals' warrant protection because invariably information about bodies and associations can often be related to individuals, in that information about a group may carry with it implications about its members, for example on matters of solvency or reputation:

> "The basic problems occur when an individual is identified or identifiable as a member of a certain group, by reason of where he or she lives or works, and receives unwanted attention in the form of solicitation..."[179].

Furthermore, people belonging to particular groups (e.g. immigrants, ethnic minorities, mentally disabled people) may sometimes need additional protection against the dissemination of information relating to that group[180]. Collective entities can also sometimes be as vulnerable as individuals, and thus should perhaps have the same right enjoyed by a natural person to correct erroneous information. A wrong or misleading credit rating can do as much harm to a trading company as to an individual.

The major problem involved in this issue is the boundary question: knowing to what extent the law should regulate an organisation's files, in order to protect the privacy of physical persons. This problem of `mixed files' applies in particular to small firms. In many European countries, financial institutions would not be willing to grant credit to small and medium-sized businesses unless some guarantee based on the personal credit of the owners or directors of the company was given. Such files would thus clearly be an indication of an individuals financial state, without being either mentioned by name in the file or by attaching an entry code. The inclusion of non-physical persons in legislation would therefore solve the problem in certain situations which:

> "...are typically characterized by the fact that data on small entities are affecting individual persons who in a specific capacity (eg. as owners or partners of a business, members of an association) are so closely related to the entity in question that virtually any information on the entity is, or contains, implicitly information on such individuals. Such data technically do not qualify as personal data because they are not directly information `on the personal or material circumstances of an identified or identifiable physical person'."[181]

---

[179] Flaherty, D., "Cumulative data are not always anonymous", p.6, Privacy Journal, 9/1985.

[180] Most national data protection legislation contains additional protection for so-called `sensitve' personal information, see Section 4.4.2 above.

[181] Hogrebe, M.E., "Legal Persons in European Data Protection Legislation: Past Experiences, Present Trends and Future Issues" (1981), at p.41; DSTI/ICCP/81.25, OECD, Paris. The citation is from the German Federal Data Protection Act, s.2(1).

In countries where small enterprises have an important economic role, there is obviously a need to formulate a flexible legal framework in order to protect an entrepreneur's privacy[182]; a person should not lose his right to privacy, simply because he is the head of a firm. Indeed, this was a major justification behind the inclusion of non-physical persons in the Norwegian Act.

The alternative viewpoint is that privacy is essentially something personal, something for which only individuals have a legitimate claim. The needs of individual protection has qualitative differences from the assurance of respect for group integrity, which is often covered by special social legislation, or corporate security, which relates more directly to commercial or property considerations. If, in fact, non-physical persons are seen as suffering from the abuse of data processing in the same way as individual persons, this should be considered separately in a detailed manner, not simply left in the abstract[183]. Hondius categorises existing legislation in two: that which solely covers the interests of individuals comes under the term `privacy protection'; while the inclusion of non-physical persons would more suitably be described as `data protection'[184]!

Obviously, the main criticisms of non-physical person protection are concerned with the economic costs involved. The majority of data transmissions would be restricted by privacy laws and it would thus slow down international business transactions and diminish the ability of companies to provide information services. This problem would be expanded if nations maintained a strict interpretation of the principle of `equivalency' with regard to transborder data flows[185]; such that trade may be restricted vis-a-vis countries which do not have an equal measure of privacy protection with regard to non-physical persons.

The major argument put forward against the inclusion of non-physical persons, is the potential disruption to, or possible loss of, standard company commercial information. A survey of multinational companies stated that many executives were concerned that the non-physical person provisions could mean notifying the company that you are starting a file on them. It would then enable the firm to gain access to the data about itself that is held by its competitor, on the

---

182 The need for a flexible test is raised in the Australian Law Reform Commission on Privacy: any data protection authority should "be entitled to pierce the corporate veil and investigate any complaint which, while in appearance one concerning a corporation, was in reality one concerning an individual", A.L.R.C. 22, (2 Vols.) Australian Government Publishing Service, Canberra 1983, p.15.

183 Grundsatze fur eine gesetzliche Regelung des Datenschutzes, p.30.

184 Hondius, op.cit. supra n.171, at p.98; see Section 4.1 above for a discussion of the problems in defining data protection.

185 See further Chapter 6, at 6.2.1.

pretext that it was checking the accuracy of the information, and thus gain a potential competitive advantage through what can be considered as legalised `industrial espionage'[186].

It would thus seem reasonable to distinguish between different types of non-physical persons, such as multinationals, individual entrepreneurs and non-profit associations, each with various information protection problems, and legislate accordingly. It has been suggested that a distinction should be made between commercial companies and private societies[187].

Despite being strongly against the extension of legislative protection to non-physical persons, even the ICC recognised that if a problem did exist for small firms that fell outside existing commercial regulations, then it could be solved by a provision within the privacy regulations, whereby the disclosure of data on `small legal persons' would be classified as similar to sensitive personal data[188]. This particular right should, however, be strictly defined, since the claim by a small company to have access to records held by a larger multinational involves political and economic considerations that are different from those which arise when privacy is considered in the human rights context.

4.5 Impact on the private sector

> "Complying with privacy laws in more than 20 countries.....is an international management issue that is part and parcel of any transfer of name-linked information between countries"[189]

This section reviews the impact that the three issues, reviewed above, has had on the use of data communications by multinationals. It is primarily based upon a review of the literature; although comments obtained from survey work carried out in the UK, Sweden and Germany[190]; as well the results and commentaries arising out of similar such studies carried out over the past two decades, are detailed.

---

[186] See Business International Report, *Transborder Data Flow: Issues, Barriers and Corporate Responses*(New York: BI, 1983); also Kuitenbrouwer, "The World Data War" (1981) 91 New Scientist, 604.

[187] Chamoux, Jean Pierre. "Data Protection in Europe: The Problem of the Physical Person and the Legal Person", p70-83, 2 Journal of Media Law and Practice 70 (1981), at p.81.

[188] International Chamber of Commerce (ICC), Policy Statement on Privacy Legislation, Data Protection and Legal Persons, adopted by the Council of the ICC in July 1984; in Transnational Data Report, vol.11, no.7, Oct/Nov 1984, p.425.

[189] Business International, op.cit. supra n.186..

[190] See Chapter 1, at 1.4.

4.5.1 International data transfers

With the emergence of data protection legislation in the early 1980s, many business commentators predicted that such regulation would have a severe impact on commercial international data flows[191]. Contrary to these fears, however, the number of publicised cases where some form of restriction has been placed on the international transfer of data by data protection authorities appear fairly few.

In France, American Express were given permission by CNIL to send transaction data to the UK for processing (before the 1984 DPA) after they were satisfied that adequate security arrangement would be established[192].

The most recent public case, concerned the transmission of certain personnel files from FIAT (France) to FIAT (Italy). CNIL required that a contract should be established between the two enterprises, stating that FIAT (Italy) would ensure that the data subjects were given the full protection provided for under the Council of Europe Convention and the French Act[193].

The issue of transborder data flow has also arisen in Germany with regard to the transfer of employee data abroad. In 1986, a case came before the Hesse State Court between the union, IG Metall, and the automotive company, GM's Adam Opel[194]. Part of the Union's case against the company was that by handing over its data processing activities to a GM subsidiary, there was a danger that some of the data could be sent abroad, therefore breaching Section 24 of the German data protection act. The Court stated that, although there was a `possibility' of an illegal export of data, it was the responsibility of the supervising authority (internally appointed `Datenschutzbeauftragter') to prevent such an occurrence becoming a `concrete reality'. Such a decision obviously considers that the powers of the supervisory authority are adequate to ensure

---

191 Eg. Coombe, G.W. & Susan L. Kirk, "Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations", pp33-66, The Business Lawyer Vol.39, No.1, November 1983; Cooper, David M., "Transborder Data Flow and the Protection of Privacy: The Harmonisation of Data Protection Law", p335-352, The Fletcher Forum, Vol.8, Prt 2, 1984; McKeaver, E.D., "Is it best not to regulate Transborder Data Flow?", pp.159-163, and Pinegar, Kevin R. "Privacy Protection Acts: Privacy Protection or Economic Protectionism?", p183-88, The International Business Lawyer, April 1984; Cole, Patrick E., "New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws.", p893-947, New York University Journal of International Law and Politics, vol.17, No.4, Summer 1985.

192 quoted in Privacy Law & Business, p.22, No.3, August 1987.

193 Déliberation no. 89-78 du 11 Juillet 1989 relative a la transmission d'informations relatives aux cadres superieurs de la societe Fiat France a la societe Fiat a Turin (Declaration ordinaire no.893.947), *reprinted in* C.N.I.L., 10e Rapport 32-34, 1989. See also Délibération no. 89-98 du 26 Septembre 1989; where health data could only be sent to Belgium in anonymous form, with provisions for French law to be applicable in Belgium. See Chapter 6, at 6.2.2.

194 quoted in Privacy Laws & Business, p.11, No.1, February 1987.

that such transfers do not occur; an extremely difficult task considering the nature of such transfers.

Concerns over this issue were raised by opposition Social Democrat Party parliamentary representatives. The German Federal Department of Labour denied such fears, stating that the export of employee data was permissible only in "exceptional cases, such as where a labour contract with a multinational corporation requires data to be reported to its international headquarters". The Department went on to state that what "further happens to the data abroad is a matter of principle outside the scope of national German law"![195]

In Norway, only one case has been turned down by the Datatilsynet, where a credit information company wanted to send its database to Sweden. The transfer went against credit-specific regulations and therefore the transfer was refused. However, foreign on-line enquires are permitted[196].

Possibly because Sweden was the first country to pass data protection legislation, it has the largest number of publicised cases involving restrictions on the transfer of data abroad. For example:

- A company was denied an application to send data to Belgium, because Belgium does not have legislation[197];
- a company was refused permission to send a tape to the UK (prior to the 1984 Act) for the printing of personal tax details[198];
- a German multinational was unable to export information on employees held on the Swedish system[199]; and
- in 1988, the Swedish Data Inspectorate refused to allow a company to send potential customer files to the United States for direct marketing purposes[200].

The Data Inspectorate has stated that it will generally give permission for the export of employee and customer data, provided that either the information "was very harmless and would be

---

[195] See Transnational Data and Communications Report, p.2, January 1988.

[196] Apenes, G., op. cit. supra n.128, at p.53.

[197] quoted in Poullet op.cit. supra n.124 at p.33.

[198] quoted in US Report "International Information Flow: Forging a new framework", 32nd Report by the Committee on Government Operations, No.96-1535, at p18 (96th Congress, 2nd Session, House Report 1980).

[199] Questionnaire returned from Hans-Ludwig Drews, Datenschutzbeauftragter der Siemens AG.

[200] Interview with Datainspektionen, 1989.

processed exclusively within the organisation or with the express consent of the individual"[201]. In the area of direct marketing, the Data Inspectorate has a very "restrictive attitude" to the export of data, and has given its permission in only one case[202]. Pharmaceutical data can only be exported where it is either made anonymous, or express consent has been given.

A general study of the data protection legislation in the Nordic countries has concluded that, in relation to data related to the export of goods, "...serious problems are unlikely to arise in connection with the Nordic legislation when paper-less practices are pursued in international trade"[203].

Since the UK Act was passed, there has only been one instance where the Registrar has issued a transfer prohibition notice. The case involved the sending of personal data to the US for direct mail purposes back into the UK. The US operation was, at the time of the request, involved in a legal action with the US Postal Service attempting to restrict the company's actions on the grounds of fraud and misleading promotions. The Registrar felt, in the circumstances, that such a transfer would likely lead to a breach of three of the Data Protection Principles which form the basis of the Act[204].

One of the reasons for the relatively small number of examples is likely to be because personal data (ie. name-linked) currently accounts for only a small percentage of international data transfers. It has been estimated that only 2-5% of international data transfers contain personal data[205]; including mailing list data, for both prospective and current customers, and company personnel information. The former types of data may be the subject of commercial trade, while the latter will tend to be intra-company transfers. The examples and comments from data protection authorities suggest that they are more concerned with commercially traded data transfers to a third-party company, than intra-company transfers, since the former transfers are perceived as being less easily controlled[206].

---

201 Wahlstrom, S., op.cit. supra n.131 at p55.

202 Ibid., at p.56. The case involved the processing, in Ireland, of marketing data on persons in certain job positions.

203 UN/ECE, TRADE/WP.4/R.99.

204 The Seventh Report of the Data Protection Registrar, p.33-34, June 1981, HMSO.

205 Briat, M., "Personal data and the free flow of information", p47, Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988. This figure would obviously be significantly higher in those countries which extend data protection legislation to cover legal persons.

206 Interviews with the data protection authorities in the UK, Sweden and Germany; as well as papers presented at the International Data Protection Commissioners Conference, Paris 1990, from Finland, Denmark, Sweden and Norway.

It could be expected that the amount of personal data being transferred internationally, for both internal and external purposes, would increase as companies send an increasing range of documents and messages via their communications networks. How much of this data will be `purely commercial', not referable to any identified or identifiable legal or natural individual? The number of examples of restrictions can therefore be expected to rise.

Alternatively, it is also possible that companies have been dissuaded from implementing IT solutions involving the international transfer of personal data, at least commercially, due to the existence of data protection legislation. Such a conclusion would not seem to be borne out, however, in the survey, where companies rarely stated data protection legislation as an restriction either experienced or expected in the future; concerns centred firmly on restrictions concerning the means of communication[207].

In terms of data processing, companies that are concerned about, or are subject to, restrictions arising out of national data protection legislation will need to establish the necessary data processing facilities in the home country[208]; for example, Grace, the multinational chemical company, stated that, although they centrally processed much of their corporate data, payroll and personnel data was always processed separately in the home country due to data protection legislation[209].
Although the need to carry out data processing in the home country may be viewed as inefficient in terms of the corporate global strategy for the organisation of IT, in terms of technical costs, there is a significant downward trend in the costs of data storage which makes any such duplication of facilities increasingly reasonable[210].

Another source of explanation for the few case examples is obviously based on the activities of the data protection authorities. Data protection authorities have, to date, generally avoided the strict use of their legislative powers, preferring to work in conjunction with the private sector to achieve workable solutions. The vast majority of negotiated solutions do not tend to be publicised, except where they are intended to serve as examples of how solutions can be achieved, such as in the FIAT case.

---

[207] See Chapter 3, at 3.3. above.

[208] Companies also establish dual processing facilities to overcome TDF restrictions; however, these are usually due to 'domestic-processing' regulations, rather than data protection legislation, see Chapter 3, at 3.5.1.

[209] Interview with R.S. Barratt, I.S. Manager, W.R. Grace Ltd.: 16/07/88.

[210] Kane, M.J. and D.A. Ricks, "The Impact of Transborder Data Flow Regulation on Large United States-Based Corporations", p28, The Columbia Journal of World Business, Vol.XXiV, No.2, 1989.

From the cases that exist, where the transborder flow of data has been restricted by the relevant data protection authority, it would seem that the authorities are not particularly concerned whether the country in question has ratified the Convention or Guidelines, or not; rather the case revolves around issues such as the perceived sensitivity of the data; the security arrangements and purpose.

Overall, it has been concluded, in a survey carried in 1989 on behalf of the Council of Europe's Consultative Committee on data protection, that:

> "The information supplied by the contracting parties tends to lead one to believe that there are no major problems posed by transborder data flows between and among them or at least no major problems have arisen so far."[211]

Certain multinational companies have also been proactive in dealing with the threat of data protection restrictions, by implementing world-wide company policies with regard to the handling of personal data. This was a course of action carried out by four of the companies surveyed: IBM, Standard Chartered, Bank of America and Dun and Bradstreet. The US companies have been particularly keen on this approach, because of concern over the lack of data protection legislation in the US private sector[212].

It must also be true that the well-publicised fears of companies, with regard to the potential for data protection legislation to restrict international data flows, were vastly exaggerated, possibly deliberately, when trying to lobby against such legislation. Certainly, in the case of the current UK government, if implementation of the 1984 Act had been found to severely restrict international business, then the Act would likely have already been amended.

Finally, it should be noted that, bearing in mind the impossibility of data protection authorities, effectively monitoring the international transfer of data, companies may have chosen to ignore the provisions of national legislation, and have transferred data as and when required. Such a conclusion, although not explicitly admitted to by any survey respondent, was often noted by the respondent as a straightforward possibility!

---

211 Observations on the replies submitted by the Contracting Parties in accordance with the decision taken by the Consultative Committee in application of Article 19(a) of the Data Protection Convention. Secretariat Memorandum prepared by the Directorate of Legal Affairs, Strasbourg 3 April 1989, para.7.

212 See also the Business International study, op.cit. supra n.186, at p.128; which also states that US companies have been particularly vulnerable to data protection legislation because of the more centralised nature of their data processing operations.

4.5.2 **Data Security**

In certain countries, data protection legislation has encouraged data users to focus their attention on the importance of adequate data security, and therefore devote greater resources. One survey has noted that, in Germany, data security was considered by data users to be the most pressing issue of the next 5 years; while, in the UK, only 7% of respondents stated they had altered their security policies as a result of the Act.[213].

In the survey carried out by the author, around half of those companies interviewed stated that their data security policy had not been altered due to data protection legislation, since they felt that existing standards were already considerably stricter than that required by the legislation; this was particularly noted by the respondents in the banking industry[214]:

> "The Bank has always maintained rigid controls over all of its records due to the sensitivity of the data held"

The other half of the respondents, those that felt that data protection legislation had had an impact on their data security, noted two main forms of influence:

- As a means of raising awareness of data security issues within the company, particularly as a means of obtaining additional resources from management[215];

- moved the focus of data security to the issue of protecting the ever burgeoning number of office PCs[216].

In contrast, data protection concerns have also prevented the adoption of certain data security techniques. The German airline, Lufthansa, wanted to put a magnetic strip on employee ID cards, in order to enhance their data security (eg. access controls); however, the trades unions prevented such a development since it was claimed that it would enable the employer to create a personal profile of the activities of employees[217].

---

[213] See the Manchester survey, op.cit. supra n.124; quoted in Walden, I., "Companies face problems with registration but not international data flows", p14, Privacy Laws & Business, no.4, November 1987.

[214] Response from Dennis Arnum, Vice-President, Bank of America.

[215] Eg. stated by Trefor Hogg, Information Centre Manager, Dun & Bradstreet.

[216] Eg. stated by Roger Grimshaw, Corporate Projects Manager, Readers Digest Association Ltd.

[217] Interview with Dieter Hermsdorf, Data Protection Officer, Deutsche Lufthansa AG; 06/04/89.

Most of the security measures implemented under data protection legislation should generally tie in closely with the data security requirements of the data users themselves:

> "The security of processing personal data is an obligation arising from the Federal Data Protection Act; the security of non-personal company data and of the processing of such data lies in the interests of economical and disturbance-free business operations"[218]

4.5.3 Legal persons

A survey conducted in the United Kingdom, before the Lindop Report, showed that among small and medium sized businesses there was a certain agreement that some protection of business files should exist[219]. On the other hand, an alternative survey of multinational companies throughout the Western industrialised nations, found unanimous feelings against data protection laws covering non-physical persons[220].

Such a divergence in views, between whether a company is in favour of protection for legal persons or fears such regulations, could be largely dependent on their size and market position. Indeed, when the EEC considered the question of protecting non-physical persons, it extended the argument in favour of protection for small businesses by stating that a failure might put small businesses at a disadvantage vis-a-vis large multinationals, since it is the large companies that have a greater interest in monitoring the progress of competitors[221].

There seems to be only two publicised situations that has involved the question of non-physical persons, on which to consider any precedents for how the question of maintaining the secrecy of commercial information may be dealt with by national data protection authorities. Both cases arose in Norway:

- IBM claimed that if customers and competitors gained access to IBM's files its marketing activities would be damaged, and thus it decided to apply for an exemption from the non-physical requirements of the Norwegian law. On February 18th 1983, Norway's Data

---

218 Deutsche Lufthansa AG, `Data Protection (Privacy) and Data Security Instruction Sheet', p3.

219 quoted in Chamoux, op.cit. supra n.187, at p.72.

220 Business International, op.cit. supra n.186, at p.108.This position was also borne out by all the respondents to the author's survey.

221 The `Bayerl' Report, op.cit. supra n.44. It would also seem true that "it is always the big who keep files on the small, and not the other way round", quoted in Chamoux, op.cit. supra n.187, at p.76.

Inspectorate granted IBM an exemption concerning access, though the inspectorate retained the right to intervene and maintain the law if a complaint was received. Such a situation, if carried through for all major companies, would seem to provide potential administrative solution between the desires of small firms for some level of privacy protection, and the multinationals demand for confidential commercial information.

- A market research company had collected data concerning the numbers of computers used in 5000 Norwegian companies. The company wanted to sell the information to computer hardware/software suppliers. The Data Inspectorate decided that use of the information contained in the database would mean revealing company confidential information and would endanger their data security[222].

Despite this lack of examples, the problem remains an important one. If a company intends to set up data communications with a company based in one of the six current jurisdictions which currently protect the use of data concerning commercial entities, then it will have significantly increased responsibilities with regard to ensuring legal compliance and legal security.

4.6 Developments in data protection

4.6.1 Technological developments

When the first national data protection legislation was passed in Sweden, in 1973, the major privacy fears were generated through the use of large mainframe computers. However, the rapid growth of micro-computers has altered the focus of concern. The ability of smaller machines to process larger amounts of information is a trend which seems set to continue in the foreseeable future.

Such rapid technological change makes legal regulation in this field potentially obsolete, and inevitably leads to criticism from both data users and data subjects. The former fear that regulation may serve to curb the development and use of new technologies. The latter warn that the new technologies create threats to personal privacy not covered by legislation. One solution to the problem of legislation becoming technologically obsolescent has been to include within the

[222] quoted in Privacy Laws & Business, p.6, No.9, February 1989.

corpus of the statute a time limit for revision of the act. Such an approach has been adopted within the data protection legislation of Canada[223] and Iceland[224].

The Council of Europe Committee of experts on data protection has published a document that considers the challenges that new technologies present for the protection of personal data, and in particular, whether the principles laid down in the Convention remain adequate as a basis for protection[225].

`Electronic tracing' is an example of a concern that has originated in the development and increased use of telematic services[226]. In this situation, `confidential' or `sensitive' personal data arises not from the level of detail of information which is stored in a database, but from the personal data that arises through the use of a service; such as monitoring a person's use of ATMs to determine spending patterns. Such large databases allow the possibility of constructing a `profile' of every user, or group of users, of a particular service[227].

The fear of `electronic tracing' has not sprung simply from the possibilities inherent in the technology, but also the developments within the European Community to remove border controls, which, it has been suggested, will "be compensated by increased use of surveillance based on electronic traces"[228].

Changing technologies would also seem to make it necessary to distinguish the idea of data files from that of the processing location. The growth of the computer network has given rise to the need for a reconsideration of legislative terminology; for example, possibly moving from the traditional data protection concept of the `controller of the file'[229], which is now considered "an obsolete concept"[230], to that of `controller of the network'. The role of the latter person would be

---

223 Canada, op.cit. supra n.3, at s.75(1) & (2). Parliament has the right to establish a committee to review the Act after a three-year period.

224 Iceland, op.cit. supra n.157, at Article 31. A three-year period.

225 "New Technologies: a challenge to privacy protection?", Council of Europe, Strasbourg 1989; also The Computer Law and Security Report, p.19-20, Vol.5, No.3, 1989. Recently, Professor Spiros Simitis, Chairman of the EC member states' Data Protection Commissioners' working group, at the 13th Data Protection Commissioners' Conference in Strasbourg, October 1991 (quoted in Privacy Laws & Business, p.1, No.19, December 1991); stated that the Council of Europe Convention "is not an adequate basis for policy now".

226 Ibid., at p.7. `Telemetry' was defined as "The remote collection of personal data by automatic means, where the data subject plays no active part in the actual process of the collection of data".

227 See Bing, op.cit. supra n.90; and Flaherty, op.cit. supra n.179.

228 Bing, ibid., at p.168. An example of this is the `Schengen Agreement', of 14 June 1985, between France The Netherlands, Belgium, Luxembourg and Germany. Under the agreement, a comprehensive data exchange system for the police authorities is to be established (based in Strasbourg) to compensate for the loss of border controls.

229 The Convention, op.cit. supra n.5, at Article 2(d): the body "who is competent...to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them".

230 Comment made by Professor Spiros Simitis, op.cit. supra n.225.

to take responsibility for all the personal data held on a data subject throughout the network[231]. However, the change would require that a legal distinction be made between the obligations and responsibilities of the `network controller' and other relevant parties, such as the network provider[232].

Also, with regard to the growth of international networks, the aim of achieving `transparency' for data subjects[233] can become significantly more difficult, as increased numbers of persons have access to the data.

In the US, a new privacy/data protection issue has arisen over the use of electronic mail systems, as a part of a company's data communications strategy. Two cases are currently being pursued against Epson and Nissan[234]; both companies are being accused of infringing employee privacy by monitoring the content of Email messages being sent and received by employees.

This raises important questions regarding the private use of company facilities. Most companies usually allow, or at least overlook, a certain use of the office telephone for private calls. In addition, the use of EMail systems is often encouraged in companies as a replacement means of communications. Companies, however, are also concerned to protect commercial trade secrets from being released, particularly when the Email system is connected to a public Email service. The status of Email messages, in the absence of legislation, need to be considered by companies, and employee guidelines should be drafted to publicise the company's position.

4.6.2 Differentiation and Self-Regulation

Over the past two years, there has emerged a `second generation' of data protection legislation within Western Europe[235]. This legislation, in the Netherlands, Switzerland and Ireland, exhibits a number of characteristics that differentiate them from countries that passed legislation in the 1970's, such as Sweden, France and Austria, although even these countries are amending their legislation in the same direction. There is a trend towards simplification; the increased use of informal and civil sanctions as a means of enforcing data protection; a greater amount of

---

231 Council of Europe Report, op.cit. supra n.225, at p.34.

232 See further Chapter 6, at 6.5.

233 See section 4.2. above.

234 See Applied Computer and Communications Law, Vol.7, No.8, 1990, at p.1-2; and Vol.8, No.2, 1991, at p.2.

235 With `first generation' data protection legislation, the focus was determined by the nature of the personal data, from trivial to sensitive; see Bing, op.cit. supra n.90.

regulatory differentiation for different sectors of data users, and a trend in favour of self-regulation[236].

The need for simplification has arisen in the face of the bureaucracy that implementation of data protection legislation has created, and the corresponding costs involved both for data users and the regulatory authorities themselves. One UK company, highly dependant on personal data has stated that implementation of the Act has cost it in the order of £200,000[237]. The UK Data Protection Registrar has already recognised that the registration requirement is not necessarily the most practical way of informing data subjects about how their personal data is to be used and has suggested that "it is sensible to seek to achieve more restricted objectives" for registration[238].

Few cases of criminal prosecutions under data protection legislation have occurred in Western Europe[239], and it would seem that data protection authorities tend to rely on informal and civil sanctions against offending data users. Informal sanctions generally involve an investigation by the authority, with the threat of publicity as the incentive for data users to remedy the identified problem areas[240].

The trend toward differentiation, the sectoral approach, of data protection rules has been a result of the ageing and experience of existing legislation. Such a process of differentiation enables both an increased level of protection for data subjects; as well as tailoring the legislation to fit in more suitably with the conditions within particular industries, and thus prevent the creation of unnecessary and unsuitable bureaucratic requirements. Divisions into sectors has occurred along such lines as the sensitivity of the data, and the purpose of the data. The Council of Europe has set up a number of sectoral working parties to draw up regulations for different categories of data users, already producing recommendations in areas such as direct marketing and medical data banks.

---

[236] See Dresner, S., "New Style Data Protection Laws: Convergence or Radical Change?", Proceedings of `Data Protection in Ireland, The Netherlands and Switzerland' Conference, 19 October, London, 1988; and Flaherty, D.H., "Towards the year 2000: The Emergence of Surveillance Societies in the Western World".

[237] Interview with Reader's Digest, 1989.

[238] The Fifth Report of the Data Protection Registrar, p.79, June 1989, HMSO.

[239] Eg. in the UK, only 70 organisations have been prosecuted; the majority of these have been for Section 5(1) `non-registration' offences. See Gaskill, S., "Data Protection: Recent Developments", paper presented at Data Security and the Law Conference, London, 8 May, 1991.

[240] See Flaherty, D.H., *Protecting Privacy in Surveillance Societies*,p.385-397, The University of North Carolina Press 1989.

Related to the greater differentiation of data protection rules is the trend towards self-regulation. Sectors of data users are drafting quasi-legal, enforceable codes of practice on data protection. Indeed, in some countries, such as Japan, voluntary codes of practice are the only form of private-sector data protection regulation[241].

In the UK, the Lindop Committee Report[242] concluded that codes of practice would be the most suitable and flexible means by which the data protection principles could be adapted to the reality of data processing practices in individual industries. The Report recommended that the drafting of such sectoral codes of practice should be the primary task of the data protection authority, in consultation with the appropriate industry organisations. The codes would then be submitted as statutory instruments, having the full force of law. Failure to abide by the code would be a criminal offence. However, the Government's White Paper[243] felt that giving the codes statutory force would not be practicable in a reasonable time frame; therefore the Registrar would simply be under a duty to encourage the drafting of such codes[244].

Under the Netherlands Act, the private sector is strongly encouraged to establish codes of conduct. After a certain period of time, in the absence of a satisfactory code, there then exists the ability to issue general administrative orders statutorily imposing codes of conduct[245].

4.7 Comment

> "..the vast information flows associated with network interconnection will inevitably lead to regulatory conflict if supervision of transborder data flows is attempted without a coherent international framework."[246]

Data protection legislation gained a significant profile during the late 1970s and early 1980s, as companies voiced their fears that the spread of data protection laws would act as an obstacle to the use of international data communication technologies[247]. Indeed, in the UK, for example,

---

241 Eg. `Guidelines on the Protection of Personal Data for Financial Institutions', published in 1988 by the Centre for Financial Industry Information Systems (FISC), Tokyo; see also Yamashita, "Protecting personal data in the private sector", 78 Japan Computer Quarterly, 30,31; and Horibe, Professor M., "Japan encourages compliance with privacy principles", p11-12, Privacy Laws & Business, No.13, 1990.

242 See the Lindop Report, op.cit. supra n.9, at para.19.24.

243 White Paper, `Data Protection: The Government's Proposals for Legislation', p4, Cmnd No.8539 (1982).

244 The DPA'84, op.cit. supra n.61, at s.36(4). The first such codes to be issued were by the Advertising Association and the Association of Brtish Travel Agents.

245 The Netherlands, op.cit. supra n.95, at s.16(1).

246 Reidenberg, op.cit. supra n.82, at p.34.

247 See section 4.5.1. above, at fn.191.

much was written about how the potential restrictions could deter the adoption of IT altogether! A review of the literature, and the results from various studies, would suggest that such fears were generally unfounded.

The multinationals, surveyed, nearly all reported that the use of data communications had resulted in new business opportunities; while no respondent stated that data protection controls had either resulted in the loss of such opportunities, or had been experienced to a significant degree at all.

Recently, however, the draft European data protection directive has given new life to the debate. The need for such a European Community initiative is itself controversial[248]; however, whatever the specific outcome is, it is unlikely that companies will need to see data protection legislation as a sufficient obstacle to the adoption of data communication technologies. However, data communication strategies need to take account of data protection requirements, when trading within Europe, both with regard to their internal procedures and in any contractual agreements[249].

The data security provisions, contained in all European national legislation, are of a vague enough nature, not to be either unnecessary or restrictive upon companies. Rather, data security managers need to use the existence of such provisions to encourage a greater priority and increased resources for general data security issues, from board level.

The European draft directive does not extend to `legal' person data, and to that extent, the debate in this area is currently quiet. However, the continued existence of `legal person' provisions in a number of national legislations could have a significant impact on commercial data flows.

The most significant current issue in the field of data protection, concerns how companies, particularly when either based in, or trading with, countries such as the United States, can achieve an international functional equivalency of protection, in the absence national legislation. If such equivalency is not possible, except in statutory form, then potential problems will continue to exist for international data flows in the foreseeable future.

---

248 See ICC "Protection of Personal Data: An International Business View", Doc. No.373/124, 1 August, 1991.

249 See Chapter 6, at 6.2.

Chapter 5 **COMMERCIAL LAW FRAMEWORK**

5.1 The Paper Environment

- 5.1.1 The legal nature of communications
- 5.1.2 Statutory requirements
  - 5.1.2.1 Document
  - 5.1.2.2 'Writing'
  - 5.1.2.3 Signature
  - 5.1.2.4 Contract Formation
  - 5.1.2.5 Negotiability
  - 5.1.2.6 International trade law
  - 5.1.2.7 Comment

5.2 Evidential Issues

- 5.2.1 Record maintenance
- 5.2.2 Admissibility
- 5.2.3 Integrity and Authentication
- 5.2.4 Comment

5.1 THE PAPER ENVIRONMENT

This Chapter is concerned with the obstacles that exist in the current commercial-legal framework to the replacement of paper documentation with electronic messages.

In Chapter 4, consideration was given to legislation that had been passed to deal with a specific aspect of the developing information revolution. However, many of the restrictions imposed on the use of data communications are due to the lag that exists between the emergence of new technologies and the ability of the law to change to account for such new methods: negative restrictions.

Legislative requirements for paper documentation could make reliance on data communications either legally unacceptable, or legally insecure; while evidential requirements and uncertainties regarding a paper back-up can negate some of the benefits of adopting electronic messaging. In order to facilitate the use of data communications, it is therefore necessary to assess the extent to which electronic messages can fulfil the traditional legal roles demanded of paper-based communications.

In the long term, such facilitation will require legislative amendment, however, the political profile of such issues would not seem to be sufficient to have an impact in the short to medium term. This lack of profile means businesses will have to have greater reliance on international organisations to bring about the necessary awareness.

5.1.1 The legal nature of communications

In order to analyse the nature of the legal requirements that exist in the current paper environment, it is initially useful to categorise the different forms of legal significance that commercial communications can possess[1]:

> "..what the lawyer focuses on is what the communication actually does - the transaction - as the communication itself is merely a means of effecting that transaction"[2].

(a) Communications with non-contractual significance: this category covers the vast majority of communications, such as statistical data. The only legal aspect of such communications are that the sender maybe liable for the accuracy of the information[3].

(b) Communications with contractual significance: these forms of communication evidence the formation of a contract, such as a purchase order. In an paper environment, such documents will often include additional information critical to the contract, such as the sender's standard terms and conditions of trading.

(c) Communications which transfer ownership or certain legal rights: ie. where physical possession of a document invests the holder with certain legal rights. The bill of lading and the bill of exchange are two primary examples in English law. With the bill of lading, transfer of the paper document represents the legal transfer of title to the goods; whereas a bill of exchange enables a transferable deferred payment obligation to arise[4].

(d) Communications that are required for regulatory purposes:

---

[1] See Goode R. & Bergsten E., "Legal questions and problems to be overcome", pp131-133, in Thomsen, H.B., & B.S. Wheble, *Trading with EDI: The Legal Issues*, IBC Financial Books 1989; and Reed, C., "EDI - contractual and liability issues", p.36-41, Computer Law & Practice, Vol.6, No.2, 1989; and Seipel, P., "Paper laws in transition", pp.99-134, in Seipel, Prof. P. (ed.), *From Data Protection to Knowledge Machines*, No.5 Computer/Law Series, Kluwer/The Netherlands 1990.

[2] Reed, C., *Electronic Finance Law*, p.132, Woodhead Faulkner, 1991.

[3] *Hedley Byrne & Co. Ltd. v Heller & Partners Ltd.* [1964] A.C. 465, H.L.

[4] See generally, Reed, op.cit. supra n.2, at p.132-144.

"a great number of rules which concern the treatment of data belong to administrative law: they provide for various declarations, authorizations, and controls by administrative authorities"[5]

These include submissions of information to the taxation authorities, such as the VAT Commissioners, and Customs authorities for international trade. An increasingly important area is the submission of data to the European Community[6].

(e) Communications that require prior legal authority, or licence: For example, as mentioned in Chapter 4.2, some national data protection legislation requires data users to obtain approval from the data protection authority before sending data internationally[7]. While in certain legal jurisdictions, the sending of encrypted data requires a licence[8].

It can seen that, in order for data communications to be used by business to replace paper-based communications, it is necessary for electronic messages to replicate the three basic functions of paper documentation: an informative function, an evidential function[9] and a symbolic function[10]. It is within the last two functions that potential unique legal issues can arise.

The symbolic function of paper documents raises the most difficult legal issues for data communications, since the nature of negotiable documents, such as a bill of lading, requires that there exists a unique `original' document upon which the parties can rely. While the nature of computer technology mitigates against `originality' in a documentary form.

5.1.2 Statutory requirements

"...though technical means exist to move trade data by automatic transmission instead of traditional paper documents, the use of such means depends on the legal force given to the information thus transmitted."[11]

---

[5] Hanotiau, Bernard, "The transborder flow of data - applicable law and settlement of disputes", p.175-197, in ICC, *International contracts for sale of information services*, ICC/Paris 1988.

[6] See, for example, Sarson, R., "1993 and the VAT information exchange", p.8-11, Electronic Trader, Vol.II, No.IV, February 1992.

[7] Eg. Austrian Data Protection Act 1987.

[8] Eg. In France, the national PTT regulates the import, manufacture, use and export of any encryption technique. A licence has to be obtained by both the supplier and the user. See Chapter 3, at 3.3.4.

[9] See section 5.2. below.

[10] See Henriksen, R., "Signature and Evidence in the international trade and transport society without documents", p.44-101, in NORDIPRO, *Legal Acceptance of International Trade Data Transmitted by Electronic Means*, Special Paper No.3, CompLex no. 10/83, Universitetsforlaget 1983.

[11] Bergsten, Eric, "Paperless Systems: The Legal Issues", p.23-26, The Computer Law and Security Report, Vol.3, No.6, 1988.

Following on from the consideration of the legal nature of communications, this section reviews the range of traditional legal terminology and practice that are commonly recognised in a legislative framework based within a paper environment.

Throughout all national legal jurisdictions, there are requirements as to documentary form. Such requirements can create obstacles to the use of data communications in traditional commercial relationships: For example:

- The English Bills of Exchange Act 1882, requires "an unconditional order in writing, addressed by one person to another signed by the person giving it.."[12];

- the Law of Property (Miscellaneous Provisions) Act 1989, s.2(1) states that "A contract for the sale or other disposition of an interest in land can only be made in writing and only by incorporating all the terms which the parties have expressly agreed in one document..";

- the Marine Insurance Act 1906, ss.22-24, states that an insurance policy must be `signed' by the insurer[13];

- the US Statute of Frauds states that "....a contract for the sale of goods for a price of $500 or more is not enforceable by way of action or defence unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought..."[14];

- and, under Danish law, there is no general requirement for an invoice to be in a certain form, although the information that is evidenced by the invoice will be taken into account, according to tax and accounting rules, only if a paper original or certified copy of the paper original is kept[15].

---

[12] Bills of Exchange Act 1882, at s.1. In the 1989 `Banking Services: Law and Practice' Report by the Review Committee [known as the `Jack Report', after its chairman, Professor R.B. Jack], Cm 622, Recommendation 7(8) called for an amendment to s.45 of the Bills of Exchange Act 1882 to allow banks "to allow payment by presentation of electronic information rather than the instrument itself".

[13] The term "marine insurance" covers all kinds of risk arising out of transport, by sea, land or air (except private motor insurance).

[14] UCC § 2-201(2). This is an absolute defense for a party to the contract, in the event of a dispute. All US States, except Louisiana, have adopted this clause. In the UK, a similar statute of frauds existed from 1604 until its repeal in 1954. A similar provision exists at 31 U.S.C. § 1501, for contractual obligations established with the US Government; however, see Decision of the Comptroller General of the United States: `Use of Electronic Data Interchange Technology to Create Valid Obligations', B-245714, December 13, 1991.

[15] See *The Legal Position of the Member States with respect to Electronic Data Interchange*, TEDIS final report, September 1989.

With such requirements, consideration needs to be given to whether the existing terminology can, or is likely to be interpreted widely enough to encompass electronic alternatives; or whether, until the provisions are amended, companies are unable to remove the paper component. Where uncertainty exists, companies then need to consider what contractual means may be adopted to establish `commercially-acceptable' legal certainty.[16]

5.1.2.1 Document

> "There is a document whenever there is writing or printing capable of being read, no matter what the material may be upon which it is impressed or inscribed"[17]

The concept of a `document' is very firmly based within an evidential context, where documents, such as bills of lading, are presented as a necessary precondition for a subsequent event occurring, such as the release of the goods. In addition, such documentary presentation is, as the above quote states, also a common part of the evidential procedure in court, particularly in the requirement for an `original' document[18].

Within administrative law, documents are required to be submitted to governmental authorities to provide certain types of information or maintained to satisfy statutory requirements. The range of documents that are required by the various (quasi-) governmental authorities can be vast, such as health certificates and certificates of origin.

Under UK law, for example, an `invoice' is given legal status under VAT regulations. VAT regulations require that there exists a unique invoice[19]. Therefore, the sending of an electronic `copy invoice' to a third party[20], via a data network or magnetic tape, might have to be distinguished from the original sent to the Customer, at some point during invoice generation within the sender's accounting system. Current electronic invoices, in the major EDI message standards, do not seem to provide a means by which to distinguish a message as a `copy', except through the use of `free-text' segments, which would require manual

---

[16] See further Chapter 6, at 6.3.

[17] *R v Daye* (1908) 77 LJKB 659 at 661. In *Huddleston and another v Control Risks Information Services Ltd.* [1987] 2 All ER 1035, in relation to evidential discovery, Justice Hoffman stated: "It seems to me that a written instrument oe other object carrying information such as a photograph, tape recording or computer disk can be....a `document'". In *Derby & Co Ltd and others v Weldon and others (No.9)* [1991] 2 All ER 901, it was stated by Vinelott, J., in relation to a computerised database, that "..the database so far as it contains information capable of being retrieved and converted into readable form, is a document within the meaning of RSC Ord. 24 of which discovery must be given...", at 902. In *Alliance & Leicester Building Society v Ghahremani & Others* (ChD NLJ 6 March p.313; The Independent 9 March) the definition of `document' was not restricted to visible writing on paper but included information stored in the hard disc, while the word `page' was defined to include a computer screen. See also the proposal to define an electronic document; UNCITRAL report `Legal Aspects of Electronic Data Interchange', TRADE/WP.4/R.649.

[18] See also ICC's UCP, 5th Edition, 1983, Doc. No.400, at Article 22(c) for a commercial definition of an `original document'. The legal value of an `original' document is obviously different depending on the context in which it is used; eg. between a buyer and seller, as opposed to the same document submitted to a third party for information.

[19] See VAT (General) Regulations 1985 (S.I. 85, 886), at para. 12-13.

[20] Eg. under a factoring agreement, companies send a copy invoice to the factor as evidence of an assignment debt.

intervention by the recipient. The requirement for a `unique invoice' arises because the VAT Commissioners are concerned to avoid fraud through the submission of dual tax returns[21].

Administrative documentary requirements are usually contained within detailed regulations (secondary legislation), which can be amended more easily and/or interpreted more widely, than primary legislative requirements. Over the past decade, various international organisations have made recommendations to member governments to review such administrative requirements[22], and in some cases, national legislation has been amended[23].

Obviously, to allow for such submissions to be made electronically will require not only changes in the terminology of certain regulations, but also the installation of the necessary equipment to receive such computer-readable data. The elimination of the documentary requirements that impede the use of data communications "has at least as much to do with administrative concerns as with legal concerns"[24].

The Customs and Excise authority has been one of the leading regulatory bodies to encourage the adoption of electronic forms of documentary submission, primarily driven by a recognition that such methods can create great efficiencies in their operations, enabling them to free up resources to focus on fulfilling their investigative functions[25].

Under commercial law, documents are a legislative requirement in particular forms of contracts, such as the sale of land and consumer credit transactions, the purpose of such requirements is usually to clarify to the parties the exact nature of the contract being formed and to protect consumers[26].

In the data communications environment, it has been suggested that resolution of the legal requirement for a document, as an obstacle, can be achieved in two ways:

---

[21] This reasoning should not apply to the `copy invoice', since the invoice is addressed to the user and thus can not be submitted by a third party. Such an opinion has been presented to the VAT authorities and has met with approval.

[22] See Section 5.4.1. below.

[23] Eg. French Tax Law was recently amended: Loi de finances rectificative pour 1990 (No.90-1169 du 29 décembre 1990), Journal Officiel du 30 décembre 1990 on 31st December 1991: Article 47 defines an electronically transmitted invoice as an `original' document for tax purposes.

[24] Bergsten, op.cit. supra n.11.

[25] See IDEA survey, `EDI and Customs around the world', December 1991; Freeman, R.C., "Legal aspects of computerised procedures for Customs administrations", p.28-42, Proceedings of CELIM Conference, `Paperless Trading and the Law in the EEC', 17-18 March, Brussels, 1986 and Morrin, J., "Customs requirements and international trade", p.42-45, Computer Law and Practice, Vol.6, No.2, Nov.-Dec., 1989. Within the European Commission, the Caddia and CD projects are encourgaing the adoption of electronic systems by national authorities; see Thomsen, op.cit. supra n.1, at p.90-91.

[26] Lindberg, Agne, Electronic Documents and Electronic Signatures, p.10, IRI Papers: The Institute of Legal Informatics, University of Stockholm, Sweden.

(a) Acceptance that electronic messages "are not documents, even electronic documents, the characteristic of which should be that they are necessarily readable by persons"[27]; and therefore seek the removal of unnecessary documentary requirements in law; and/or

(b) redefine the legislative definition of `document' to cover electronic alternatives, such as in the UK Civil Evidence Act 1968: `document' includes..."any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced...".[28] The International Standards Organisation (ISO) defines a document as "a data carrier and the data recorded on it, that is generally permanent and that can be read by man or machine"[29].

5.1.2.2 `Writing'

Can an electronic message be considered a `writing'?

In a 1990 UNCITRAL report[30], it was noted that requirements for information to be `in writing' had arisen for four main reasons:

- to reduce disputes;
- to make the parties aware of the consequences[31];
- to enable third party reliance,
- and to facilitate tax, accounting and regulatory purposes[32].

In addition, recent legislative concerns have re-asserted the concept. Public authority procurement contracts, for example, is an area which has been the subject of significant legislative activity in recent years, particularly from the European Community, in an attempt

---

[27] Troye, A., "The European Dimension: Particular legal requirements to consider when trading throughout Europe", paper presented at EDI'90, London, Oct. 30-Nov. 1, 1990.

[28] CEA, at s.10(1). See also the Finance Act 1985, s.10(5)&(6). The Taxes Management Act 1970, at s.20D(3), defines a `document' to include "books, accounts and other documents or records whatsoever". However, it also states that "copies of documents may be delivered instead of the originals; but - (a) the copies must be photographic or otherwise by way of facsimile; and (b) if so required by the inspector....the originals must be made available for inspection..." [s.20B(4)]! In Italy, the legislative definition of an `adminstrative document' was recently redefined to remove administrative restrictions on the use of electronic means to fulfil statutoy requirements for information: "Any graphic, film, electromagnetic or any other kind of representation of the contents of documents.." [Law No.241 of 7 August 1990 in Article 22].

[29] ISO DP 6760. A data carrier is "a data medium that is designed for storage and/or transportation of data".

[30] `Electronic data Interchange: Preliminary study of legal issues related to the formation of contracts by electronic means', A/CN.9/333, 18 May. 1990.

[31] This is seen, in most European countries, to be particularly important in consumer contracts; see TEDIS final report, op.cit. supra n.15.

[32] Ibid., at p.5.

to open up competition[33]. However, the processes established to ensure such legislation is complied with, has meant the re-assertion of the concept of `written' contracts.

Under the Interpretation Act 1978, "`writing' includes typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form"[34]. There is an issue to be decided, therefore, whether the recording and transmission of electronic impulses within a data communication system falls within this definition; the crucial question would seem to be whether an electronic message is considered to be in `visible form'[35]. It does, however, seem unlikely that the courts would be prepared to accept that a literal interpretation of this definition extends to electronic messages.

An alternative definition of `writing' is provided under Section 178 of the Copyright Designs and Patents Act 1988, which defines `writing' as "any form of notation or code, whether by hand or otherwise and regardless of the method by which, or medium in or on which, it is recorded"[36]. Such an expansive definition would surely include electronic messaging; indeed, it would seem wide enough to cover any computer code representation, however fleetingly held[37].

Within the regulatory framework, the VAT requirements have been amended to accept the electronic submission of invoices as satisfying the requirements for a written invoice record[38]. It would therefore seem possible that the courts could view such regulatory provisions as a precedent for how new technologies should be accepted. However, it is also possible that the courts may conclude that, since the definition of `writing' has been expressly broadened in certain legislation, then where such wide definitions have not been explicitly adopted, the traditional paper-based interpretation should stand[39].

---

[33] See Kemp, R., "Acquiring IT: A legal perspective", p.5-7, Applied Computer and Communications Law, Vol.8, No.8. In the US, contracts with the Federal Government are governed under Public Law 97-258 (codified at 31 USC 1501), which requires that contractual offers be "supported by documentary evidence...in writing, in a way and form...authorized by law".

[34] Schedule 1.

[35] Millard, C.J., `Contractual issues of EDI', p.47 (in Walden, I., (ed.), *EDI and the Law*, Blenheim Online/London 1989), believes that the requirement for `visible form' "might militate" against electronic messages being considered a `writing'; while Bradgate, R., in `Evidential Issues of EDI', p.32 (in Walden), states that "Arguably, this is wide enough to include EDI messages". Reed, C., in "Contractual and Liability Issues", Proceedings of the EDI and the Law Conference, London, 3-4 October 1989, is categorical that they will not satisfy the definition.

[36] See also the UNIDROIT Convention on International Factoring 1988, Article 1(4)(a) which states that: "`notice in writing' includes, but is not limited to, telegrams, telex and any other telecommunication capable of being reproduced in tangible form.". See also The UNCITRAL Model Law on International Commercial Arbitration, Article 7.

[37] This has been criticised as being too expansive. See Chalton, S., "Dematerialisation of financial instruments", p.30-34, Computer Law & Practice, Vol.7, No.1, 1990.

[38] The Value Added Tax Act 1983, Schedule 7, s.3. French tax law has recently been amended to allow electronic invoices, op.cit. supra n.23.

[39] Lindberg, op.cit. supra n.21, at p.26.

In the US, the Uniform Commercial Code defines a `writing' as "any....intentional reduction to tangible form"[40]. In the US, therefore, the unresolved issue is whether the courts are prepared to accept electronic messages as being reduced to a `tangible form'[41]. The courts have accepted telexes as a `writing' under the Statute of Frauds[42], although the fact that telexes are printed out upon receipt may have been a critical factor. Alternatively, the Federal Rules of Evidence provide a very extensive definition of `writings', consisting of "letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostatting, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation"[43].

Under the UN Convention for the International Sale of Goods, no writing is required for contracts subject to the Convention:

> "A contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form..."[44].

The European Commission's study of legal restrictions on electronic communications concluded, with respect to need for a `writing' for evidential purposes, that such requirements "in civil law countries would lead to difficulties only in the fields of credit (particularly consumer credit) and insurance.."[45].

Overall, in the absence of a court case to decide whether an electronic message can be a `writing'; or statutory amendment to specifically take account of such electronic messaging systems, this is an area of legal uncertainty and insecurity. In each situation where a statutory requirement for a `writing' exists, the issue "must be assessed on the basis of its own statutory language and any case law decided under it"[46].To mitigate against such

---

[40] UCC s.2-201.

[41] See Baum, M.S., "Analysis of legal aspects", p.124, in Walden, op.cit. supra n.35. Wright, B., in *EDI and American Law*, p.4, TDCC: The Electronic Data Interchange Association, 1989, concludes that an EDI message is in a tangible form "because it makes a symbolic representation that is more than fleeting and is capable of being perceived (even though a computer must aid perception)". The ABA in `The Commercial Use of Electronic Data Interchange', p.1645, 45 Business Lawyer, No.5, June 1990, states that EDI messages are "inherently similar" to telegrams, telexes and telecopies, all of which have been found by the courts to satisfy the UCC definition.

[42] Eg. *Hawley Fuel Coalmart Inc. v Steag Handel Gmbh*, 796 F.2d 29,33 (2d Cir. 1986).

[43] Fed.R.Evid. s.1001(1).

[44] Art.11, known as the `Vienna Convention', signed 11 April 1980, came into force 1 January 1988 [Annex I, U.N. Doc.A/Conf. 97/18 (1980)]. The Convention has been signed by over 20 states, including the US, but not the UK. Art.96 states that Convention countries may require a written form of contract, by a Declaration which cannot be overruled by an agreement of the parties. The Convention can be adopted to apply (a) only to contracts where parties are in States adhering to the Convention, or (b) all contracts governed by the law of the signatory state. See further, Hermann, A.H., "New Trade Pacts and Incoterms 1990", paper presented at the International Company Lawyers' Conference, Lisbon, 20-22 February, 1991.

[45] Tedis report, op.cit. supra n.15, at p.287.

[46] McCarthy Tétrault, `Electronic Data Interchange: A survey of the legal issues', p.6, prepared for the EDI Institute, January 1991.

insecurity, the parties might decide to include an appropriate provision within a contractual context[47].

5.1.2.3 **Signature**

Within English law, there often exists the requirement that in certain circumstances legal documents have to be authenticated by the person/s involved; such a process is usually referred to in terms of a document being under hand[48], signed[49], seal or deed[50]. Indeed, a recent study of the use of facsimile signatures, noted that a `signature' was a legal requirements in 27 international trade documents, and was standard commercial practice in 14 others. The report concluded:

> "...any further growth in the use of computer systems and electronic communication....will be severely restricted if present requirements continue."[51]

Traditional requirements for a deed or seal can not be replicated in an electronic environment and require legislative amendment to enable the use of electronic alternatives[52]. However, `under the hand of' is defined as:

> "For the purpose of determining whether a document is `under the hand' of the granter, the signature is more than a mere formality or solemnity, and its unique significance as the recognised and indispensable token of deliberate authorisation of a written document, whether formal or informal, has long been accepted by common usage"[53]

Therefore, `under the hand of' can generally be held to denote the use of a `signature' without any specific formalities; which is intended to assert that the document originated from

---

47 See Chapter 6, at 6.2.2.

48 Eg. in the factoring industry, a legal assignment is governed by the Law of Property Act 1925, section 136: "Any absolute assignment by writing under the hand of the assignor...".

49 Eg. the Marine Insurance Act 1906, s.22-24.

50 "A deed is required to be written on parchment or paper and to be sealed by a seal...", Chalton, S., "The Authentication of the Origin and Content of Paperless Transactions, and Questions of Liability in Common Law", CELIM Conference, op.cit. supra n.25, at p.103.

51 See "Facilitation Measures Applicable to Particular, Selected Procedures", TRADE/WP.4/R.555.

52 Eg. The Law of Property (Miscellaneous Provisions) Act 1989, s.1(1):

"Any rule of law which -

(a) restricts the substances on which a deed may be written;
(b) requires a seal for the vaild execution of an instrument as a deed by an individual; or
(c) requires authority by one person to another to deliver an instrument as a deed on his behalf to be given by deed,

is abolished."

See also Companies Act 1989, at s.130, which inserts s.36a of the Companies Act 1985, removing the requirement for a seal.

53 *Waterson's Trustees v. St. Giles Boys Club* [1943] S.C. 369, per Lord Justice-Clerk at p.374.

a particular person (the signature being unique to the signatory) and that the person therefore authenticates the contents of the document as being correct/accurate[54].

The functions of a signature need to be identified when considering whether an electronic alternative could, or should, be legally acceptable. One author has identified five distinct functions of a signature: identification of the signer; authentication of the contents; the evidential function; finalization, ie. that the contents of the document are in their final form, and as a warning to the signer that he is accepting legal responsibility for the contents[55].

In UK law, there is no formal legal definition of a `signature'; however, past English court cases have held that a wide range of alternatives to handwriting satisfy the requirement for a signature, including a rubber stamp with a facsimile signature[56] and initials[57]. Indeed legal opinion has even suggested that the answerback of the sender of a telex would constitute a signature:

> "I reached a provisional conclusion in the course of the argument that the answerback of the sender of a telex would constitute a signature, whilst that of the receiver would not since it only authenticates the document and does not convey approval of its contents."[58].

It would therefore not seem unreasonable for the courts to accept electronic alternatives, such as a `digital signature'[59], as adequately fulfilling the legal functions of traditional signatures: a sign, symbol or mark, unique to the signatory and intended to authenticate or assent to the contents of the document/message.

International legal instruments are another source of `signature' requirement, and has been defined in two major transport-related conventions as:

---

[54] The National Committee on International Trade Documentation of the United States defines the role of a `signature' as "a means of identifying the person responsible for the preparation and verification of the information. It establishes a source responsible for the genuineness of the data transmitted", quoted in TRADE/WP.4/GE.2/R.79.

[55] Lindberg, op.cit. supra n.26, at p.39.

[56] *Goodman v J.Eban* [1954] 1 Q.B. 550.

[57] *Re Wingrove* 15 Jur. 91.

[58] Staughton, J. obiter in *Clipper Maritime v Shirlstar Container Transport* [1987] I Lloyds Rep.546, 554.

[59] A `Digital Signature' is defined in ISO standard (ISO 7498-2) as: "Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery". See also ISO Publication DIS 9594-8: 1988/E. See further Chapter 2, at 2.3.3.

"The signature...may be in handwriting, printed on facsimile, perforated, stamped, in symbols, or made by any other mechanical or electronic means, if not inconsistent with the law of the country where....the document is issued."[60]

However, this wide interpretation has not be adopted in other international conventions, which have characterised the means of signing particular documents much more restrictly[61].

As with the `writing' requirement, it might be appropriate, in terms of legal security, for companies to include a specific provision, within a contractual context, stating that the parties agree to accept electronic means of authentication as having an equivalent status to a hand-written signature.

5.1.2.4 **Contract formation**

Generally, contracts can be distinguished into one of three categories:

- solemnised contracts that require certain specific formalities to be completed, for them to be valid, such as for the sale of land;

- real contracts which are subordinated to the delivery of the object of the contract, such as a mortgage;

- and consensual contracts, which require only the agreement of the parties[62].

It is only this final category that can be straightforwardly achieved via an electronic messaging system.

In order for a contract to be created, it is necessary that the persons involved have the necessary authority to bind the company into the contractual relationship. This could create legal problems in a pure EDI-type communication system, where the order message for goods (the offer) may be automatically generated by the Company's system when stocks reach a certain level. Could the company later deny that the machine had the authority to make such an offer?

---

60 The 1978 United Nations `Convention on the Carriage of Goods by Sea' (the "Hamburg Rules"), at Article 14; and the 1980 UNCTAD (United Nations Commission on Trade and Development) `Convention on International Multi-modal Transport of Goods', at Article 5(3).

61 Eg. Montreal Protocol No.4 (to amend the Convention for the Unification of certain rules relating to International Carriage by Air, signed at Warsaw on 12 October 1929, as amended by the Protocol signed at the Hague on 28 September 1955), which states that the signature "may be printed or stamped" (Article 6(3)).

62 Amory, B. and Mark Schauss, "EDI as a way to perform and conclude contracts", paper presented at COMPAT'88, 29 Feb.-2 Mar., The Hague, Holland. See generally, "La formation des contrats par echange de donnees informatisees", Tedis final report, July 1991.

One author has suggested that the parties could, possibly in a communication agreement[63], explicitly designate the role of `system executive', who would be the person responsible for the functioning of the communication system (eg. the IS manager), and would be accepted by the parties to represent the offeror in the contract formation process[64]. A similar idea has been adopted in the UK Copyright Designs and Patent Act 1988, which states that the author of a computer-generated copyrightable work is the person "by whom the arrangements necessary for its creation are undertaken"[65].

Another traditional requirement for contract formation is that the parties to a contract declare their intent to form such relationships[66]. Can such a declaration be made within an automatic communication system? It is not necessary, under English law, for the person accepting a contractual offer to have read its contents in order to be bound by it, therefore, allowing for automatic acceptance[67]. For both parties, the courts are likely to conclude that an intent to form contractual relations can be implied by the implementation of such a system.

The requirement for contractual intent to exist, however, is more likely to create a jurisprudential problem as communication systems become completely automatic, within an open-trading environment. For example, it could be envisaged that a system, upon reaching a pre-determined level of stocks, contacts a central directory of suppliers, containing information concerning price and quantity of stock available for purchase, etc.. The system would then determine which supplier was most suitable to fulfil the requirements and then generate an appropriate purchase order for the required amount. In the event of a dispute arising, it could be argued by the company that wishes to opt out of the arrangement that insufficient intent on behalf of the company can be shown to have existed[68]. Such a conclusion is obviously an issue for the courts to decide

Alternatively, it has been suggested that data elements could be created, which trading parties would agree to use, within a message that would correspond to a `commitment opening clause' and `commitment closing clause'. The parties would include such data

---

63 See Chapter 6, at 6.2.

64 Lindberg, op.cit. supra n.26, at p.54.

65 Copyright Designs and Patents Act 1988, s.9(3).

66 *Kleinwort Benson Ltd v Malaysia Mining Co.* [1989] 1 WLR 379, CA.

67 *L'Estrange v F. Graucob* 1934 2KB 394 and *Thorton v Shoe Lane Parking* [1971] 2 QB 163..

68 "Contract Formation and Open EDI Systems", letter sent by Ake Nilson to Jan Freese, Chairman, ICC Working Party on EDI, 19.11.1991. This potential issue is also noted in the Tedis study, "La formation des contrats par échange de données informatisées", paras. 2.3.1.3/4, to be published in 1992; quoted in UNCITRAL report, A/CN.9/WG.IV/WP.53, 16 December 1991. See also Allen, Thomas, "Electronic Data Interchange, computer ordering and the formation of contracts", pp.2-13, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992 and Marsh, D., "Legal aspects of EDI', pp.427-430, Proceedings of EDI 92, Paris, 2-4 June 1992.

elements when they intended a message to have contractual effect. Such a technical process could contribute greatly to clarity and legal security[69].

These issues may need to be clarified, however, where the parties are piloting such an EDI system, with traditional paper communications being maintained as back-up. If, for example, the electronic offer message is received, but the paper offer fails to arrive, what is the legal status and intention of the electronic message? Such issues may need to be resolved by prior agreement[70].

Traditional contract formation involves the basic requirements of offer and acceptance. However, the place and moment of contract formation, both potentially critical commercial issues[71], varies according to which of four rules the legal jurisdiction, in which the dispute arises, applies:

> "the declaration rule, the contract is formed at the moment and the place the decision to accept has been taken..;
> the expedition rule, the contract is formed at the moment and the place the declaration of the acceptance is sent..;
> the reception rule, the contract is formed at the moment and the place the declaration arrives at destination..;
> the information rule, the contract is formed at the moment and the place the offeror takes notice of acceptance."[72]

Under English law, the general rule concerning electronic modes of communication, such as telex, seems to have been initially set out in *Entores Ltd v Miles Far East Corporation*[73], which stated that the instantaneous nature of electronic communication means that acceptance of a contract, and therefore the time and jurisdiction, occurs when the message is received (the reception rule).

However, does this rule apply to contracts made by all electronic messaging systems? In some network provider contracts, there are no guarantees regarding the time in which the

---

[69] de Vries, Dr H., "How to secure legal effect for commercial deals made by electronic messages transmission", UN/ECE, `Proposal for the Inclusion in the Trade Data Elements Directory (UNTDED) of Data Elements Signifying "Legal Acceptance"', TRADE/WP.4/R.399.

[70] See Chapter 6, at 6.2.

[71] Eg. where the contract involves high-value funds transfers, the moment of contract formation could mean significant differences in interest payments due etc..

[72] Elias, Lieve, "Data security and formation of contracts", paper presented at `Data Security in Computer Networks and the Legal Problems' Conference, Hannover, 23-24 September, 1991.

[73] 2QB 327 (1955). In the US, the `Restatement on Contracts (second)' states that "telephone or other medium of substantially instantaneous two-way communication is governed by the principles applicable to acceptances where the parties are in the presence of each other".

message will be sent[74]; and although in most cases the message is sent virtually instantaneously, the addressee may not receive it in that instant, since the recipient can choose when to `open' his electronic mailbox[75], or he may not be present at a suitable terminal.

In a 1982 case, *Brinkibon Ltd., v Stahag Stahl und Stahlwarenhandelsgesellshaft GmbH*[76], the *Entores* decision concerning instantaneous modes of communications was confirmed, Lord Wilberforce outlined the principles upon which future similar decisions would be made:

> "No universal rule can cover all such cases: they must be resolved by reference to the intentions of the parties, by sound business practice and in some cases by a judgement where the risks should lie."[77]

To date, the UK courts have yet to resolve the question of whether an EDI-type data communication system should follow the traditional `postal' (expedition) rule[78], where acceptance takes place when the message is submitted to the communication provider; rather than that established for other forms of electronic communication[79].

This problem is obviously made more complex within an international environment, where different rules apply to the moment at which a contract is concluded[80]. Under Articles 15, 18 and 23 of the UN Convention on the International Sale of Goods, contracts are formed at the moment the indication of the assent reaches the offeror[81]. Amory and Schauss have suggested that such issues should be decided according to three key criteria: the degree of instantaneous, the quality of the dialogue and the security of the communication[82].

---

74 see Chapter 6, at 6.3.

75 Indeed, with agreement of the network provider, some communication systems enable the sender to remove the message even after delivery to the recipients mailbox; see Sharpe, D.M., "EDI - The Legal Issues", p.8, paper presented at the `Gain the competitive edge with EDI' Conference, Sydney/Melborne, May, 1990.

76 [1982] 1 All ER 293.

77 The judgement also noted circumstances where the `reception rule' might not apply, eg. "messages may be sent out of office hours, or at night, with the intention, or upon the assumption, that they will be read at a later time"; "There may be some error or default at the recipient's end which prevents receipt at the time contemplated and believed in by the sender. The message may have been sent and/or received through machines operated by third person.", Ibid., at 296.

78 *Household Fire Insurance v Grant* (1870) 4 Ex.D. 216.

79 For further discussion of this point see Harvey, S., and J.Newman, "Contracts by Electronic Mail: Some Issues Explored", p2-6, The Computer Law and Security Report, Vol.3, No.6, 1988. Also Chalton, op.cit supra n.50, at p108; which views electronic mail systems as instantaneous. Alternatively, Sharpe, op.cit. supra n.76, at p.7, argues that electronic systems should be classified as instantaneous only if the recipient has the ability to interrupt a message to ask questions etc. See also Millard, op.cit. supra n.35, at pp.45-46; and Schauss, M., "Issues of Contract Law", at p.78-81, in Poullet, Y. & G.P.V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law*, No.1 Computer/Law Series, Kluwer/The Netherlands 1988.

80 See Uncitral 1990 Report, op.cit. supra. n.17, at p18 and Tedis Report, op.cit. supra n.15.

81 Vienna Convention, op.cit. supra n.44.

82 Amory, op,cit. supra n.62.

In contract formation, based upon documentation such as purchase orders, rather than prior agreement, the purchaser's standard trading terms and conditions tend to be incorporated within the body of the document (usually in small grey print on the reverse of the order!). How can such standard terms and conditions be incorporated in an electronic messaging environment, without significantly increasing the length and cost of the message?

The rules concerning how a contracting party should incorporate its standard terms and conditions of trading are, in certain legal systems, specifically provided for in legislation[83]; although the general rule would seem to be that the courts will:

> "consider whether it can reasonably be inferred from the context that the party against whom general conditions are asserted has had an opportunity to be informed of their contents or whether it can be assumed that the party has expressly or implicitly agreed not to oppose all or part of their application."[84]

Electronic trading partners need to be aware of such rules when concluding international electronic trading agreements. Some legal forums, such as the ABA Model Trading Partner Agreement and UNCITRAL, have recommended that such term and conditions should be included in the communication agreement[85]. The CMI Rules for Electronic Bills of Lading[86] state that standard international trade terms and conditions must be considered as part of the contract of carriage by mere reference; although a copy of them must be readily available[87].

An alternative, technical, solution would be to refer to any standard conditions of trading within a data element of an electronic message[88]. Indeed, the reference could be to an electronic copy of the company's standard terms and conditions maintained on a database system, similar to the X.500 development[89].

---

[83] Eg. The German General Terms and Conditions Act ["AGB-Gesetz" of December 9, 1976] Section 2(2) states:

1.The Users of the terms and conditions must point out prior to or upon the conclusion of a contract that they wish to see them included in a contract;
2. the other party must consent, but not necessarily by express declaration;
3. it is not necessary to transmit the terms and conditions to the other contracting party, the other party is expected to ask for such a transmission.

[84] Schauss, M., op.cit. supra n.80, at p.77.

[85] See the American Bar Association report, `The Commercial Use of Electronic Data Interchange', prepared by the Electronic Messaging Services Task Force, p.1645, 45 Business Lawyer, No.5, June 1990; and Uncitral, 1991 report, op.cit. supra n.69, at p.17. See also Chapter 6, at 6.2.

[86] See 5.2.5.1. below.

[87] CMI Rules, op.cit. supra n.108, below, at Rule 5(a) & (b).

[88] See UN/ECE, `Legal Aspects of Automatic Trade Data Interchange', p.10, TRADE/WP.4/R.185/Rev.1, 21 October 1982.

[89] See Chapter 2, at 2.2.3.1.

It should be noted, that a failure to deal with the issue of standard terms and conditions could lead to a continuation of the traditional battle of forms scenario[90]. It has been commented that:

> "one of the most salutary effects that the introduction of EDI could have on business practices would be to require the formulation of mutually acceptable (and therefore more reliable) terms of dealing between important trading partners through conscious negotiation of new master agreements."[91]

5.1.2.5 **Negotiable Instruments**

> "...where an instrument is, by the custom of the trade, transferable, like cash, by delivery, and is also capable of being sued upon by the person holding it *pro tempore*, there it is entitled to the name of a negotiable instrument, and the property in it passes to a bona fide transferee for value..."[92]

As mentioned in the introduction to this chapter, one of the most difficult areas to replicate in an electronic environment is the symbolic function that paper can possess in certain commercial contexts: where the physical possession of a document confers certain legal rights. The two most prominent examples, in UK commercial practice, are bills of exchange[93] and bills of lading[94]. Such legal instruments are used primarily for international trade transactions and money transmissions, but can also act as securities within a financing arrangement.

There are three distinct features of a negotiable instrument: full legal title is passed upon delivery of the instrument; no notice of transfer need be given to the issuer of the instrument and the title is passed unfettered (ie. free of equity)[95]. In order to fulfil the first and last of these features, there needs to be a unique document in existence. It is this aspect which creates particular concerns in an electronic environment.

---

[90] See Wright, op.cit. supra n.41, at 29; Nilson letter, op.cit. supra n.69 and Savage, R., "How to resolve legal issues in EDI agreements: Acknowledgements and the Battle of Forms", pp.66-71, EDI Forum, No.1, 1991.

[91] Crawford, B., "Strategic Legal Planning for EDI", p.70, Canadian Business Law Journal, Vol.16, 1989.

[92] 1 Sm.L.C.456, summarising *Miller v Race* and quoted with approval by Blackburn J., *Crouch v Credit Foncier of England* L.R. 8 Q.B. 381-382.

[93] See generally, *Byles on Bills of Exchange* (26th ed.), F. Ryder & A. Bueno, Sweet & Maxwell, 1988.

[94] See generally, Atiyah, P.S., *The Sale of Goods* (8th. ed.), Pitman, London, 1990 and Goode, R., *Commercial Law*, Penguin/Allen Lane, 1982.

[95] This final feature is not true for bills of lading, since title remains subject to prior claims from third parties, and therefore they can be classified as quasi-negotiable instruments.

Over recent years, there has been a number of initiatives taken by international organisations to enable the communication of such negotiable instruments by electronic communication systems. Within this work, three separate approaches can be distinguished:

(i) Amendment of the relevant legislation[96].

Where the law provides that possession of a negotiable instrument establishes a presumption of evidence of legal title, then changes in legislation will be required, due to the requirement for a `writing'[97].

(ii) Create an electronic procedure which replicates the symbolic function[98].

(iii) Encourage commercial practices to change.

The negotiable bill of lading, for example, is used by companies for the vast majority of international trade; however, the vast majority of trade does not require the use of such a document, because the cargo is not bought and sold in transit[99]. A number of recognised alternatives to the bill of lading currently exist[100], and yet companies still prefer to make use of a document they have used for years.

5.1.2.5.1 Bills of lading

The negotiable bill of lading is seen as one of the most difficult legal instruments to transform into an electronic environment[101]. The traditional bill of lading can be seen to fulfil three functions:

1. Evidence of the condition of the goods at the time of shipment; signed by the carrier as evidence in any future dispute;
2. the terms of the contract of carriage, and

---

96 Eg. when the Norwegian Registry of Securities became paperless in 1987, the Stock Act 1976 had to be altered to allow for the transfer of ownership through electronic registrations in the accounts of the system; see Galtung, Andreas, *Paperless Systems and EDI: A survey of Norwegian law*, p.24, Complex 4/91, Tano, Oslo, 1991.

97 See Section 5.2.2. above.

98 Eg. see details of the CMI Rules for Electronic Bills of Lading, at 5.2.5.1 below.

99 Roy Goode has estimates that 80-90% of Bills of Lading are never negotiated; quoted in Sarson, Richard., "EDI in the Dock", p.124, Network, May 1989.

100 "Bills of lading are frequently replaced by non-negotiable documents similar to those which are used for other modes of transport than carriage by sea. These documents are entitled `sea waybills' - `liner waybills' - `freight receipts' - or variants of such expressions. These non-negotiable documents are quite satisfactory to use except where the buyer wishes to sell the goods in transit...However, when the contracting parties know that the buyer does not contemplate selling the goods in transit they may specifically agree to relieve the seller from the obligation to provide a bill of lading..."; Introduction to `Incoterms 1990', ICC Publication no.460.

101 See, for example, Gronfers, "The Paperless Transfer of Transport Information and Legal Functions", in Schmitthoff & Goode (ed.), *International Carriage of Goods: Some Legal Problems and Possible Solutions*, 1988.

3. the document of title[102].

However, in terms of modern international trade its use creates significant obstacles. Developments in transportation, particularly containerisation, means that in many cases the goods move faster than the associated paper documentation. This is especially the case if the bill of lading has been traded several times during transportation (possibly as much as 100 times in the case of bulk oil cargoes), and therefore it can take many months for the bill of lading to arrive at the port at which the cargo was discharged.

Such problems have meant that international traders have resorted to practical techniques designed to overcome the delays, but which, in the process, seriously undermine the legal validity of the bill of lading[103]. Some carriers, for example, carry a copy of the bill of lading aboard ship, so that it can be passed to the appropriate person at the port of arrival, therefore protecting the carrier from liability for releasing the cargo to the wrong party. Bill of lading guarantees are also used, where a guarantee is presented to the carrier at the port of discharge, stating that the bank agrees to indemnify the carrier against liability when releasing the cargo without a bill of lading[104].

This breakdown in the reality of the bill of lading as a secure legal instrument, has encouraged the drafting of schemes designed to `dematerialise' the bill of lading: remove the paper backing! Indeed, dematerialisation by removing the delays of moving paper documentation may be a means to restore the traditional securities and functions of this legal instrument.

The most prominent attempt to establish a practical electronic trading system for bills of lading was set up by INTERTANKO; called the SeaDocs scheme[105]. It was designed for the trade of bulk oil cargoes, an area of trade where substantial changes of ownership evidenced by transfers of the bill of lading, occur during the period of transportation. Under the scheme, the Chase Manhattan Bank would act as central registry for the bill of lading and, acting as an agent for all parties, would transfer ownership upon electronic notification. However, the scheme failed to become fully established for two major reasons: lack of interest by

---

[102] A document of title to goods is "a document relating to goods the transfer of which operates as a transfer of the constructive possession of the goods, a may operate to transfer the property in them.", Benjamin, *Sale of Goods* (3rd ed.), 1987, at para. 1433.

[103] See Todd, P., "The effect on letters of credit of new documentation, and the introduction of electronic and paperless transactions", paper presented at IBC's International Letters of Credit Conference, London, 3rd July 1990.

[104] However, see *The Delfini*, [1990] 1 Lloyd's Rep 252.

[105] For further details see Gram, P., "The INTERTANKO project - delivery of tanker cargoes without presentation of bills of lading", p.176-189, in Nordipro, op.cit. supra n.10; Urbach, A., "The Electronic Presentation and Transfer of Shipping Documents", in Goode, R.M., *Electronic Banking: The Legal Implications*, The Institute of Bankers 1985 and Centre for Commercial Law Studies, Queen Mary College, University of London, and Love, K., "Seadocs: The lessons learned", in proceedings of `The Future of Bills of Lading', 7-8 April, London, 1992.

companies concerned for the commercial privacy implications; and the prohibitive cost of obtaining insurance coverage for the bank's liability under the scheme.

Learning from the experiences of the SeaDocs scheme, the Comité Maritime International (CMI)[106], decided to formulate an alternative system. In 1990, the CMI published a set of rules that can be contractually adopted between international trading partners to permit the electronification of the bill of lading: the CMI Rules[107]. The scheme operates on the basis that the bill of lading is held by the carrier, who alters the ownership of the bill upon electronic notification. Such notification requires the sending of a `private' authentication code[108], which then triggers a registered change of ownership and a new private code is issued, by the carrier, to the new consignee or holder.

Under the CMI scheme, the parties need to contract for the use of electronic communications[109], as well as the contract for carriage. The parties are also able to opt-out of the scheme and demand the issuance of a paper bill of lading at any point during the period of the contract.[110]

An alternative version of this scheme has been put forward by the US International Trade Facilitation Council. This proposal suggests the establishment of the position of `control party':

> "Party to the shipment or computer/communications company designated by the shipper to perform the following functions:
>
> 1. Provide or obtain reliable communications required;
> 2. Test communications prior to the shipping of the goods with all parties to the shipment as designated by the shipper;
> 3. Maintain records of all related actions and transmissions;
> 4. Provide and assign Individual Authentication Code (IAC)....., to shipper and all subsequent consignees."[111]

---

106 The CMI is composed of more than 50 national maritime law associations.

107 Produced by the CMI Subcommittee on `Electronic Transfer of Rights to Goods in Transit', Chair, Professor Jan Ramberg (University of Stockholm). Adopted by the CMI on 22 June 1990, Paris Convention (hereinafter referred to as the CMI Rules). See Introduction to CMI Rules Electronic Bills of Lading, Paris/ELECTRO 15, and Chandler III, George F., "The Electronic Transmission of Bills of Lading", p571-579, Journal of Maritime Law and Commerce, Vol.20, No.4, October 1989. See Nilson, A., "An introduction to the BIMCO B/L project", Marinade; a paper which describes the practical implementation of the CMI rules.

108 Eg. RSA Public-Key Encryption systems, see Chapter 2, at 2.3.3.

109 CMI Rules, at Rule 1.

110 Ibid., at Rule 10.

111 `Electronic Bill of Lading' - Transmitted by NCITD, UN/ECE TRADE/WP.4/R.710, 15 August 1990, at p.3.

This scheme is similar to the CMI Rules, except that the responsibility does not need to be placed upon the carrier, if the parties would prefer to use of a bank, as in the SeaDocs scheme.

With all these schemes, there is the additional issue of how to deal with the subsidiary legal documents, such as the insurance contract/certificates, which need to be transferred at the same time as the goods[112]. If such documentation, particularly when required by governmental authorities, can not be `dematerialised', then the parties may lose many of the benefits of an electronic bill of lading.

Recently, in the UK, an Act, `The Carriage of Goods by Sea'[113], was passed which amends the Bill of Lading Act 1855. Clause 1(5) of the Act provides:

> "The Secretary of State may by regulations make provision for the application of this Act to cases where a telecommunication system or any other information technology is used for effecting transactions corresponding to -
>
> (a) the issue of a document to which this Act applies;
> (b) the indorsement, delivery or other transfer of such a document; or
> (c) the doing of anything else in relation to such a document."

Another source of quasi-international trade law, relevant to bills of lading, are the ICC's INCOTERMS[114] which grew up out of trade practice and reflect internationally recognised trade terms, such as CIF (Cost, Insurance Freight), which calls for a `clean on board bill of lading'. In 1990, a new edition was published, which recognised the emergence and use of electronic modes of communication:

> "where the seller and the buyer have agreed to communicate electronically, the document....may be replaced by an equivalent electronic interchange (EDI) message"

Such legislative amendment will encourage the further development and adoption of the electronic schemes outlined above; however, these changes do not remove all the legal insecurities regarding the use of electronic bills of lading[115].

---

112 Eg. certificates concerning questions of origin, health, packaging and safety features.

113 Passed 20 July 1992, comes into force from 15 September. The Act was based on a Law Commission Report: `Rights of Suit in Respect of Carriage of Goods by Sea', No.196, Scot. Law Com. No.130, HMSO, London 1991.

114 Current edition INCOTERMS 1990, No.460, published on 1 July, 1990. The Incoterms were first published in 1935.

115 See Hermann, "Incoterms are revised but leave issues uncovered", p.8, Financial Times, August 6, 1990; and Reed, op.cit. supra n.2, at p.146-147.

5.1.2.5.2 Dematerialisation of financial instruments

With the rapid growth of the financial markets over the past three decades, the burden created by the need to administer the paper component of financial deals became an obvious area where the use of electronic communication systems could be effectively applied. Certain aspects of finance have been electronified for a number of years, such as electronic funds transfer systems[116]; however, other aspects are currently being reviewed: for example, documentary credits and share certificates.

Documentary credits are a chain of contracts between banks, whereby receipt of the appropriate shipping documents gives rise to a payment between one bank and the previous bank in the chain. Due to the international nature of such arrangements, it has been necessary to provide standard contractual terms governing documentary credits: The ICC's Uniform Customs and Practice for Documentary Credits (UCP)[117]. In 1990, the ICC's Banking Commission agreed to establish a sub-committee to consider the possibility of revising the current rules to permit the use of an `electronic trade credit'[118].

In the UK, and other financial centres, there has been a move towards the creation of electronic share trading systems, to replace the current heavily paper-based system. The UK scheme is known as Taurus[119]. The implementation of the scheme has required amendment to the UK Companies Act 1989, to permit share ownership to be evidenced in other than a paper medium[120].

Any system of dematerialisation needs to be able to replicate the functions of the paper system:

---

116 Both interbank EFT systems, eg. SWIFT; bank-company systems, eg. BACS, and bank-customer systems, eg. EFTPOS. For a detailed description of such services see Chapter 5 of *The Encyclopedia of Information Technology Law*, General Editor, Stephen Saxby, Sweet & Maxwell, 1990.

117 ICC's UCP, 5th Edition, 1983, Doc. No.400. Article 2 defines documentary credits as "any arrangement....whereby a bank, acting at the request and on the instructions of a customer, is to make payment to or to the order of a thrid party....against stipulated documents...". The USA is one of the few countries which has incorporated documentary credits into domestic legislation:

> "a credit must be in writing and signed by the issuer.....A telegram may be a sufficient signed writing it it identifies its sender by an authorised authentication. The authentication may be in code and the authorised naming of the issuer in an advice of credit is a sufficient signing." [UCC, s.5-104]

118 ICC Banking Commission, 24th October 1990, ICC Doc. 470/575. One means of removing the documentary requirement is the use of `stand-by' letters of credit, where the bank only agrees to pay the seller if the buyer defaults on the payment; see Wheble, B.S., "EDI in International Trade", paper presented at *EDI and the Law 90: Making Paperless Trade Legally Secure*, London, 14-15 November 1990. See also Power, L., "The legal implications of commercial electronic letters of credit", pp.115-137, in Proceedings of the *3rd National Conference on Law, Computers and Artificial Intelligence*, University College of Wales, Aberystwyth, 30 March-2 April 1992 and Reed, C., "Electronic Trade Documentation: Legal Obstacles and Solutions", pp.35-55, *EDI & the Law*, 7 May 1992.

119 For further details, see `Project Taurus - A Prospectus for Settlement in the 1990s', International Stock Exchange, March 1990; Pym, J. and Peter Hill, "Taurus", pp.13-22, Practical Law for Companies, Vo. II, No.7, August 1991, and Reed, op.cit supra n.2, at p.123-127.

120 Part IX, s.207 "Transfer of Securities".

- Uniqueness;
- It evidences the obligation represented by the instrument, eg. the debt in the case of a bond; and
- It evidences the chain of transfers to the current holder[121].

The electronification of financial instruments can either occur through full dematerialisation, where no paper instrument is created, such as the Taurus share-dealing scheme; or alternatively, partial dematerialisation, where the paper instrument exists, but is traded electronically, via a clearing system, and which can be recovered when required at the end of the transaction chain, such as under SeaDocs.

In either case, the method for achieving such dematerialisation can involve one of two options:

(a) Central registry: Eg. SeaDocs and Taurus. A central registry would serve the function of `custodian of the instrument' and record-keeper of all the transactions involving the instrument; as such, a central registry would need to be an `independent' third-party, with respect to the trading parties[122]. The cost of establishing such a service, in terms of the IT systems maintained by the registry and the need for multi-party communications, would seem to limit this option to situations involving high volume, high value transactions.

(b) `Stand-alone' system: Following traditional paper-based practice, the trading parties would simply move the electronic instrument between themselves, according to the trading chain. Although this methodology has not currently been adopted, the technology, particularly the use of public key cryptography[123], would make such a system feasible in terms of security.

The key factor behind the successful adoption of either methodology is the perceived `legal security', such as non-repudiation of origin/receipt and claims of ownership and possession, that such a system can provide users.

An additional issue raised by the dematerialisation of financial instruments, concerns the means of evidencing the chain of transfers. In an electronic environment this could be

---

121 Reed, op.cit. supra n.2, at p.114.

122 The Jack Report, op.cit. supra n.12, at para. 8.33-8.38, recommends legislation to allow the use of central registry systems, approved by either the Bank of England or the Treasury. See also EC Tedis Report, 'Trusted Third Parties and Similar Services' (final), November 1991; and "A Service Infrastructure for EDI Security", TEDIS final report, December 1991.

123 See Chapter 2, at 2.3.3..

achieved either by reference to the records held by the central registry; or by enabling the document to keep track of its own history, ie. maintaining the digital signatures of all parties that have traded the instrument. In certain situations, however, the trading parties might demand anonymity, and therefore rules would have to be established to maintain such confidentiality[124].

5.1.2.6 International trade law

> "Legal problems of international trade facilitation may be the outcome of usages, ie. of established commercial practice, or be a result of national law - of the exporting country, the importing country or a third party `transit country'. They may also stem from the effects of international law, whether bilateral agreements or international conventions"[125]

One of the main drives towards the use of data communications came from the international trade community, where speedier communications could be seen as significantly improving efficiency, and therefore facilitating trade. The key pre-requisite to the adoption of data communications was the need to review the vast array of existing trade documentation in order to simplify such data requirements to enable conversion into a suitable electronic format[126]. Within the European Community, the creation and introduction of the Single Administrative Document (SAD)[127], replacing the use of over one hundred existing paper documents, was a significant contribution to the process of facilitating trade throughout the Community.

This section reviews the major initiatives that have been taken, by certain international organisations, in this critical area.

The primary organisation to actively consider the legal issues raised by the use of data communications was the United Nations Economic Commission for Europe (UNECE). Its activity in this area has primarily been related to trade facilitation, carried out by a sub-group of the UNECE, the Working Party on Facilitation of International Trade Procedures (WP.4), which was established in 1961. The terms of reference of WP.4 are that it shall:

---

124 See `Presentation of Services and Possible Solutions', draft report for Task 1, Tedis B7 (March 12, 1992), presented at Tedis Workshop, Brugge, 27-28 April 1992. This report discusses the use of cryptographic methods to provide a range of security services for electronic messaging, including `interactive authentication' and `anonymity'.

125 UN/ECE TRADE/WP.4/GE.2/R.102, quoted in Wheble, Bernard, "International Trade Procedures", p20, The Computer Law and Security Report, vol.3, no.2, 1987.

126 Eg. the UN Layout Key; see Thomsen, op.cit. supra n.1, at p.11-31.

127 Came into operation from the 1 January 1988.

"facilitate international trade and transport by promoting rationalisation of trade procedures and effective use for this purpose of electronic or other automatic data processing and transmission"[128]

During the 1970s, as part its work on simplifying trade procedures, the Working Party devoted increasing attention to the use of data communications technology to speed up the movement of information required in international trade. To date, its most significant achievement has been the development of the United Nations Electronic Data Interchange For Administration, Commerce and Transport (UN/EDIFACT), as an international messaging standard[129].

Considerations regarding the facilitation of trade have inevitably involved studying the potential legal impediments to the use of data communications[130]. In this respect, the Working Party has issued a number of recommendations which outline the necessary legislative amendments that member states need to consider in order to facilitate the use of data communications in international trade. One of their first recommendations calls upon governments and international organisations to allow for the possibility of authorisation by electronic means, rather than the traditional signature.[131]

The Working Party has also encouraged the relevant authorities to adopt the 1975 Montreal Protocol No.4 to the Warsaw Convention on International Carriage by Air, Article 5(2), which would abolish the legal requirement for an airwaybill[132]. Unfortunately, as with the 1978 United Nations `Convention on the Carriage of Goods by Sea'[133], and the 1980 UNCTAD `Convention on International Multi-modal Transport of Goods'[134], and similar activities arising within public and private international law, the Protocol has not yet been ratified.

In 1982, the Working Party accepted a report which concluded:

"that there is an urgent need for international action to establish rules regarding legal acceptance of trade data transmitted by telecommunications. Since this is essentially a

[128] Introduction to UN/EDIFACT, TRADE/WP.4/INF.105, 12 July 1988.

[129] See Chapter 2, at 2.2.3.2.

[130] See `An Overview of Legal Problems of Trade Facilitation', TRADE/WP.4/GE.2/R.102, 10 November 1977.

[131] Recommendation No.14, TRADE/WP.4/INF.63. See also Recommendation No.12 (TRADE/WP.4/INF.61): Measures to Facilitate Maritime Transport Document Procedures, and Recommendation No.13 (TRADE/WP.4/INF.62): Facilitation of Identified Legal Problems In Import Clearance Procedures.

[132] Recommendation No.18, facilitation measure 7.5, ECE/TRADE/141.

[133] Article 14: "The signature on the bill of lading may be in handwriting.....or electronic means"; see section 5.2.2. above. However, the `Hamburg Rules' still retain the concept of a paper document: Article 1.7: "A bill of lading means a document....by which the carrier undertakes to deliver the goods against surrender of the document".

[134] Article 5 reiterates Article 14, ibid. See also the Council of Europe Recommendation No.R(81) 20 to Member States "on the harmonisation of laws relating to the requirement of proof and to the admissibility of reproduction of documents and recordings on computers".

problem of international trade law, the United Nations Commission on International Trade Law (UNCITRAL) would appear to be the central forum."[135]

Consequently, at the seventeenth session of UNCITRAL, the legal implications of data communications in international trade became a priority item on their work programme.[136]

The first report, presented by the Secretariat at the eighteenth session of UNCITRAL, in 1985, concerned `the legal value of computer records'[137]. It was based upon an international survey on the use of computer records as evidence within court proceedings. It was also linked to work carried out in co-operation with the Customs Co-operation Council to ascertain the "acceptability to customs authorities of a goods declarations in computer-readable form".

The Report found that overall the vast majority of respondent nations have adequate evidential rules to allow for the submission of computer records into court proceedings. However, they also concluded that requirements that documents be `signed' or in paper form, posed an important obstacle to the adoption of automatic data processing techniques in international trade. As a result of the report, the Commission adopted four main recommendations for governmental action:

"(i) to review legal rules affecting the use of computer records as evidence in litigation in order to eliminate unnecessary obstacles to their admission, to be assured that the rules are consistent with developments in technology, and to provide appropriate means for a court to evaluate the credibility of the data contained in those records;
(ii) to review legal requirements that certain trade transactions or trade related documents be in writing, whether the written form is a condition to the enforceability or to the validity of the transaction or document, with a view to permitting, where appropriate, the transaction or document to be recorded and transmitted in computer-readable form;
(iii) to review legal requirements of a hand-written signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication;
(iv) to review legal requirements that documents for submission to governments be in writing and manually signed with a view to permitting, where appropriate, such documents to be submitted in computer-readable form to those administrative services

135 `Legal Aspects of Automatic Trade Data Interchange', TRADE/WP.4/R.185/Rev.1.

136 Official Records of the General Assembly, Thirty-ninth Session, Supplement No.17 (A/39/17), para.136.

137 A/CN.9/265, presented to the 18th session of UNCITRAL in Vienna.

which have acquired the necessary equipment and established the necessary procedures;"[138]

These recommendations were subsequently endorsed by the United Nations General Assembly, in a 1985 resolution, in which the General Assembly:

"....Calls upon Governments and international organisations to take action, where appropriate, in conformity with the Commission's recommendation so as to ensure legal security in the context of the widest possible use of automated data processing in international trade;...."[139]

The Customs Co-operation Council (CCC) has also been actively involved in the promotion of the use of data communications in international trade. As an international organisation, it represents the national customs authorities from over a hundred member countries. The CCC's primary objectives are to encourage the development of standardised and simplified Customs procedures, as well as ensuring the enforcement of the relevant national legislation. Over the past decade, the CCC has had an active programme to encourage the adoption of automatic data processing among its members, especially since the use of such techniques has been seen as crucial if Customs authorities are to satisfactorily fulfil the burgeoning responsibilities placed upon them by government.

There are three major legal issues involved in the adoption of EDI by Customs authorities: the authentication of electronic data transfers; the admissibility of such data as evidence in legal proceedings, and the need for traders to retain records of all relevant trade for a certain time, in order to give Customs authorities the ability to carry out audits.

The CCC is a representative body, not a controlling body, therefore it is only able to offer guidance to national authorities. On 16 June 1981, the Council adopted a recommendation concerning the transmission and authentication of automatically processed goods declarations. The recommendation calls upon the relevant authorities to allow goods declarations to be made via EDI, and to allow such declarations to be authenticated by electronic means rather than by hand-written signature.

It was also recognised by the CCC that despite an increasing number of organisations making use of the facility for automatic goods declarations, many organisations using such

---

[138] Report of the United Nations Commission on International Trade Law on the work of its eighteenth session, Official Records of the General Assembly, Thirty-seventh Session, Supplement No.17 (A/40/17), para.360.

[139] Resolution 40/71, paragraph 5(b), of 11 December 1985, *United Nations Commission on International Law Yearbook*, 1985, vol.XVI, Part One, D. (United Nations publications, Sales No.E.87.V.4).

technology for trading will still need to submit paper-based submissions to Customs authorities. Therefore, in June 1982, an additional recommendation was adopted which called upon the relevant national authorities to allow organisations `greater freedom in the format for presentation of the data', in order to increase the efficiency with which they can make the appropriate declarations, even by paper.

Further action was taken in June 1986, when the CCC adopted a resolution `concerning the use of computer-readable data as evidence in court proceedings'.[140] This resolution suggested that there should be a review of all national legal requirements concerning the need for a `signature', and what constitutes a `document'.

Recently, the movement towards enabling Customs authorities to allow for the submission of electronic documentation has been encouraged by the creation of international standard messages designed to fulfil traditional information requirements. Within the UN EDIFACT process, six customs messages have recently been accepted and can be used, including CUSDEC for customs declarations[141].

5.1.2.7 **Comment**

This section has considered the range of requirements that exist in the current commercial legal framework that can create obstacles to a reliance on the use of data communication systems. The extent to which such legal requirements have had an impact on a company's decision to use data communications is, however, difficult to ascertain. For example, a US report has noted:

> "The failure of the Uniform Commercial Code to specifically accommodate the electronic communication of data has not been fatal to either the continued growth of electronic commercial practices or the continued vitality of the code itself...Yet the existence of a less than ideal fit....has had an impact upon adoption of EDI in commercial use."[142]

Despite this claim, it does not offer any evidence to back up such a claim. From the respondents to the EDI survey[143], only seven stated that legal barriers had been a significant

---

[140] TRADE/WP.4/R.330.

[141] `EDIFACTS Bulletin', Issue 8, Spring 1991. See also Chapter 2, at 2.2.3.2.

[142] American Bar Association (ABA), The Commercial Use of Electronic Data Interchange - A Report, prepared by the Electronic Messaging Services Task Force, p.28-29, 44 Business Law, 1990.

[143] Appendix B1/B2.

obstacle to the implementation of EDI, and only one of them noted a specific piece of legislation[144].

It would seem, therefore, that traditional legislative requirements have not been a significant barrier in general commercial communications. However, the relevance of such issues can be expected to increase in the future, based upon two reasons: data communications will be used for a wider range of `legally significant' forms of commercial communication; and case law should arise which may illustrate how flexibly the courts interpret statutory provisions in the context of such techniques, and therefore how legally secure current data communication practices are.

Requirements as to form have generally, historically, been motivated by a desire to ensure legal security for the parties involved. A study carried out by the European Commission concluded that requirements "to establish, deliver, send or store documents on paper and hand-written signed" were "in general linked with the validity of the legal deed, with publicity (in order to ensure the applicability to third parties), or with evidence"[145]. Therefore, any legislative revision to update such requirements to take account of the new technologies, must also maintain the need for protection[146]. Indeed, as in the case of bills of lading, the use of data communications might enable the traditional legal functions and securities of certain legal instruments, which had been increasingly ignored due to the practical inefficiencies created by paper, to be restored.

It should also be recognised, that commercial agreements, conventions and practice can also create quasi-legal obstacles to the introduction of EDI: `we have always done it that way, so why should we change'! This has been noted with respect to the use of bills of lading. When embarking on the implementation of data communications, companies therefore need to review existing contractual agreements for terminology and procedures that could be obstacles to the adoption of data communications.

---

144 i.e. Shell Nederland Chemie B.V. noted a requirement under dutch law to maintain a paper back-up. In the UK, the author was commissioned by the Association of British Factors and Discounters to consider the statutory obstacles to the adoption of EDI by its members.

145 See Troye, A., op.cit. supra n.27. Overall, the TEDIS report, op.cit. supra n.15, at p.279, concluded that "...no formal condition is required in EEC Member States for concluding or drawing most commercial contracts, or for sending purchase orders, general conditions of sale, invoices or the like..".

146 See Fresse, Jan, "EDI and National Legislation" - Teresa (86) Draft Report, ICC Doc. No. 460-10/Int.43. This report proposes a `Computer Code' of principles which should "be implemented in..statutes or regulations, so as to adapt these to EDI technology". The Code consists of seven articles, including: security aspects; contract formation; accounting and auditing; Customs and Excise; insurance and evidence.

5.2 EVIDENTIAL ISSUES

A disadvantage of electronic messaging systems is their `fleeting' nature. It can be difficult to produce an acceptable record of what has occurred between trading parties, in the event of a dispute. The use of data communications, as a substitute for paper, therefore gives rise to a number of evidential issues:

- What is the legal status of the various documents being communicated?;
- what statutory record-keeping requirements exist?;
- what rules regulate the submission of electronic records to court in the event of a dispute?;
- how can we prove to a court that our records are authentic and have integrity?,
- and what record-keeping procedures should be agreed, or laid down, between the users of data communications and the network providers[147]?

This section reviews the impact of evidential issues on the use of data communications. For the purpose of this thesis, `evidence' has been defined widely, to include requirements to maintain records of commercial events; as well as the submission of evidence in the event of a legal dispute. In either sense, however, evidential requirements need to be considered during the implementation of systems, since legal requirements for paper-based documents may prevent reliance on electronic processes. Evidential issues are also an important precautionary element of establishing `legal security'.

5.2.1 Record maintenance[148]

Companies, whether operating in a paper or electronic environment, need to ensure that adequate record-keeping procedures are established for a number of complementary reasons:

- The evidencing of events in case of dispute;
- as security against loss, destruction etc.; and
- to fulfil various statutory/quasi-regulatory requirements[149].

---

147 For a discussion of this issue, see Chapter 6, at 6.4.

148 See generally Lass, J., "Business Records and Paperless Trading", paper presented at `The Changing Pattern of Business' Conference, London, 25-26 September 1989; and List, W., "International EDI - the implications for record keeping", p.474-480, Proceedings of the 3rd International Congress of EDI Users, Brussels, 4-6 September, 1991. For a discussion of record-keeping requirements in the US, see Wright, B., *The Law of Electronic Commerce - EDI, Fax and E-mail: Technology, Proof and Liability*, at Chapter 11-12, Little, Brown and Company, Boston, 1991.

149 Eg. Companies Act 1985 and the Securities and Investment Board. See also non-statutory record-keeping requirements imposed by the professional bodies, such as Chartered Institute of Accountants and the Law Society.

The latter requirements can also be sub-divided into two broad categories: record retention requirements, such as the Companies Act 1985, ss.221-223[150]; and requirements to disclose information to various authorities/persons, which imply the need to maintain records, such as the Data Protection Act 1984.

Under English law, an action can be brought for breach of contract up to six years after the date of the breach, as laid down in the Limitation Act 1980. Documents that originate through the existence of the contract and evidence the events arising under the contract should therefore be maintained for that six year period.

The Value Added Tax Act 1983, which expressly authorises the electronic recording of information for VAT purposes, provides that the VAT Commissioners may require all accounting documents to be preserved for a period of 6 years[151].

There are no general regulations in the UK governing the medium used for archival recording, although certain authorities can require that their approval is obtained before a company relies exclusively on electronic records: For example,

- Finance Act 1985: records held for tax purposes can be maintained on computer if: the data carrier is easily convertible into a readable form; and the records are made available to the customs and excise inspectors on request.

- The Value Added Tax Act 1983, provides that computer generated invoices are acceptable provided that:

  i) the inspector is informed in writing at least 1 month before;
  ii) any conditions laid down by the inspector are followed[152].

- The Banking Act 1979, amending the Banker's Books Evidence Act 1879, expressly recognises that books includes records "kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanism[153].

---

150 Eg. a record of all assets, liabilities and monetary transactions; records of all sales and purchases of goods and stocktaking details. See also s.722(2), which states: "Where any such register...or accounting record is not kept by making entries in a bound book, but by some other means, adequate precautions shall be taken for guarding against falsification and facilitating its discovery".

151 Schedule 7, s.38, art.7.

152 Schedule 7, s.3. See `Guidelines for users exchanging accounting information', issued by the Computer Audit Branch of HM Customs & Excise.

153 Schedule 6. The books are those records which are the primary source of information within the bank; thus is paper records are transferred to microfilm or computer storage the new records become the `books'; see *Barker v Wilson* [1980] 1 WLR 884, in Reed, op.cit. supra n.2, at p.128. See also Bank of England 's "Guidance Note on Accounting and other records and internal control systems and reporting accountant's reports thereon", BSD/1987/2, September 1987.

Such record-keeping requirements will obviously mean that the electronic records need to be continuously maintained in a readable format for the relevant period from creation. Companies therefore need to ensure adequate procedures are in place to enable such maintenance. Some national evidential legislation makes explicit provision for the implementation of such procedures:

> "The computer program manuals, descriptions and instructions must be directly readable and kept meticulously updated by whoever is in charge of maintaining them"[154]

Similar such conditions have been laid down by the appropriate regulatory authorities in other countries. In Norway, for example, the Banking, Insurance and Securities Commission permitted a third-party company to store audit data on behalf of the banks, in computerised form, on condition that they could guarantee at least 10 years data readability; that the data would be printable for at least 3.5 years after registration; they established secure procedures to prevent data manipulation and that regular back-ups were made and the records were stored centrally[155].

In Canada, the Income Tax Act permits the retention of microfilm copies of various required documents, providing the microfilming process complies with the government-approved standard[156]. It has been suggested that such an approach would be applicable to electronic messaging: a technical standard for record retention would be defined, and then "provide in legislation that records kept in accordance with such a standard would satisfy statutory record retention requirements"[157].

Apart from the general requirements outlined above, there are no clear and comprehensive statutory rules detailing which data and transmission records should be maintained and in what form. The issue of record-keeping therefore needs to be given explicit consideration within a contractual context.

---

154 Luxembourg Grand-Ducal Regulation of 22 December 1986, Art.3.

155 Galtung, op.cit. supra n.97, at p34.

156 "Microfilm as documentary evidence", CAN-72.11-79. In the UK, there is a BSI Standard, No.6498, "Guide to the preparation of microfilm and other microforms that may be required as evidence", 1991. There is also a draft discussion document (DD206) entitled "Recommendation for the preparation of electronic images (WORM) of documents that may be required as evidence".

157 McCarthy Tétrault, op.cit. supra n.46, at p.17.

5.2.2 Admissibility[158]

Under English law, there exists a complex body of law relating to the forms of evidence that can be used in the event of a dispute going to court. For the purpose of this thesis, the issue will be divided in two: can electronic records be submitted into court to evidence an event; and what value or weight will the court give to such evidence?

The rules of evidence differ significantly between common law and civil law jurisdictions. In common law jurisdictions, the main obstacle to the general admissibility of computer records is the `hearsay rule':

> "It derives from the adversarial nature of legal proceedings in the common law tradition whereby a party proves his case by calling witnesses with personal knowledge of events...A witness without first hand knowledge of the events...cannot be challenged in cross-examination in this way and so such evidence..is generally excluded."[159]

Whether the computer records fall under this rule depends "on the content of the computer record, the reason for using it in evidence and the way it was compiled"[160]. The main situations under which computer records avoid the hearsay rule are:

- where the records have been classified as `real evidence'; for example, where computers are operating in a mechanistic way, as automatic recording systems or simply as calculating tools[161];
- where the record is produced simply to show that a statement was made, not whether it is true;
- or where the parties to the dispute agree to allow the use of such evidence[162].

Where computer records are considered to fall under the hearsay rule, English law has made special additional provisions to allow for computer records to be admitted[163]. The Civil Evidence Act 1968, Section 5 states:

---

158 See generally, Cross, R., and C. Tapper, *Cross on Evidence* (6th ed.), London, 1985; and Bender, D., *Computer Law*, Volume 3: `Litigation', Matthew Bender, New York, 1991.

159 Bradgate R., "Evidential Issues of EDI", p.12, in Walden, op.cit. supra n.35. See also Amory, B.E. and Yves Poullet, "Computers in the law of evidence - a comparative approach in civil and common law systems", pp.114-124, Computer Law & Practice, March/April 1987.

160 Bradgate R., "The evidential status of computer output and communications", p142, Computer Law & Practice, Vol.6, No.5, May-June 1990.

161 See *The Statute of Liberty* [1968] 2 All ER 195 and *Castle v Cross* [1984] Crim.L.R. 682. In *Sophocleous v Ringer* [1988] R.T.R. 52, the courts held that where a computer was used as a tool to facilitate analysis, then the hearsay conditions did not apply, see below.

162 Civil Evidence Act 1968, s.1(1). See also Chapter 6, at 6.3.3.

163 The general hearsay provisions of the Civil Evidence Act 1968 are contained in sections 2 and 4. It is uncertain whether the conditions of s.5 apply to all computer evidence or only when admitted as hearsay; the latter case is true in criminal evidence, see *R v Spiby*, [1990] The Times, 16 March. For a further discussion on this point see the Reed, op.cit. supra

"In any civil proceedings a statement contained in a document produced by a computer shall...be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible..."

However, only if the following conditions are satisfied:

"1. The document was prepared during a period over which the computer was regularly used to process information for the purposes of any activities regularly carried on over that period.

2. Information of the kind contained in the document, or from which it is derived, was over that period regularly supplied to the computer in the ordinary course of those activities.

3. Throughout the period the computer was operating properly or, if not, the reason for any malfunction or closedown was not such as to affect the accuracy of the document.

4. The information contained in the document reproduces or is derived from information supplied to the computer in the ordinary course of the activities for which it is used."[164]

To satisfy the court that these conditions have been met, it is necessary to obtain either oral testimony or, in the vast majority of cases, a signed statement from the person that occupies "a responsible position in relation to the management of the activities for the purposes of which the computer was used"[165].

Section 5(3) of the Civil Evidence Act 1968, includes the use of `a combination of computers' and `different computers acting in succession'. This would seem to extend the provisions to the use of records produced and maintained by the value-added networks providers[166].

These requirements were laid down when computer technology was at an early stage of development, based on large mainframe processors, and therefore the conditions appear as potentially stringent obligations, as well as slightly irrelevant. The conditions, for example,

---

n.2, at p.91-100; Tapper, C., *Computer Law*, at Chapter 9, (4th ed.), Longman 1989 and Miller, C., "Proving the transaction took place", pp. 55-83, in Proceedings of `Legal, Contractual, Responsibility & Evidential Issues in EDI, EFT, EM, Fax & Telex Communications', London, 20 February 1992.

164 Bradgate R., op.cit. supra n.160, at p.17.

165 CEA, s.5(4). See also Order 38, Rule 25 of the Rules of the Supreme Court, Civil Evidence Act Notice; see generally Style C., and C. Hollander, *Documentary Evidence*, Longman, 1991.

166 Wheble, B.S., "Creating Legal Relationships with Trading Partners", p.131, in Gifkin, M., and D. Hitchcock, *The EDI Handbook*, Online Publications, Middlesex, 1988.

only have to be satisfied at the time the record is produced, not when the information was recorded, which seems a mistaken viewpoint based on the well known premise: `garbage in, garbage out'. The conditions also fail "to address issues which might be considered to be of fundamental importance, such as the security of the system"[167]; and indeed, the terminology only seems to cover computer hardware, not the software involved[168].

Overall, commentators have noted that the draftsman of the Civil Evidence Act 1968 would seem to have confused issues concerning the weight that should be given to computer evidence, with that of its admissibility to court[169]. It is feared, that such a situation could "lead to erroneous decisions and act as a brake on the introduction of new technology"[170]. It could also mean the introduction of over-complex audit practices by companies wishing to ensure that the court will accept the authenticity of their records. Some commentators have even called for computer evidence to be no longer treated as `hearsay'; replacing such controls with:

> "guidelines and codes of practice (perhaps eventually having legally enforceable weight) aimed at ensuring an objectively high standard of computer reliability and security"[171].

It should be noted, however, in spite of these legislative requirements and uncertainties, the courts have stated that in "the absence of evidence to the contrary, the courts will presume that [mechanical instruments] were in order at the material time"[172].

In the event of a dispute actually reaching court, the parties to the dispute are required to give mutual discovery of all documents relevant to the dispute[173]. This process usually means that the parties agree on the submission of evidence in advance without the need to follow any formalities outlined above. Indeed, despite the academic controversy that

---

167 Bradgate, op.cit. supra n.161, at p145.

168 The Act defines a `computer' as "any device for storing and processing information", at s.5(6).

169 For example, see Bradgate, op.cit. supra n.160?; Castell, Dr S., `The APPEAL Report', Eclipse Publications 1991; Silverleaf, M., `Evidence', Chapter 9, in Computer Law (Ed. Reed), Blackstone Press, 1990; Tapper, `Evidence', Chapter 11, in Encyclopedia of information Technology Law, Sweet & Maxwell, 1990.

170 Reed, C., "The admissibility and authentication of computer evidence - a confusion of issues", p15, The Computer Law and Security Report, Vol.6, No.2, 1990. See also *R v Pettigrew* [1980] 71 Cr.App.R.39.

171 Castell, Dr S., "EDI evidential requirements: is EDI `legally reliable'?", p98, Proceedings of the EDI and the Law Conference, London, July 1991. Chris Reed in his response to the Law Commission paper states that "Published standards for the authentication of computer documents, validated under legislation, would reduce this uncertainty [in the CEA 68] to an acceptable level".

172 *Phipson on Evidence* [13th Ed., 1982, p.209], quoted with approval in *R v Spiby*, The Times, 16th March 1990. See also *R v Governor of Pentonville Prison, ex parte Osman* [1990] 1 WLR 277 at 306, which states that where a large computer printout contains no internal evidence of error, it may be inferred that the the machine was operating properly.

173 See further Armstrong, N., "The Disclosure of Computerised Evidence in Civil Proceedings", p.3-5, Applied Computer and Communications Law, Vol.8, No.10, 1991, and Tapper, op.cit. supra n.164, at Chapter 10.

surrounds Section 5 of the Civil Evidence Act, "...its construction has attracted remarkably little judicial attention."[174]

In recent years, the provisions of the Civil Evidence Act 1968 have come under increasing criticism for being unnecessary and out-moded for current technology. The Law Commission is currently considering recommendations to alter the legislation to more accurately reflect the position of computers in modern business[175].

In computer crime cases, the admissibility of computer evidence is subject to section 69 of the Police and Criminal Evidence Act 1984[176] and sections 23 and 24 of the Criminal Justice Act 1988[177]. The Act contains similar requirements to those in civil proceedings.

An additional potential obstacle to the admissibility of computer evidence, in common law systems, is the `best evidence' rule, whereby a party should submit to court the original evidential document rather than a copy. This can obviously cause problems where information is electronically recorded, since any printout will necessarily be a copy of the original.

The UK courts have held that films, tapes and video recordings are not to be regarded as documents for the purpose of the `best evidence' rule, since "they are by their nature reliable"[178]. This interpretation could be applied to computer records, although some commentators have noted that where a document has undergone processing, as well as recording, it will not apply[179]. Fortunately, the UK courts have also stated that the `best evidence' rule is not a requirement where the original is either lost, or "its production is physically impossible or extremely inconvenient"[180].

---

174 Tapper, op.cit. supra n.170, at p.11021.

175 "The Hearsay Rule in Civil Proceedings", pp72-76, The Law Commission, Consultation Paper No. 117, HMSO (London, 1991). The recent poll tax case, *Camden LBC v Hobson* (Times 28 January 1992), has given added strength to the calls for reform; see Bradgate, R., "The Evidential Status of Computer Output: Confusion compounded", pp.1-4, Applied Computer and Communications Law, Vol.9, No.2, February 1992. The Local Government Finance Act 1992, s.13A, introduced procedures for the admissibility of computer records into Magistrates courts.

176 See Bradgate, ibid.

177 See *R v Harper; R v Minors* [1989] 2 All ER 208. In *R v Spiby*, [1990] The Times, 16 March, the courts stated that the admissibility conditions of s.69 do not apply where the computer records are held to be `real'.

178 *Kajala v Noble* [1982] 75 Cr.App.R.149, which involved video tape; see also *Buxton v Cumming* (1927) 71 Sol.Jo 232, involving a dictaphone record, and *R v Senat* (1968) 52 Cr. App. Rep. 282, involving taped recordings of telephone conversations.

179 Amory, op.cit. supra n.160., at p.117. However, Reed, op.cit. n.2, at p.92, states: "It is probable that computer-stored copies will be treated in a similar fashion" as films and videos.

180 Reed, C., "Authenticating Electronic Mail Messages - Some evidential problems", p652, Modern Law Review, Vol.52, September 1989. See also *Brewster v Sewell* [1820] 3 B&Ald 296; *Owner v Beehive Spinning Co.* [1914] 1 KB 105 and *Lucas v William & Sons* [1982] 2 QB 113, p.116, CA per Lord Escher, MR.

In the US, electronic records are not required to fulfil any additional conditions for admissibility, rather they are treated as `business records', which are excluded from the hearsay rule as long as they were

> "...kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness."[181]

The courts have not been prepared to exclude electronic records simply because alterations are theoretically undetectable.[182] Although, conversely, some elements of the US judiciary has also reflected public concerned regarding the reliability of computer records:

> "As one of the many who have received computerised bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of Holy Writ."[183]

Civil law judicial systems tend to have a much more straightforward evidential system, arising out of the inquisitorial nature of such systems:

> "the problem does not arise....in relation to admissibility before the courts and tribunals, but to satisfying legal requirements concerning on the one hand the storage of documents and on the other the conclusion of transactions"[184]

The vast majority of such jurisdictions allow all forms of relevant evidence to be admitted, leaving the court with the task of assigning such evidence an appropriate weight, according to the circumstances[185]. A few civil law countries, however, such as Venezuela, have drafted an exhaustive list of the types of evidence which are admissible in court, and therefore, computer records require explicit recognition before being acceptable.

Such differences in approach to computer evidence has been seen by international organisations as a potential obstacle to the adoption of information technology[186]. In 1985, a

---

181 Federal Rules of Evidence, Rule 803(6) - Records of regularly conducted activity.

182 See *US v Vela 673 F 2d 86* (1982) and US v Sanders 749 F 2d 195 (1984), quoted in Reed, op.cit. supra n.181, at p15.

183 *Perma Research and Development v Singer Co.*, 452, F.2d 111 [1976], dissenting opinion of Judge Van Graafeiland.

184 Amory, op.cit. supra n.160, at 117.

185 Eg. Norwegian Civil Procedures Act, s.183 states: "When nothing else is provided by law, it is up to the court to determine after an assessment of the whole procedure and the line of argument, what facts are to be used as a basis for the judicial decision". This covers both issues of admissibility and value.

186 See section 5.4.1 below.

UN Commission on International Trade Law (UNCITRAL) report was published, entitled: `The legal value of computer records'. It surveyed all Member States, and recorded that:

> "Almost all of the countries that replied to the questionnaire appeared to have legal rules which were at least adequate to permit the use of computer evidence and to permit the court to make the evaluation necessary to determine the proper weight to be given to the data"[187]

Despite this conclusion, in 1981 the Council of Europe passed a Recommendation calling for harmonisation of evidential rules with respect to the admissibility of computer records[188]. The Recommendation calls on Member States to introduce rules for the admissibility of electronic records and limit requirements for the storage of records to a maximum of ten years. Some countries, such as France[189] and Luxembourg[190], have revised their evidential rules to remove any unnecessary obstacles to the use of computer records.

Overall, however, getting computer records submitted as evidence in court is only the first aspect of the evidential requirements companies need to address in a data security policy; getting the court to accept the contents as adequate proof, or a good record, is perhaps an even more important consideration.

5.2.3 Integrity and Authentication

> "Au-then+tic *adj* 1. of undisputed origin or authorship; genuine"
> "In+teg+ri.ty *n* 2. the quality of being unimpaired, soundness"[191]

Electronic records and messages need, both commercially and legally, to have integrity and to be authentic. The former relates to the content of the message and whether it has been altered, eg. what if the EDI message accidentally orders 5000 rather than 500 widgets. The

---

187 A/CN.9/265, p.21, presented to the 18th session of UNCITRAL in Vienna.

188 Recommendation R(81) 20, Information Bulletin on legal activities within the Council of Europe and in Member States, no.13, September 1982.

189 Article 109 of the Commercial Code, as amended by Law No.575 of 1980: Commercial legal instruments can be evidenced `por tous moyens'.

190 Article 1348 of Civil Code, as amended by the Grand-Ducal Regulation of 22 December 1986. Article 1 states:

"The computer-stored information must:

(a) be an accurate and durable reproduction or recording of the original document or information forming the basis of the recording (The concept of `durable' used here can be applied to any indelible reproduction of the original and any recording which entails an irreversible modification of the input medium.);
(b) be recorded in a systematic manner with no omissions;
(c) be recorded in concordance with the working instructions which have been preserved for the same amount of time as the reproductions and recordings;
(d) be carefully preserved in a systematic way, and protected against any alteration."

191 Collins dictionary. "Authentication refers to the establishment or verification of a claimed identity", ISO 7498-2-1 988(E) § 3.3.8.

latter is comprised of two related elements: can it be shown that a message came from the purported sender; and does the means of authentication satisfy any statutory requirements, such as for a `signature'[192].

Maintaining message integrity within a electronic messaging system depends primarily on technical means[193]; for example, `expert systems' could be used to interrogate messages, before they enter business-critical applications (eg. sales ledger), to ensure that the message falls within certain pre-defined, acceptable parameters. However, in addition, the parties could agree on contractually-enforceable procedures, whereby messages will be manually checked for various levels of accuracy before they are accepted.

It has been suggested that the development of an effective legal framework for the protection of electronic records, under criminal law, such as the UK Computer Misuse Act 1990[194], can also lead to electronic records being trusted to a higher degree, and therefore giving them greater legal value and integrity, both in commerce and possibly in the courts[195].

Both English law's civil and criminal evidential statutes contain provisions concerned with how the court should judge the weight, or probative value, of the evidence. The Police and Criminal Evidence Act 1984 states that:

> "In estimating the weight, if any, to be attached to a statement regard shall be had to...in particular -
> (a) to the question whether or not the information...was supplied to the relevant computer...contemporaneously with the occurrence or existence of the facts...; and
> (b) to the question whether or not the person concerned with the supply of information...had any incentive to conceal or misrepresent the facts."[196]

Another aspect of data integrity is the circumstances under which the evidence was produced. Obviously, when a party is already in dispute with another party, they may have a particular incentive to alter the relevant records prior to their submission to court[197]. However, if such an action is feared by the other party, and that party can convince the court that such a threat is real, the court could issue an appropriate restrictive legal instrument, such as an Anton Piller order. An Anton Piller order permits the party taking the legal action

---

[192] This issue has been considered in section 5.2.3. above.

[193] See Chapter 2, at 2.3.3.

[194] See Chapter 3. at 3.4.3.3.

[195] Lindberg, op.cit. supra n.26, at p.34.

[196] Schedule 3, Part II: Provisions Supplementary to Section 69, at 11. See also the Civil Evidence Act 1968, at s.6(3)(c).

[197] For a discussion of the impact of pre-trial procedure on electronic records, see Armstrong, op.cit. supra n.174.

to enter the premises of the other party, under supervision of a court official (often plaintiffs solicitor!), to seize any relevant documents etc. that could be destroyed or altered. The use of such a legal instrument would seem particularly appropriate in an electronic environment[198].

The traditional means by which a message or document is authenticated is through the use of a signature. In terms of the adoption of data communications, authentication can be required for two separate purposes:

- To fulfil a requirement for notice `under the hand of' or `signed'. As discussed in Section 5.2.3, electronic signatures should be accepted by the courts as satisfying this requirement; and

- providing evidence that a message originated from a particular place/individual[199].

With regard to the latter issue, the Criminal Justice Act 1988 allows parties to authenticate documents in any manner approved by the courts[200].

Various types of electronic authentication exist, or are under development. Currently, the most common forms used are passwords or PIN systems[201]. In the financial sector, the banks have long relied upon the use of `test keys' to authenticate funds transfers carried out via telex[202]. In the future, once they become commercially viable, the development of biometric techniques[203] should provide for extremely high levels of authentication.

More recently, the use of encryption techniques has been adopted to enhance the security of electronic signatures. Encryption systems can be distinguished into symmetric, such as DES[204], and asymmetric forms, such as RSA public key/private key encryption system. The

---

198 See *Gates v Swift* [1981] F.S.R. 57 & [1982] R.P.C. 339. However, there has recently been considerable criticism of the use of such orders: "Anton Piller powers are draconian in nature and there is a danger of oppression. Salutory lessons have been learned from excessive enthusiasm (see *Lock International Plc v Beswick* [1989], 1 WLR 1268).", paper given by Hollander, C., `Interlocutory applications for discovery', Conference, London, 6 Dec., 1991.

199 With some Customs Authorities, contracts for the use of electronic submissions state that in the event of a dispute, the onus of proof is on the authorised user to establish that they did not transmit a document using the electronic signature; quoted in Sarson, op.cit. supra n.100, at p.127.

200 CJA, at s.31.

201 See also the development of `dynamic' passwords techniques, which change after each use, based on Smart Cards: Caelli, W., D. Longley, and M. Shain, *Information Security for Managers*, at p.235, Macmillan Stockton Press, 1989; and De Soete, M., "Smart Cards and their applications", pp.147-154, Proceedings of *Compsec 91*, London, 30 Oct.- 1 Nov., 1991. The National Westminister Bank's `Bankline Interchange', electronic trade payment service, controls access and authorisation via a smart card.

202 The `test key' is a numerical representation of a pre-agreed set of numbers combined with a portion of the message content. The recipient is able to compare the received key with its own recomputed version for any alterations.

203 Six alternative access control techniques are currently being developed: Retinal scans, thumbprint, hand geometry, voice, signature, keystoke dynamics. See Castell, op.cit. supra n.172, at p.97.

204 Data Encryption Standard, originating in the US, its use is restricted in other countries. See further Chapter 2, at 2.3.3.

latter method is considered to provide for higher levels of authentication, since they prevent the signature being repudiated, ie. the message could only have come from the sender as `signed'. Symmetric cryptosystems can not provide for proof of origin and non-repudiation unless used in conjunction with a trusted third party[205].

The use of technical security mechanisms can have an important impact on the legal requirement for a `signature', since, together with certain associated procedures, they can replicate the functions of traditional hand-written signatures[206]. The SeaDocs scheme[207], for example, required that electronic messages fulfil three tests before they are accepted as adequate authentication:

> "(i) each party's message must be confirmed by at least one or more messages,
> (ii) messages are re-filed to the presumed sender and must be reacknowledged, and
> (iii) each message has a header code which is unique to sender and message as it must contain an element from the prior sender and from the computer acknowledgement message"[208]

One issue that has been raised within an UNCITRAL report, is whether legislation which permits authentication electronically should:

> "..require evidence of conformity with an applicable EDI protocol, at least as a condition of attracting a presumption of authenticity, the onus of proof being shifted to the party asserting the authenticity of the message in cases where the requirements of the protocol are not satisfied."[209]

Overall, the use and status of electronic techniques has yet to be accepted by the courts[210]. However, initially, the sophistication of the adopted authentication technique will primarily be

---

205 See further Baum, Michael S., Henry H. Perritt, JR., *Electronic Contracting, Publishing and EDI Law*, Chapter 4-5, Wiley Law Publications, New York, 1991; and Chamoux, F., "The Electronic Notary", pp.149-150, Tedis Legal Workshop, Brussels, June 19-20, 1989.

206 The security services required in an EDI environment have been identified as the following: user identification, content integrity, non-repudiation of origin, non-repudiation of delivery and content confidentiality. See `A proposal concerning the use of Digital Signatures in EDIFACT': A report prepared by Cryptomathica/s, 29 November, 1990.

207 See 5.2.5.1 above.

208 Urbach, A., op.cit. supra n.106.

209 `Electronic data Interchange: Preliminary study of legal issues related to the formation of contracts by electronic means', A/CN.9/333, 18 May. 1990, at p.15, para.59.

210 The Home Office has recently proposed the use of a `digital signature' for authenticating information exchanged with Magistrates' Courts; letter to EDIA Legal Advisory Group, 19/2/1992. Such developments will inevitably influence the courts' attitude to the acceptability of electronic signatures. See also the American Bar Association, `Security Techniques in Electronic Transactions' (Draft), proposed ABA policy. The paper is intended to contribute to the legal standing of electronic transactions, by ensuring "wide legislative and judicial recognition that properly secured electronic communications satisfy traditional legal indicia of reliability..", at 1.

a commercial decision based on the value of the information being communicated, against the cost of using certain forms of electronic signature[211].

5.2.4 Comment

> "Reliability in the legal context is something that needs to be addressed by software and hardware engineers when designing and implementing systems."[212]

The purpose of this section has been to review the evidential issues that companies need to address when operating in an electronic communications environment. As the quote indicates, to achieve legal security, companies need to ensure that such requirements are incorporated during the implementation of such systems.

Achieving `legal reliability' will also allow companies to fully exploit the efficiencies of data communications. Of the survey respondents[213], a third stated that they maintained a paper back-up as part of their security procedures, not to satisfy statutory record-keeping requirements. Such continued reliance of paper will represent an increasingly significant opportunity cost to companies, as data communications pervades a wider range of business activities. As data user experience matures, possibly assisted by assurances from judicial decisions, then the desire to maintain a paper back-up can be expected to recede.

In the event of a dispute, the issue of system `reliability' could be the critical aspect of a case, therefore, ensuring reliability during implementation should greatly assist the company in proving its claim. As noted, with regard to the rule on admissibility, the company will need to have identifiable persons who are able to certify, or give oral testimony, regarding the operation of the system. The degree of expertise that should be available to a company will obviously vary according to the importance of the records in question:

> "Virtually every device will involve the person who made it, the persons who calibrated, programmed or set it up...and the person who uses or observes the device. In any particular case, how many of these people it is appropriate to call must depend upon the facts of, and the issues raised and concessions made in that case."[214]

---

211 See further Chapter 6, at 6.3.3 `Authentication'.

212 Miller, C., "Computer-generated evidence - implications for the corporate computer user, Part 1", p178-184, Computer Law & Practice, Vol.6, No.6, 1990.

213 See Appendix B3.

214 *R v Wood* [1982] 76 Cr. App.Rep. 23.

Where record keeping provisions originate in legislation or regulation, then it is usually the case that companies can not move to a total electronic system without the approval, and possibly audit, by the appropriate regulatory authority. However, even where this is not the case, comprehensive record keeping should be an integral aspect of general commercial security. Indeed, the use of electronic messaging systems should enhance a company's ability to maintain full and accurate records.

> "...it is clear that the existence of an international economy based on transborder data flow makes it necessary for us to consider the need for an international law of evidence in the computer field."[215]

The differences in approach to electronic records taken by each legal jurisdiction can be an important issue in a dispute, for example, where trading partners communicating between different countries, agree to use the archive records of their mutual network provider, based in a third country . Indeed, evidential issues may be an important factor in a company choosing to contract under a particular national law[216].

---

215 Amory, op.cit. supra n.160, at p122.

216 See the discussion on `conflicts of law' issues in Chapter 6, at 6.1.2.

Chapter 6 **CONTRACT LAW**

6.1 Contractual relationships

As discussed already in this thesis, companies concerned with the legal aspects of information security will find scant assistance in the legislative framework. In many cases, relevant legislation either does not exist; the provisions are drafted in very general terms, or the legislation is couched in terms that does not seem to enable the adoption of new techniques. This section considers how traditional contractual agreements can be used by organisations to establish detailed data security procedures for their international data communication activities.

Contractual relationships form a specific legal framework, separate from, but complementary to, the legislative framework. It has been estimated, for example, that ten different contracts "directly underpin the provision and use of an EDI network service"[1], such as the contract for

[1] `Security in Open Systems' Report, prepared at the request of the European Commission for SOGITS (Senior Officials Group Information Technologies Standardization); quoted in Troye, A., "European Issues", paper presented at

the provision of the communications software. However, it is beyond the scope of this thesis to consider the whole range of contracts impacting on the use of data communications[2].

In some cases, contracts may be directly linked to, and reinforce, a particular statutory security requirement. In the area of data protection, as discussed in Chapter 4, the use of international communication networks can enable national legislation to be circumvented. This chapter will consider the nature and suitability of contractual provisions to ensure that the protection provided under such legislation can be extended to cover the use of the data in those countries that lack relevant provisions. Contractual compliance has also been adopted by certain regulatory authorities, such as Customs Authorities who have permitted parties to submit relevant declarations electronically after they have agreed by contract to the conditions governing such submissions[3].

Two other forms of data communications-related contracts are analysed in this chapter and should be seen as central to establishing `commercially reasonable legal security'. The first, communication contracts, are a completely unique form of contract between trading partners and are designed to tackle the legal security issues arising from the communication technique itself; while the second, network provider agreements, concerns the contractual form for the provision of value-added data communication services[4].

6.1.1 The form of contract

There are two main contractual formats by which data communication legal security issues could be dealt with, according to the nature of the relationship between the data communication issues and the underlying commercial agreement. The first methodology, would be to amend existing commercial agreements; the second, would be to draft a separate agreement. The chosen option will be determined by a range of business considerations, not least the impact that any new conditions could have on existing business relationships.

The first option can be achieved either:

EDI'90, London, Oct. 30-Nov. 1, 1990. Katus, Sergej, distinguishes three categories of contract related to EDI; see "Three Types of EDI Contracts", pp.89-94, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

[2] However, see for example: Tapper, C., *Computer Law* (4th edition), Longman 1989; Reed, C. (ed.), *Computer Law*, Blackstone/London 1990; Bigelow, R.P., *Computer Contracts: Negotiating and Drafting*, Volume 1-2, Matthew Bender, New York, 1990.

[3] UNCITRAL report, A/CN.9/265, at p.119.

[4] The `value-added' qualification (see Chapter 2, at 2.2.2) therefore excludes the consideration of contracts for leased lines and other such basic communication links, which are traditonally provided by the national PTT.

(i) through the insertion of new clauses into the standard contract;
(ii) issuing a `deed of variation' to the contract[5].
(iii) the adoption of data communication-specific requirements in a schedule/appendix to the main contract.

Solution (i) would seem the least suitable particularly bearing in mind the incremental way data communications tends to be adopted with existing trading partners. In addition, since data communications is usually established between existing trading partners, then an underlying trading contract will already be in place.

Solution (ii) is a legal solution which is akin to the use of a separate agreements, described below, due to its distinctive contractual nature, but is still bundled in with the underlying commercial contract for goods and services. The cost involved in drafting a separate agreement is the usual reason why parties adopt this technique[6].

The adoption of data communication-specific terms and conditions, or a check-list of good communication business practices, which each party agrees to abide by, solution (iii), could provide a suitably flexible means of achieving secure data communications. The terms of such a check-list would, however, be closely based around those issues outlined below in relation to a separate agreement[7].

The second major option is the use of a separate contractual agreement, governing the use of electronic messaging as the means of business communication. Distinguishing the two forms of agreement has a number of practical advantages over making additions/alterations to the existing commercial agreements:

- it allows the communication procedures to be agreed between the parties without the interference of the commercial pressures that arise out of the underlying commercial relationship;
- it enables the parties to clearly distinguish the issues that arise through the use of data communications from those responsibilities and obligations that arise through the trading relationship;
- in the event of a dispute arising over the use of the communication medium, it enables resolution with less chance of it impacting on the underlying customer relationship;

---

[5] This is commonly described as a `supplemental deed' when the additional terms are completely new issues, rather than variations.

[6] For certain types of contract, eg. the sale of land, the drafting of a separate agreement could attract additional stamp duty.

[7] See the UNCID Rules, ICC Document No.452 (1988), at section 6.3.1. below. Such a code of conduct could be incorporated as an appendix to the main agreement.

- a separate agreement can be drafted that covers all existing and future commercial agreements;
- data communications are designed to facilitate trade, however, inclusion of communication security issues into the underlying commercial contract could involve lengthy re-negotiations, eg. over standard terms and conditions;
- security concerns should be shared rather than reflecting the relative bargaining strengths of the parties.

Where the sale and exchange of personal data is the central substance of the contract, then data protection issues, such as communication notification[8], will be closely related to the nature of the commercial deal. Therefore, it would seem more suitable to incorporate the data protection provisions into the main contract.

For agreements designed to deal specifically with the consequences of establishing data communications between trading partners, rather then the nature of the commercial deal itself, the second option would seem to be the most appropriate.

6.1.2 **Private international law**: `the conflict of laws'[9]

Where a commercial relationship exists between companies situated in different legal jurisdictions, it is important that the parties know under which national law any contracts will be judicially considered, in the event of a dispute. The final jurisdiction determines, not only the applicable law[10] and regulations, but may also introduce any relevant customary practice that might exist in the industry[11].

The issue of which national law applies in an international commercial dispute will usually only arise where the parties to the contract have failed to include an explicit jurisdictional clause in their trading contract; or when trading is done purely upon the exchange of each parties' standard trading documentation, including their respective terms and conditions (ie. the `battle of the forms' scenario[12]); or the dispute involves a third party, with whom no contract exists.

---

[8] See Chapter 4, at 4.3.5.

[9] See generally, Dicey & Morris, *The Conflict of Laws* (11th ed.), Stevens, London, 1987.

[10] Eg. in the UK, the Civil Jurisdiction and Judgements Act 1982, implementing the Convention on jurisdiction and the enforcement of judgements in civil and commercial matters, signed at Brussels on 27th September 1968 (including the Protocol on the interpretation of the 1968 Convention by the European Court, signed at Luxembourg on 3rd June 1971).

[11] Eg. a particular national trade association might have adopted the UNCID rules as the basis upon which their members will exchange data.

[12] See Bradgate, R., and N. Savage, *Commercial Law*, at p.22-23, Butterworths, 1991.

Conflict of law issues are not altered by the use of data communications, they are the same for any long-distance contract, except to the extent in which the range and complexity of reconciling the potential jurisdictions can increase when the communication networks are international:

> "When an electronic message is generated in country A, switched in country B and C, transits country E, F, G and H, processed in country I and J, stored in country K and involves entities residing in or operating in yet other countries, it is debatable whether existing choice of law and conflict of law doctrines are adequate. What law applies to data processing carried out by computer aboard a synchronous orbit satellite?"[13]

One author has suggested that, where the case involves data protection legislation, the preferred law should be the `law of the data subject's habitual residence'[14]. However, the data user's place of residence has also been seen as the relevant jurisdiction[15]. In the `Explanatory Memorandum' to the OECD Guidelines, although the problem of jurisdiction is recognised, no answer is suggested, except a call that:

> "Member countries should work towards the development of principles, domestic and international, to govern the applicable law...."[16]

There appears to be only one recorded case where an international data flow dispute was decided on the basis on private international law. In this case, it is reported that the relevant court applied the law of the state of origin, where the data was collected, which is likely to be the data subject's residence[17].

With regard to international credit transfers, usually made via international electronic funds transfer networks[18], UNCITRAL has recently drafted a model law, which includes a `conflict of laws' provision that states:

> "...in the absence of agreement, the law of the State of the receiving bank shall apply"[19]

---

13 "Testimony" of William L. Fishman, US Senate, Banking Committee, Sub-Committee on International Finance and Monetary Policy, 9 November 1981, mimeo., p.10-11; quoted in Sauvant, K P, *International Transactions in Services: The Politics of Transborder Data Flows*, The Atwater Series on the World Information Economy No 1, Westview Press/London, at p.164.

14 Lowry, Houston Putnam., "Transborder Data Flow: Public and Private International Law Aspects", Houston Journal of International Law, vol.6 part 2 (1984). See also Rigaux, "La loi applicable a la protection des indivudues a l'egard du traitement de donnees a caractere personnel", p.443, Revue Critique de Droit International Prive, 1980.

15 Hondius, F.W., "Data Law in Europe", p.109, 16 Stanford Journal of International Law, 1980.

16 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, 1981, at p.12.

17 Noted in International Bureau of Informatics (IBI), First Meeting of the International Working Group on Data Protection and International Law, May 25-26, 1981, TDF 104 (Summary Record).

18 Eg. the SWIFT network; see generally, Reed, C, *Electronic Finance Law*, Woodhead Faulkner, 1991.

However, in the absence of prior agreement, the rule of applicable English law, relevant to international data communications, is that the jurisdiction will be the place where contractual acceptance of the offer was received by the offeree[20].

6.1.3 Comment

There are two major legal limitations to the use of contracts to establish legal security for the use of data communication, in the absence of statutory provision: the express provisions of the legislation and principle of `privity of contract'.

Existing statutory law, based within a paper environment, may not allow parties to contract out of its provisions; for example, doubts have been expressed, concerning:

> "...whether a contractual definition of an original could validly deviate from a statutory provision listing a limited number of circumstances where a copy could be substituted to the normally required original with the same evidential value."[21].

Where a statute's provisions contain an explicit requirement for a paper copy of a document, often as an aspect of consumer protection[22], then the parties will be unable to contract out of such requirements. However, where the terminology simply implies the use of paper documentation based in traditional concepts, then the parties may be able to contractually re-define such requirement or the courts may interpret the provisions widely.

Within English commercial law, the fundamental legal principle of `privity of contract'. There are three elements of this principle:

> "(i) a person cannot enforce rights under a contract to which he is not a party;

---

[19] Article 18, in `Comments on the Draft Model Law on International Credit Transfers - Report of the Secretary-General', 15 May 1991, A/CN.9/346. Following UNCITRAL's Twenty-fourth session, Vienna, 10-28 June 1991, the Commission has adopted the first 15 of 18 proposed articles.

[20] *Brinkibon Ltd. v Stahag Stahl und Stahlwarenhandelsgesellschaft GmbH* [1983] 2 AC 34 (see also Chapter 5, at 5.2.4). In the UK, since 1 April 1991, the Contracts Applicable Law Act 1990 applies. This Act implements the Rome Convention on the law applicable to contractual obligations, opened for signature in Rome on 19th June 1980 (signed by the UK on 7th December 1981). See also the Restatement (Second) of the Foreign Relations Law of the United States, Sec.40: "five principles which should be considered in balancing the interests of conflicting jurisdiction" - (1) the states vital national interest; (2) extent and nature of hardship that would be imposed by inconsistent enforcement; (3) extent to which conduct occurs in the other jurisdiction; (4) nationality and (5) extent to which enforcement action can achieve compliance with the rule prescribed in the state (quoted in Brown, R.W., "Economic and Trade Related Aspects of Transborder Data Flow: Elements of a Code for Transnational Commerce", p.53, Northwestern Journal of International Law and Business, Spring 1984, Vol.6, No.1).

[21] Eg. UNCITRAL report, `Electronic Data Interchange', A/CN.9/350, 15 May 1991, at p.22; and Bensoussan, A., p.20, `La gazette de la télématique et de la communication inter-enterprises', No.11, spring 1991. See also Chapter 5, at 5.2.1.

[22] Eg. The Consumer Credit Act 1974, s.8.

(ii) a person who is not party to a contract cannot have contractual liabilities imposed on him;

(iii) contractual remedies are designed to compensate parties to the contract, not third parties."[23]

In general, the rule of privity means that a contract is not applicable to third parties. Privity of contract could therefore create problems and injustices where the nature of elements of a contract are designed to provide for protection for a third party, such as in a data protection context (see section 6.2 below); or where an open trading environment exists involving multiple parties. English law, both legislative[24] and case law, has over the years created a number of exceptions to this general rule, such as collateral contracts[25], but the rule will apply in the vast majority of commercial relationships.

Over the years, this rule has met with significant criticism within all areas of the legal profession; for example:

> "an anachronistic shortcoming that has for many years been regarded as a reproach to English private law."[26]

Recently, the Law Commission circulated a consultation document in this area, which proposes legislative reform of the rule:

> "a third party should be able to sue on a contract made for his benefit where it is the intention of the contracting parties that he be given enforceable rights.."[27]

Such a reform would bring English commercial law into line with other major trading nations[28].

---

[23] The Law Commission, Consultation Paper No.121, `Privity of Contract: Contracts for the Benefit of Third Parties', p.1, para.1.1 [completed 23 October 1991]. See *Dunlop Pneumatic Tyre Co. Ltdv Selfridge & Co. Ltd* [1915] A.C. 847 and *Beswick v Beswick* [1968] A.C. 58.

[24] Eg. The Bill of Lading Act 1855, s.1.

[25] Eg. *Shanklin Pier Ltd v Detel Products Ltd.* [1951] 2 KB 854, [1951]2 All ER 471 and *Wells (Merstham) Ltd. v Buckland Sand & Silica Ltd.* [1965] 2 Q.B. 170.

[26] Statement by Lord Diplock in *Swain v Law Society* [1983] 1 A.C. 598, at 611.

[27] op.cit. supra n.23, at p.103, para.5.10.

[28] Eg. common law countries: The US second Restatement of Contracts (1981), s.302 (1) and the New Zealand Contracts (Privity) Act 1982, s.4. In civil law countries: French Civil Code, Article 1121 and German Civil Code (Burgerliches Gesetzbuch (BGB), Article 328.

6.2 Data protection contracts

> "The individual...will have to trade some control over information about him in exchange for the services that a record-keeping organisation provides, but both parties to the exchange should participate in setting the terms of the exchange"[29]

The above quote illustrates the concept behind this section, that data subject privacy considerations need to be balanced against the needs/desires of the private sector to collect and communicate data. If this assumption is accepted, as it has been in the UK data protection legislation[30], then contractual agreements could be a particularly apt means of securing international communications involving personal data.

This section is concerned with contractual means by which a company could transfer data to a country without data protection legislation, or a particular form of protection (eg. legal persons), and thereby offer adequate protection for the data subjects and satisfy the concerns of the home country's regulatory authority.

6.2.1 The issues

In Chapter 4, the impact of data protection legislation on the commercial use of data communications was discussed. Provisions have been laid down to regulate various types of data communications, both nationally and internationally, to protect the subject of the data transfer.

Data communications is "an international medium par excellence"[31], and therefore it is technically comparatively easy for companies to avoid national data protection legislation by processing data in so-called `data havens', with no legislation. All national legislation therefore includes provisions to protect against such avoidance[32].

Significant international initiatives have also been established to provide for a level of harmonised protection between countries, and therefore hopefully avoid the need for national restrictions of international data communications, based on privacy grounds. However, despite these international efforts, a number of the major trading nations still lack significant legislative data protection, particularly in the private sector[33].

---

29 Eger, J.M., "Transborder Data Flow", p.50, 24 Datamation, Nov.15, 1978.

30 See Chapter 4, at 4.2.

31 Hondius, F., *Emerging data protection in Europe*, North Holland, Amsterdam, 1975, at p.5.

32 See Chapter 4, at 4.4.1.

33 Eg. the USA and Japan.

Where countries do not have legislation, or indeed where the level of protection is of a different nature (eg. extended to manual data), there is the problem of equivalency: does the country to which the data is to be sent have `equivalent' protection?

This question can be answered in two ways, legally or functionally[34]:

- Does the recipient country have substantive data protection legislation;
- or can data protection be guaranteed through other means?

Where the legislative approach is taken, it is not sufficient to look solely at the legislation, since in most cases the legislation is drafted in vague terms and principles, which are then given flesh by the actions and decisions of the national data protection authority. The requirement for `legislative equivalence' can be a significant obstacle for a company wishing to transfer data to a country without legislation, since there is often scant legal authority upon which to base any assurances[35].

The requirement for `functional equivalence', on the other hand, allows companies to show that equivalent data protection exists in the recipient country, and/or that the real risk to personal data is low, due one, or a combination of alternative forms of control; for example:

- constitutional provisions[36]
- state, province, territorial, or local legislation[37]
- sectoral law[38]
- industry self-regulatory codes[39]
- corporate data protection and security procedures and codes of conduct[40]
- consumer protection measures[41]
- judicial decisions[42]
- consensual arrangements[43]

---

[34] Epperson, Michael G., "Contracts for transnational information services: Securing equivalency of data protection", p163, Harvard International Law Journal, 22, Winter 1981.

[35] See Nugter, A.C.M., *Transborder Flow of Personal Data within the EEC*, No.6 Computer/Law Series, Kluwer/The Netherlands 1990.

[36] When Spain ratified the Council of Europe Convention, they stated that the data protection principles (Chapter 4, at 4.3.5) were quaranteed as a constitutional right. To date they do still not possess specific statutory provisions.

[37] Eg. in Quebec, Canada, the `Access to documents held by public bodies and the Protection of personal information' Act 1982.

[38] Eg. in the US, the Fair Credit Reporting Act 1970 (15 U.S.C.,s.1681).

[39] Eg. in Japan, the `Guidelines on the Protection of Personal Data for Financial Institutions', published in 1988 by the Centre for Financial Industry Information Systems (FISC), Tokyo.

[40] Eg. the Bank of America and IBM, see Appendix A3.

[41] Eg. in the US, the Right to Financial Privacy Act (12 U.S.C.,s.340).

[42] Eg. in Germany, the Constitutional Court Judgement of December 15, 1983, Bundesverfassungsgericht [BVerfG], 65 Entscheidungen des Bundesverfassungsgericht [BVerfGE] 1, which recognised an individual's right of `informational self-determination'.

- adherence to international instruments"[44].

These different concepts of how to evaluate whether a country has `equivalent' data protection, would seem to be reflected in the positions taken between the two major international data protection instruments, the Council of Europe Convention and the OECD Guidelines[45]. Article 12 of the Convention states that the Parties, on the grounds of privacy, can restrict international transfers "except where the regulations of the other Party provide an equivalent protection". This would seem to link the concept of equivalency to the need for regulations, and would suggest that the drafters of the Convention did not envisage the use of contracts to achieve equivalency. The Guidelines, however, simply allow for restrictions on the flow of data where the importing country "provides no equivalent protection", therefore allowing for the use of the alternative forms of control outlined above.

Such a difference can also be found in the United Nations Guidelines on data protection and the European Commission's draft directive[46]. The former requires `comparable' protection, but includes this provision in the section entitled the Principles concerning the minimum guarantees that should be provided in national legislations, therefore, if the protection is not provided in legislation, how can it be regarded as `comparable'? On the other hand, the EEC draft directive simply requires that `adequate' protection exists, with no qualifications.

It would seem, therefore, that the Convention and the UN Guidelines view equivalency in the legal sense; while the OECD Guidelines and the European draft directive embrace the concept of functional equivalency. Currently, within Europe, the Council of Europe Convention is the leading legal instrument in data protection; however, this position can be expected to change when the European Community adopts the draft directive, therefore promoting the `functional' stance. For the purposes of the following discussion, the latter viewpoint, which suggests the possibility of providing for equivalence through contractual means, is adopted.

6.2.2 Draft Terms

Under a contractual approach to data protection equivalence, it is important to be able to prove to the data protection authority (DPA) that two critical factors can be provided for:

---

[43] Eg. in France, the contractual agreement between Fiat France and Fiat Italy; see Chapter 4, at 4.5.1.

[44] ICC "Protection of Personal Data: An International Business View", p.7, Doc. No.373/128, 4 October, 1991.

[45] See Chapter 4, at 4.3.

[46] Ibid.

- The ability of either the data subject, the DPA or the data user transferring the data, to sue the recipient for any abuse that arises; and
- that an effective remedy exists that can be applied in the relevant courts[47].

The literature and practice suggests two approaches to this problem: contract terms and `choice-of-law' provisions.

Contract terms

The contractual approach can be achieved in two ways. The first method involves the parties agreeing to the inclusion of certain procedures and commitments into the contract governing the transfer of data.

In one example of this practice, CNIL, the French DPA, required that a US multinational, that wanted to transfer data between its French and British subsidiaries, should provide for a contract stipulating a number of data protection provisions:

- that the customer had to give consent to the transfer, via a signature at the point of purchase;
- a warranty that the data sent to the UK would be used in France only by the company, or on its behalf;
- that security measures and the names of those persons with access to the database be disclosed to CNIL,
- and that data subjects would have guaranteed access to the information held on them[48].

Under the Austrian data protection legislation, where data is transmitted to a foreign entity for processing, under licence from the Data Protection Commission, then the third party is obliged to evidence that it will fulfil certain requirements:

- after processing, the data must be sent back to the data controller in Austria;
- the data will be passed to a third party only on instruction from the Austrian data controller;
- the data is kept secure from improper access;
- the data processing organisation has a duty to take proper care of the data at all times;
- the data subject has all the usual rights of access, correction and deletion;

---

47 Epperson, op.cit. supra n.34, at p171.

48 quoted in Napier, B.W., "Contractual solutions to the problem of equivalent data protection in transborder data flows", p.20-21, International Computer Law Adviser, September 1990. See also the FIAT case, at Chapter 4, at 4.5.1.

- the Austrian data controller remains responsible in law for failures to comply with the legislation[49].

When considering the award of an data export licence, the Data Protection Commissioner will therefore examine the contract between the data user and the third-party data processor to ensure that such terms have been covered in the agreement[50]. A similar practice is carried out by the Danish data protection authority[51].

One advantage of the contractual approach, is the similarity that data protection provisions can have to those often already included in commercial contracts, such as for computer software licensing. Such similarities should encourage their adoption; for example:

> "7.1 Unless [the sender] shall indicate in writing to the contrary [the recipient] shall be entitled to use the materials once only on the date for the purpose specified by [the sender] at the time of acceptance of his order and using only materials supplied by [the sender].
> 7.2 [The recipient] shall not be entitled to retain a copy, pass on, disclose or otherwise communicate the list or any part thereof data or information extracted or derived therefrom to any addressing bureau, computer bureau or any other third party unless otherwise agreed in writing by [the sender].
> 7.3 [The recipient] covenants that it will use the list for its own use only. [The recipient] shall not without prejudice to the generality of the foregoing analyse, sell, licence, rent or use the list for any other purpose nor shall [the recipient] use the list to identify names from any list maintained by [the recipient] for rental to third parties"[52]

As well as intellectual property licensing, such clauses are also similar to standard confidentiality provisions[53]. However, the limitation of such confidentiality-type provisions is that they only impose negative duties upon the recipient, such as not disclosing certain information; they do not provide for positive obligations, such as subject access rights.

---

[49] The Austrian Act, Bundesgesetz vom 18.Oktober 1978 uber den Schutz personenbezogener Daten; Bundesgesetzblatt 1978, pp.3619 ff (as amended July 1, 1987); at s.19.

[50] See Privacy Laws and Business, p11, no.2, May 1987. See also a Business International Report, 'Transborder Data Flow: Issues, Barriers and Corporate Responses', p.129, New York, 1983.

[51] See Chapter 4, at 4.4.1.

[52] quoted in Napier, op.cit. supra n.48, at p.15, they are taken from the standard terms and conditions for the supply of personal data to an electronic database. The terms are obviously intended to protect the commercial interests of the data owner, in maintaining the integrity and preventing the exploitation of the data, rather than the data subject.

[53] See further Chapter 3, at 3.4.4.2.

Recently, a drafting group within the Council of Europe's Committee of Experts on data protection has circulated, for comment, six draft clauses for inclusion in "a model contract designed to ensure equivalent data protection in the context of transborder data flows"[54].

The clauses are primarily intended for situations where a `Contracting Party' to the Council of Europe Convention receives a request to export personal data to a State which has not legislated for data protection. The clauses are not, however, intended to replace the need for legislation; as stated at a Council of Europe Conference in March 1990:

> "pourraient etre utilisees neanmoins comme palliatif ou complement au cadre juridique de la protection et des flux trans-frontieres des donnes."[55]

The following summarises the issues covered in the model contract:

1. **License granting the right to use data**

   This general license clause provides the licensee with a right to use the data for a specified sum. In similar fashion to software licenses, the licensee's right is limited to exclusive pre-specified purposes[56]. The licensee also warrants that he will abide by certain data processing principles, such as maintaining accurate data[57].

2. **Right of access of the data subjects**

   This clause requires that both parties give the data subject access to his data, for a reasonable fee. The parties also agree to modify/rectify the information where incorrect.

---

54 Council of Europe, "Revised version of proposed clauses for inclusion in a model contract designed to ensure equivalent data protection in the context of transborder data flows", T-PD (91) 8; see also Early, L., "Securing equivalent protection among nations in the context of transborder data flows: a possible role for contract law", pp.10-14, Droit de l'informatique et des telecoms, 1990/4..

55 Stated at the Conference, `Access to public sector information, data protection and computer crime', held by the Commission of the European Communities and the Council of Europe, Luxembourg, 27-28 March, 1990, quoted in Early, ibid., at p.13.

56 It is possible for a collection of personal files to be classified as a `database', particularly when it is traded as a product (see *Express Newspapers Plc v Liverpool Daily Post and Echo* [1985] F.S.R. 306 at 309, Ch.). This would give the licensor copyright protection against use of the database, without need for a contract; see Chapter 3, at 3.4.4.1. Following the recent European software directive (see Dumbill, E., "EC Directive on computer software", pp.210-213, Computer Law & Practice, Vol.7, No.5, 1991), the European Commission is currently drafting a directive covering copyright in databases, to clarify and harmonise the legal protection in this important area.

57 See the discussion on the data protection principles, Chapter 4, at 4.3.5. It has been suggested that this Article should explicitly state that the `principles' are for the benefit of the data subjects; a requirement for giving data subjects' rights of action under US law; see Reidenberg, J.R., "An American solution to TBDF personal data contractual problems", p.12, Privacy Laws and Business, No.19, December 1991.

3. **Liability** (and 4)

A standard form liability clause, whereby the licensee indemnifies the licensor against the consequences of his actions[58].

5. **Arbitration**

> "Any dispute arising out of the implementation of this agreement shall be submitted to the arbitration and the adjudication of an arbitrator. The arbitrator shall be chosen from a list of experts drawn up by the Consultative Committee established under the Council of Europe Convention[59].....In settling any dispute, the arbitrator shall base himself on the general principles of data protection laid down in...the Convention, taking account of any relevant judgement of the European Court of Human Rights."

In the event of a dispute, the use of an arbitration clause is designed to ease the enforcement of the contract, without the deterrence of full-scale legal proceedings. It will also encourage the development of a consistent approach to this issue, through the establishment of a set of precedent case law from experts in the field.

6. **Termination of the Contract**

The licensor reserves the right to terminate the contract, in the event of `bad faith', or following a refusal by the licensee to abide by any specified recommendations with regard to the personal data. Upon notice of termination, the licensee is required to destroy all copies of the data held. A failure to abide by an arbitration decision will also mean the licensee is required to pay a penalty fee to the licensor[60].

The second contractual method for ensuring international data protection is through incorporation, either directly or by reference, of the provisions included in either (a) the national data protection legislation of the exporting country, or (b) one of the international legal instruments. The problem with the latter is that both, the Council of Europe Convention

---

[58] An additional indemnity clause is suggested to cover (a) damages arising from an arbitration decision (see clause 5.); and (b) the actions the licensor can take in the event that the licensee refuses a data subject access.

[59] The Council of Europe's Consultative Committee have also discussed the possibility of drafting a model code of procedure for transborder data flows. Such a code could be incorporated directly, or by reference, into a contract between the sender and recipient of the data. Parties agreeing to transmit data internationally would include in the transfer some form of declaration, which the recipient of the data would be contractually bound to abide by. Such a declaration could include the following information: The name and address of the recipeint; the authorised uses of the data; the unauthorised uses of the data; the recommended storage time for the data, and the recommended appropriate level of security (see Privacy Laws and Business, p3, no.10, May 1989).

[60] Reidenberg, op.cit. supra n.57, at p.13, suggests that this should be expanded to cover awards to data subjects for breaches of obligations by the data recipient.

and the OECD Guidelines, are primarily principle-based and therefore do not necessarily provide for any clearly applicable actions or standards.

Following the inclusion of contractual safeguards, the next issue is whether such contractual provisions can be sufficiently enforceable. The data user exporting the data is unlikely to suffer damage from any breach of such contractual terms and will therefore have little incentive to either police the agreement or sue for any breach[61]. However, as mentioned in Section 6.1 above, under English private law, the primary legal obstacle to any third party, such as a data subject, acting against the importing data user is the rule of `privity of contract', whereby only the parties to a contract can enforce its obligations[62].

Pending possible future legal reform, the `privity of contract' rule could be overcome through the use of two complementary legal procedures:

(a) The law of agency:

A data subject can only take action against a data recipient, for breach of the data protection provisions, where there exists a contractual relationship between the two parties. The law of agency could be one means of establishing that necessary link. In such an arrangement, the domestic data user would be acting as agent for the data subject with respect to the enforcement of the international data protection aspects of the contract.

Such an agency relationship could arise through the courts accepting that, in addition to the commercial contract between the data sender and recipient, there can be implied the existence of a collateral contract between the recipient and the sender, on behalf of the data subject[63]. However, under English law, for an agency relationship to be recognised, the principal (ie. the data subject) has to have given his consent in advance. In a data protection context, such consent might be extremely difficult to ascertain, particularly where the data sender is several steps removed from the relationship under which the data subject initially provided the data.

Therefore, an alternative approach to establishing an agency relationship would be through the provision of an explicit clause in any contract that might exist between the data sender and data subject, such as in certain consumer contracts or employment contracts. This latter

---

61 Epperson, op.cit. supra n.34, at p.171.

62 Under US law, second Restatement of Contracts (1981), s.302 (1), third parties may sue when they are the `intended' beneficiaries of a contract; although the third party (ie. the data subject) needs to be notified of the agreement.

63 See *Re Flavell (1883) 25 Ch D 89, CA*. See generally, Bradgate, op.cit. supra n.12, at pp. 73-137.

option, with respect to consumer contracts, has not however been welcomed by direct marketing organisations, since it is seen as acting as a deterrent to the obtaining of data[64].

(b) Assignment of the right to act:

In this scenario, the exporting data user would assign its rights to sue the data recipient to the data subject or the domestic data protection authority[65]. Such an arrangement is the legal basis upon which factoring agreements operate[66], where the factor is usually given power of attorney to act on behalf of his client against the debtor.

The advantage of assigning the right of action to the data protection authority would be the financial resources available to the DPA, as opposed to those of the data subjects. The incentive upon the data user to adopt such a method would be the potential refusal of permission from the DPA to transfer the data. Alternatively, a clause could be included in the contract stating that in the event that a data subject takes a successful action against the data recipient, then he will recover his costs[67].

Remedies are obviously a critical component in the use of such contractual methods. In the contract between the data subject and the data exporter (eg. consumer contacts), the data exporter could undertake to pay compensation to the data subject if the recipient breached any of the terms.

To protect the data exporter against the consequences of potential legal actions taken by either the data subject or the domestic data protection authority, the data recipient could agree to either repay any damages suffered by the data exporter under an indemnity clause[68], or through the provision of liquidated damages clauses for specific types of breach[69]. The latter option is more problematic due to the need to assess a realistic estimate of the cost of any damage, or potentially have the courts view the clause as a penalty clause. Such a proposition would seem particularly difficult in a data protection context.

---

64 quoted in Napier, op.cit. supra n.48, at p.15.

65 Epperson, op.cit. supra n.34 at p.171.

66 Where a company sells its debts to a third party, know as a factor, to recover, in exchange for a credit advance.

67 Reidenberg, op.cit. supra n.57, at p.13.

68 Napier, op.cit. supra n.48, at p.17.

69 Epperson, op.cit. supra n.34, at p.172 and Reidenberg, op.cit. supra n.57, at p.13.

Choice-of-law

A second element in ensuring `functional equivalency' would be through the adoption of a jurisdictional, or `choice-of-law' clause. Where the contract method is chosen, the jurisdiction provision could mean that any disputes were settled under the data exporters legislation, thereby providing the data subject with some certainty as to his rights.

Alternatively, a contractual provision could state that a US court, for example, should consider disputes over the data protection terms of the contract as being interpreted under the UK Data Protection Act 1984[70]. In such a situation, the DPA of the exporting country could apply for standing to take the action, instead of the data exporter, on the grounds of the express intent of the parties[71]. The remedies that a foreign court would be prepared to enforce would depend on the legislation of the foreign country. Criminal penalties, not present in the foreign jurisdiction, would not be upheld, but civil fines are likely to be[72].

6.2.3 Comment

The use of contractual means to achieve international data protection equivalency is certainly a solution being promoted by industry at the current time[73]. It is recognised that the legislative process is slow enough that it could be many years, if ever, before certain major trading nations introduce appropriate legislation; while significant differences will always exist between the various national approaches to protection. Companies therefore perceive contractual terms as a practical means of providing for data protection.

The widespread adoption of such terms will, however, depend partly on the attitude of the appropriate national data protection authority. At the 13th International Data Protection Commissioners Conference, in Strasbourg, October 1991, the Commissioners' explicitly stated that the use of such contracts should not be accepted as an alternative to legislation[74].

The problem of `legislative equivalency' could be solved between states that have some form of data protection legislation, enforced by a regulatory authority. In such situations, it is

---

[70] See Epperson, op.cit. supra n.34, at p.172-3. Such a solution would not be possible in Germany, where the courts have held that a foreign law should never be applied if a contract is governed by German law; see Hoeren, T., "EDI and Transborder Flow of Personal Data: The perspectives of private international law and data protection", at p.83, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

[71] Ibid., at p.174

[72] Ibid.

[73] See ICC report, op.cit. supra n.44.

[74] Professor Spiros Simitis, Chairman of the EC member states' Data Protection Commissioners' working group; quoted in Privacy Laws & Business, p.1, No.19, December 1991.

possible that the data protection authority of the state with the weaker legislation could agree to cancel a data user's licence/registration, or even impose a fine, for a violation of another state's data protection legislation. This would require legislative provision giving the data protection authority the power to apply such criteria, or it may "necessitate a system of letters rogatory between data inspection boards in different countries"[75].

Alternatively, it could be enshrined within the various international data protection instruments, as a general data protection principle[76], that:

> `data users should ensure that they abide by the privacy provisions of any national jurisdiction to which they transfer, or from which they receive, personal data'.

To be effective, however, it would still require that the international legal instrument be incorporated into national law, in some form.

Within the national commercial-legal framework, general data protection provisions are being adopted in standard trading contracts. The survey of multinationals[77] found that respondents, in all three countries, were including data protection-related clauses in an ever-widening number of contracts, both with suppliers and customers. The German airline Lufthansa, for example, includes data protection clauses in their credit card contract and their employment contracts. Such a clause was not placed in the passenger contract, although passengers are given the right to block the transfer of their data by Lufthansa to third-parties[78].

In terms of the use of data protection contract provisions for international equivalency, none of the respondents had adopted such techniques. Indeed, the only examples in the literature, where contractual provisions have been used, are those initiated by a particular data protection authority, as noted above. This would suggest that, despite the interest shown in such contractual techniques, companies have either:

- not had a practical need for such provisions,
- or do not consider them to be suitable.

---

[75] Gotlieb, A., C. Dalfen and K. Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", pp227-257, The American Journal of International Law, Vol.68, 1974.

[76] See Chapter 4, at 4.3.5.

[77] See generally Appendix A1-3. See also section 6.3 below.

[78] Interview with Dieter Hermsdorf, Data Protection and Security, Deutsche Lufthansa AG; 06/04/89.

Reidenberg, for example, notes that such contract terms would only be workable for point-to-point transfers, such as the FIAT case[79]; while for TDFs passing over a global network, such as ticket reservation systems, such an approach "does not appear viable" because of the need for an extended hierarchy of interlinking agreements[80], particularly where extensive use is made of third-party Network Providers[81].

6.3 Communication agreements

> "any method of communication requires discipline in order to be effective. The discipline is achieved by applying rules of conduct which by their use have become customary or by law have been imposed. Electronic data interchange has not yet been in existence long enough to have acquired in these ways a collection of standard rules of conduct"[82].

`Interchange agreements', `communication agreements' and `trading partner agreements' have all made their appearance over recent years in relation to the regulation of data communications between businesses. Indeed, such agreements represent "the first time we need an agreement on how we communicate!"[83].

Interchange agreements are set-up between users of data communications, and are generally designed to fulfil a number of different functions:

- Enhance the enforceability of EDI transactions;
- reduce confusions and misunderstandings;
- apportion liability;
- define data security obligations;
- and as an educational/implementation tool[84].

Such agreements can also be used as an adhesion contract between a group of users[85], which "can be adhered to by new entrants to the group by simply signing the interchange

---

[79] See Chapter 4, at 4.5.1.

[80] Reidenberg, op.cit. supra n.57, at p.13, Privacy Laws and Business, No.19, December 1991.

[81] See further 6.3 below.

[82] The UK EDI Association's `Explanatory Commentary', p.1, to the Standard Electronic Data Interchange Agreement; see Appendix C2.

[83] Statement by Gill MacMahon, ICI, delegate at `Paperless Trade' Conference, London, 13-14 Feb., 1989.

[84] See generally Baum, Michael S., Henry H. Perritt, JR., *Electronic Contracting, Publishing and EDI Law*, at p.49, Wiley Law Publications, New York, 1991; Shaw, S.N.D., "Drafting an interchange agreement", pp.24-26, Proceedings of the EDI and the Law Conference, London, 4 July, 1991, and Walden, I. and R.N. Savage, "The Legal Problems of Paperless Transactions", p.112, The Journal of Business Law, March 1989.

[85] Eg. industry/trade EDI user groups, such as Odette (motor manufacturers) and Cefic (chemical industry).

agreement"[86]. An interchange agreement could also be used to govern the relationship between such user groups.

The use of such agreements has been particularly prominent among EDI users, and therefore this discussion will focus on these forms of agreement. However, the rationale behind such agreements could extend to other forms of data communications between trading partners[87]. The reason why the concept of using such agreements has arisen primarily in the field of EDI is because a pure EDI communication system should remove the human interface, thereby allowing companies to trade completely automatically. It would seem that it is this critical element, of removing the need for a human interface, that has alerted business to the legal insecurities involved in trading via data communications.

6.3.1 The UNCID Rules

> "codes of conduct will be increasingly used in the international community to deal with problems which countries are unable to solve on a national level."[88]

The work of the international organisations, reviewed in Chapter 5, at 5.4.1, has generally involved identifying the range of obstacles that inhibit the use of data communications in international trade. Such obstacles originate either in national law, international commercial practice or the administrative regulations of public authorities. Their work also recognised that the removal of these obstacles would take several years of co-operation, goodwill and activity, particularly on behalf of governments and administrations. However, in order to enable companies to exploit the opportunities offered by the existing technology, it was recognised that some form of interim commercial/contractual solution was necessary.

An initial project was carried out by the Nordic Legal Committee, under the auspices of the UN/ECE Working Party on Facilitation of International Trade Procedures, and was entitled "Proposal for Uniform Rules for Communication Agreements (UNCA)"[89]. This document provided a draft text for a contract which could be adopted by trading partners who wish to use data communications.

UNCA was composed of twenty-four articles covering questions of application, security, verification, authentication, confirmation, privacy, storage of data, liability, insurance and

---

[86] SITPRO South Africa, `Model Contract Interchange Agreement', p.2,

[87] See the discussion in section 6.3.5.

[88] Waldman, R.J., *Regulating International Business through Codes of Conduct*, American Enterprise Institute for Public Policy Research, 1980.

[89] ECE document TRADE/WP.4/R.300 and in ICC document No.374/1.

interpretation. However, it was decided that the task of drafting a standard communication agreement would be impracticable, "due to the differing requirements of various user groups"[90].

The document therefore recommended that a code of conduct, based on a uniform set of rules, would be a more appropriate solution. It also recommended that the work be passed on to the International Chamber of Commerce (ICC) due to their experience in the drafting of such rules.

Subsequently, the ICC established a special joint committee to consider the issues, which held its first meeting at ICC, Paris, on 16-17 January 1986. Those attending this first meeting included representatives from the CCC, the UNCITRAL Secretariat, ECE, the International Organisation for Standardization (ISO), the UNCTAD Special Programme on Trade Facilitation, the Commission of the European Community (EC), and a number of user group representatives.

This committee, representing all possible interested parties, established its deliberations on five principles, eventually expanded into eleven specific articles. The result of the Committee's work was the `Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission' (UNCID)[91]. The principles state that the rules should:

> "a) aim at facilitating the use of ETDI through the establishment of an agreed code of conduct between parties engaged in such electronic interchange;
>
> b) apply only to the interchange of data and not to the substance of trade data messages transmitted;
>
> c) incorporate the use of ISO and other internationally accepted standards - to avoid confusion;
>
> d) deal with questions of security, verification and confirmation, authentication of the communicating parties, logging and storage of data;

[90] NORDIPRO *Creating Legal Security in Electronic Data Interchange*, p.19, Special Paper No.4, Tano/Oslo 1988.

[91] The `Rules' were approved by the ICC Executive Board and the UN/ECE Trade Facilitation Working Party in September 1987: ICC Document No.452 (1988), and ECE document TRADE/WP.4/R.483. The Articles will be referred to within section 6.3.3. below.

e) establish a focal point for interpretation that might enhance a harmonised international understanding and therefore use of the code."[92]

The rules are not a binding legal instrument, they are intended as a `bridging operation' until national and international legislation and practice are suitably altered to take account of data communications. Nevertheless, UNCID is intended to be viewed as providing for a level of commercial `good practice' to which all organisations will find it prudent to accede. As stated by the Secretary of UNCITRAL:

"once seen by the business and legal communities as stating appropriate rules of conduct, UNCID will undoubtedly acquire a semi-legal status as the standard to which trade partners communicating by EDI should adhere."[93]

Therefore, if UNCID becomes accepted internationally as the basic standard of professional behaviour for trading partners using data communications, it is possible that a court may decide that failure to maintain this standard should be regarded as evidence of `negligence' on behalf of the dissenting party[94]. As part of the process of UNCID becoming an international standard, it has been adopted by the United Nations, as the legal basis for the UN/EDIFACT standard[95].

The UNCID rules have also become a legal instrument through incorporation into interchange agreements, drafted between trading partners, or within industry groups. Such incorporation can occur either through reference or by direct inclusion into the text of the agreement.

At the same time that the UNCID rules were being developed, contractual agreements were being drafted within the various EDI user groups that were being established within Europe, such as ODETTE in the automotive industry and DISH in the shipping industry. Legal committees within these groups drafted agreements to be used by members of the group to govern the use of EDI within the group.

The role of interchange agreements is now gaining increasing recognition within the EDI community. In 1989, the UK EDI Association adopted the Standard Interchange Agreement

---

[92] ECE, ibid., at p.3.

[93] Quoted at EDI`87: Conference on Paperless Trade, paper delivered by Bernard Wheble. Indeed, with respect to model interchange agreements, Baum, op.cit. supra n.84, notes that they "have provided quasi-authoritative sanctioning of electronic trading and have served to reflect and unify, as well as suggest, appropriate customs and practices"; at p.104.

[94] See further section 6.5.4. below.

[95] TRADE/WP.4/171.

(SIA)[96], while in February 1990, the American Bar Association (ABA) published a US Model Trading Partner Agreement (TPA)[97]. The TEDIS programme[98] of the European Commission, designed to promote the use of EDI, is also currently drafting a European model agreement[99].

Despite this recent activity, it should not be concluded that the use of such agreements are industry standard. The Electronic Messaging Services Task Force, which published the TPA, surveyed a large number of US firms using EDI, and discovered that most EDI activity occurs in the absence of any form of written agreement[100]. Two main reasons for this situation were suggested by the Task Force:

- Historically, EDI has been initiated with long-established and trusted trading partners, with whom the existing relationship supersedes any concern for contractual formalities; and

- due to the previous lack of information on the legal issues raised by EDI, the need for an agreement has not made an appearance on a company's EDI implementation checklist[101].

In Europe, the author's survey of EDI users revealed that a third of respondents had no formal legal agreement with their trading partners, concerning the use of EDI, and were not intending to use any such agreement[102]. One such company simply stated:

> "EDI was written into our commercial agreement with our key vendors, as an understanding";

---

96 The EDI Association Standard Electronic Data Interchange Agreement. The first edition was published in March 1989; subsequently, a second edition was published in August 1990. This Chapter will discuss the second edition unless otherwise stated; see Appendix C2.

97 "Model Electronic Data Interchange Trading Partner Agreement and Commentary", 45 Business Lawyer 1719 (1990), prepared by the Electronic Messaging Services Task Force of the American Bar Association. It was "written specifically for the purchase and sale of goods", under the Uniform Commercial Code, art.2, within the US: See Boss, Amelia H., "The Proliferation of Model Interchange Agreements", p.542, Proceedings of the 3rd International Congress of EDI Users, 4-6 September, 1991.

98 Council Resolution 87/449/EEC of Oct.5, 1987, on the Introduction of a Community Programme Concerning the Transfer of Electronic Data for Commercial Purposes via Communications Networks (Trade Electronic Data Interchange Systems: TEDIS), OJ L 285/35 of Oct.8, 1987. This was initially a two-year programme, commencing 1 January 1988, with a budget of ECU 5.3 million. Agreements were concluded with the EFTA countries in December 1989 (approved by Council 21 Dec. 1989) to join the programme. The second phase of the TEDIS programme (COM (90) 574 Final) was adopted by the Council of 22 July 1991 (91/385/EEC, OJ L 208), for a three period, with a budget of ECU 25 million.

99 `European Model EDI Agreement' [AT/fv 91-01173] - Final Draft circulated for comment May 1991.

100 "The Commercial Use of Electronic Data Interchange", 45 Buiness Lawyer 1645, June 1990.

101 Boss, op.cit. supra n.97, at p.541, notes, that the current increase in the use of interchange agreements "reflects growing recognition of the complexities and subtleties involved in electronic commerce, and the increased ability of the parties to resolve these matters contractually".

102 See Appendix B3. In 1990, the UK EDI Association's Legal Advisory Group surveyed the Association's members: Only 25% of respondents used such an agreement; although 80% of the non-users stated their intention to use the SIA.

while a German electronics company stated that:

> "our policy...is one of a `Gentleman's Agreement', that both partners will act together and in mutual interest. Increasingly we talk of supplier/customer relationships as partnerships and believe that generally the companies we wish to do business with will act in a fair and reasonable manner..."

Such attitudes are perhaps likely to become increasingly common as EDI gains wider acceptance as the form of commercial communication and the legal security provided through interchange agreements becomes redundant.[103]

It can therefore be seen, that the use of interchange agreements should not be viewed as a prerequisite for the use of data communications in electronic trading.

6.3.2 Relationship to other agreements

When drafting an interchange agreement, the basic rule is to ensure that the terms of the interchange agreement do not conflict with those contained within the underlying commercial contract for goods and/or services[104]. EDI is simply a means of communication, and should not alter the underlying contractual relationships. Overall, this fundamental principle should enable the communication agreement to be short and fairly simple to adopt[105].

However, this perspective has not been shared by all countries. Agreements from the United States, Australia and Canada[106] have adopted a slightly different position, based on the belief that EDI does impact on the trading relationship to a more significant degree than simply as a means of communication. This has meant that interchange agreements emanating from these countries have tended to cover a wide range of business issues, including the respective companies' terms of trade[107]:

> "an interchange agreement will allow parties to specify the terms and conditions applicable in the underlying commercial transaction, thereby eliminating the need to

---

[103] See section 6.3.5 below.

[104] UNCID op.cit. supra n.7, at Principle (b): "apply only to the interchange of data and not to the substance of trade data messages transmitted".

[105] Mike Flynn, ICI's EDI Manager, believes that such an agreement should be simple enough to fit on the back of an order form, otherwise it facilitates against EDI; quoted in Sarson, Richard., "EDI in the Dock", p.127, Network, May 1989.

[106] The US American Bar Association's Trading Partner Agreement was the first to adopt this approach, which has since been followed by Canada and Australia. See also Wright, B., *EDI and American Law*, TDCC: The Electronic Data Interchange Association, 1989; and Crawford, B., "Strategic Legal Planning for EDI", p66-77, Canadian Business Law Journal, Vol.16, 1989.

[107] See section 6.3.3 at *Electronic Trading / Contract Formation* below.

include them in the electronic transmissions and eliminating the uncertainties which may arise.."[108]

This would seem to suggest the need for a long contract negotiation period prior to the adoption of EDI[109]. These differing perceptions of EDI's impact on the nature of business activity represents one of the main currents of debate within the field of data communications law.

EDI is the interchange of structured messages by agreed message standards, therefore a `user manual' or `technical annex' will be a necessary pre-requisite for parties to communicate via EDI[110]. The `user manual' should contain all the details that enable an electronic transfer to take place, including the agreed types of messages to be exchanged (eg. invoices)[111]; this would include details of any legally-required trade specific messages[112] or specify the legal significance of a particular message type[113]; and the procedures that will be implemented to ensure technical security (eg. specific access procedures and means of authentication).

Since the technical procedures are liable to be updated frequently (eg. as new messages are adopted), the user manual is usually a separate document from the Interchange Agreement, which the parties agree to amend from time to time[114]. However, the technical manual is commonly incorporated as part of the Interchange Agreement, either as a schedule or appendix; as stated in the ABA Agreement:

"Each party may electronically transmit to or receive from the other party any of the transaction sets listed in the Appendix..and transaction sets which the parties by written agreement add to the Appendix (collectively `Documents')....All Documents shall be

---

108 Boss, op.cit. supra n.97, at p.541; and Savage, R., "How to resolve legal issues in EDI agreements: Acknowledgements and the Battle of Forms", pp.66-71, EDI Forum, No.1, 1991. See further Chapter 5, at 5.2.4.

109 Boss, ibid., at p.553, also notes that "the use of electronic data interchange...may be inconsistent with negotiation over the terms of every individual contract.".

110 See Chapter 2, at 2.2.3.2.

111 Eg. "...some portions of the Pedi protocol specify generic mechanisms that cannot be used in practice without either bilateral agreements between the sender and the receiver, or a functional group or industry usage guideline."; see Hill, Richard, *EDI and X.400: using Pedi*, p.99, Technology Appraisals, 1990.

112 Eg. in the shipping industry, a `hazardous cargo declaration' message; or IATA dangerous goods declaration.

113 Eg. "..specific issues relevant to the insurance industry could be set down in the User Manual, where it could be explained which messages constitute an offer, which an acceptance" [8.8], Minutes of the EDIA Legal Advisory Group Meeting, of 19th October, 1989. See also Baum, op.cit. supra n.84, at p.102: eg. under the US X.12 standards, the FOB message segment details loss and delivery responsibilities.

114 See UN/ECE report, `Trade Data Interchange Protocols', TRADE/WP.4/R.609, calling for amendments to the UN/EDIFACT Syntax Implementation Guidelines to stress the two-part nature of the interchange agreements: legal and technical.

transmitted in accordance with the standards [and the published industry guidelines] set forth in the Appendix."[115];

or by reference, as stated in the UK EDI Association Agreement:

"This agreement shall apply to all Messages between the parties using the Adopted Protocol and the parties agree that all such Messages shall be transmitted in accordance with the provisions of the User Manual."[116]

It has also been suggested that the parties should distinguish within the User Manual between `systems rules' (eg. security procedures) and `operational rules' (eg. technical data processing); whereby the latter, purely technical aspects, would not be legally binding.[117]

It should also be noted, that the nature and information contained within a `user manual' will bestow it with implicit legal quasi-contractual significance, even in the absence of an express interchange agreement between the parties. In a dispute, the courts would be likely to place significant reliance on this document to determine the intention of the parties and their respective obligations and responsibilities.

6.3.3 Drafting considerations

This section reviews the form that such contracts have taken, on a clause by clause basis; although liability issues will be separately in Section 6.5.2. below. The analysis is based upon a survey of 34 different interchange agreements, from many of the major trading nations, except Japan[118]. There is, however, a basic division in the style of interchange agreements between the US approach and the UNCID/UK approach, discussed previously.

It should not be forgotten, however, that a wide range of alternative contractual solutions have been adopted by EDI trading partners, such as amending standard trading terms and conditions, as well as none at all. For example, the ABA Model Trading Partner Agreement was only published in 1990, and yet around 10,000 EDI users were already trading via EDI in the US.

---

115 TPA, op.cit supra n.97, at Section 1.1.

116 SIA, op.cit. supra n.96, at Section 2.1. However, the second edition recognises that not all EDI users may have developed a formal User Manual, and therefore a clause 2.2 was added stating that the parties could agree technical procedures relating to the interchange of data that are included in an appendix to the agreement.

117 Roy Goode, quoted in Sarson, op.cit. supra n.105, at p123.

118 See Appendix C1 and the SIA.

Definitions and Scope

Since EDI is a new mode of business communication with its own unique terminology, it is common, as an aid to the parties, to preface the agreement with a set of standard definitions to be used throughout the agreement[119]. Definitions in a contract generally serve two purposes: preventing the need for the repetition of long phrases, and to enhance understanding and certainty between the parties.

The reviewed agreements seem to agree on a core set of five defined terms:

`Adopted Protocol': "the accepted method for the interchange of Messages based on the EDIFACT[120] standard for the presentation and structuring of the transmission of Messages, or such other protocol as may be agreed in writing by the parties"[121];

`Technical Annex': "The handbook, sometimes known as the `User Manual', which includes the technical, procedural and organisational rules and specifications for the exchange of EDI messages"[122];

`Message': "means an identified and structured set of data elements and segments covering the requirements for a specific transaction transmitted electronically between the parties"[123], an alternative term used is `document' ;

`Trade Data Log': "A collection of trade data transfers that provides a complete historical record of trade data interchanged"[124], intended to act as the primary evidential record;

`Supply Agreement': "means the agreement(s), between the parties for purchase and supply of products and services, and attached as, or otherwise identified in Schedule A..."[125], more commonly described as the `trade transaction', its purpose is to reference the underlying contract.

---

[119] See UNCID, op.cit. supra n.7, at Article 2, `Definitions'.

[120] United Nations standard, Electronic Data Interchange For Administration Commerce and Transport, see Chapter 2, at 2.2.3.2.

[121] Eg. SIA, op.cit. supra n.96, at 1.

[122] Eg. Tedis, op.cit. supra n.97, at Art.1.

[123] Eg. EDI Council of Australia: Model EDI Trading Agreement, at Part 1.1.

[124] Eg. New Zealand Customs Department (CEDI): Interchange Agreement, March 1990.

[125] Eg. EDI Council of Canada: Electronic Data Interchange Agreement, at 1.01 (j).

A wide range of other definitions have also been used, including defining EDI; the message `sender' and `receiver'; whether the parties intend to use a VAN; and the standard business day[126]. The ABA, the Tedis and the Australian agreements define `signature', in an attempt to satisfy any statutory requirements for certain contracts to be signed[127]. The ABA Agreement states:

> "Each party shall adopt as its signature an electronic identification consisting of symbol(s) or code(s) which are to be affixed to or contained in each Document transmitted by such party..."[128]

While the Australian Agreement also defines `writing' for a similar purpose[129].

Often when embarking on the use of EDI, the parties will run an initial pilot project or trial period, in order to test the system and establish confidence in its security. In such circumstances, the parties may wish to define the nature and time limits of this period[130].

As is usual with most standard commercial contracts, the parties should state their intentions with regard to the scope of the interchange agreement. All the agreements focus on the fact that the contract is primarily concerned with using EDI as a mode of communication. This is the case even in the US-style agreements, which at the same time also closely relate the interchange agreement to the underlying contract for goods and/or services, as is stated in the commentary to the ABA Agreement:

> "The Agreement does not attempt to resolve all aspects of commercial trading relationships....Counsel is cautioned to consider the additional issues which arise from the underlying Transactions (issues which are not unique to the use of EDI) and to develop appropriate responses."[131]

It is therefore also generally clarified that the underlying commercial contract will take explicit priority, in the event of a dispute, except for the specific scope stated in the interchange agreement.

---

126 Eg. Tedis op.cit. supra n.99, at Art.1. Such a clause impacts on the period within which the recipient is under an obligation to acknowledge receipt, or notify the sender of any mistakes.

127 See Chapter 5, at 5.2.3.

128 Eg. TPA op.cit. supra n.97, at Section 1: Prerequisites, 1.5.

129 See also Australia, op.cit. supra n.123, at Part 2(3), and the discussion under *Electronic trading/ Contract Formation.*

130 Eg. DISH Pilot Project Interchange Agreement.

131 TPA op.cit. supra n.97, at para.1, p.2.

The other point made in the majority of agreement regards the relationship of the interchange agreement to the User Manual, as discussed in section 6.3.2. above.

Electronic Trading/Contract Formation

In Chapter 5, Section 5.2, the discussion was concerned with the legal insecurities created by the use of EDI within a statutory-commercial framework that presumed the use of paper documentation. This thesis has already considered the range of statutory requirements laid down for business communications to be `in writing' and `signed', as well as uncertainties regarding the process of contract formation within an electronic environment.

The legal status of electronic communications have been addressed in all the interchange agreements. As stated in the section on definitions, some agreements have tried to deal with these issues through the drafting of expansive definitions designed to encompass electronic communications. Overall, three slightly differing approaches have been adopted within the agreements, either acting together or separately:

(a) Re-defining the terms[132]:

> "The parties agree that correspondence and documents electronically transmitted...shall be construed to a `writing' or `in writing' and have been `written' or `signed', and that the computer printouts of the information contained...are `original' for all purposes.."[133];

(b) Agreement to treat the same as paper:

> "Each party accepts the integrity of all Messages and agrees to accord these the same status as would be applicable to a document or to information sent other than by electronic means.."[134]; and/or

(c) Agreement not to challenge the validity of EDI messages[135]:

---

132 The so-called `definition strategy', see UNCITRAL report `Electronic Data Interchange', p.18, A/CN.9/350, 15 May 1991.

133 IBM: Electronic Data Interchange Agreement, at 4(d).

134 SIA, op.cit. supra n.96, at 5.2. See also CMI Rules ("Introduction to CMI Rules: Electronic Bills of Lading", Paris/ELECTRO 15, June 1990), at Art.4(d) "..shall have the same force and effect as if the receipt message were contained in a paper bill of lading."; FINPRO, Model Agreement on Transfer of Data in International Trade, at Art.8 "When using electronic data interchange the legal bondage of documents is dependent on the legality of original documents and that deed is legally sound". With respect to civil law systems, it has been noted that it is "possible to derogate from the written document rules in an evidential clause stating that legal transactions performed on a telematics system may be proved by any means ..", in Amory, B.E. and Yves Poullet, "Computers in the law of evidence - a comparative approach in civil and common law systems", p119, Computer Law & Practice, March/April 1987.

135 UNCITRAL 1991 report, op.cit. supra n.132, at p. 20, defines this as the `waiver strategy': "mutual renunciation by the parties of the rights or claims they might have to contest the validity or enforceability of an EDI transaction under possible provisions of locally applicable law."

"The parties agree not to contest the validity or enforceability of such Messages in any legal proceedings between them respecting or related to a Transaction and hereby expressly waive any right to raise any defence or waiver of liability based upon the absence of a memorandum in writing or a failure of execution"[136]

The use of such terms should greatly enhance the status of such messages in a court of law, and therefore legal security.

In some contracts, the parties are required to explicitly accept the use of electronic communications as a means of sending contractually enforceable statements of offer and acceptance[137]. In terms of legal security, therefore, the parties should specify what message types are to be considered legally binding: for example, a `purchase order acknowledgement' should be distinguished from a `functional acknowledgement' message, as the means by which an offer can be accepted[138]. In a 1989 US case, for example, the court decided that where the defendant's order-taking computer system issued a order-tracking number, in response to the plaintiff's electronic order, this was an administrative message and was not contractually binding[139].

In addition, with regard to contract formation, it may be important to clarify what the parties agree to regard as `message receipt', since this could be particularly important for certain payment-related messages (eg. due date): For example, is `receipt' to be the point at which the message is deposited in the electronic mailbox of the recipient, or at the point at which it is retrieved from the mailbox?[140] The parties might also decide to prevent the party which sends an offer from sending a `revocation of offer' message electronically, since the nature of the recipient's processing operations may mean that it has already acted upon the offer[141].

Within a European trading environment, there are various different rules with regard to the time and place at which a contract has been concluded; therefore, the Tedis Draft Agreement states that the contracts shall be considered as concluded "where the EDI message

---

136 Australian Agreement, op.cit. supra n.123, at 3.4; TEDIS op.cit. supra n.99, at Art. 10.1. The CMI Rules also adopt this approach, op. cit. supra n.134, at Rule 11: "In agreeing to adopt these Rules, the parties shall be taken to have agreed not to raise the defence that this contract is not in writing".

137 Eg. Canada, op.cit. supra n.125, at 6.02 and TPA, op.cit. supra n.97, at 2.3.

138 The latter is a security procedure, see below.

139 *Corinthian Pharmaceutical v Lederle Laboratories*, 724 F.Supp.605 (SD Ind.1989). See also Wright, B., "Contracts without paper", p.61, Technology Review, July 1992.

140 See Shaw, op.cit. supra n.84, at p.33. See also TPA, op.cit. supra n.97, at 2.1.

141 See "Contract Formation and Open EDI Systems", open letter from Ake Nilson to Jan Freese, Chairman, ICC Working Party on EDI, dated 19.11.91. In English common law, an offeror may revoke his offer at any time before acceptance: *Routledge v Grant* (1828) 4 Bing 653.

constituting the acceptance of an offer is made available to the information system of the receiver"[142].

Another issue discussed in Chapter 5, at 5.2.4, was whether there was a need to incorporate a company's standard trading terms and conditions into the data communication process. As noted above, at 6.3.2, the UK's EDIA Legal Advisory Group view is that the use of electronic messaging does not impact on the underlying trading contract, and therefore the issue of applicable standard terms and conditions should have been dealt with at a different point. This has not been the approach in other countries, where some interchange agreements have explicitly included or incorporated the trade terms and conditions[143].

Security and Confidentiality

Technical security procedures are obviously the critical component in protecting data communications and establishing trust in such systems; such trust then facilitates the spread of electronic messaging between, and within, companies. In addition, security measures can also enhance the legal efficacy of electronic messages[144]. Trading partners therefore need to agree to implement and maintain a certain level of security.

The security of a network is as effective as the user with the weakest security procedures. However, many respondents to the survey[145] seemed to view data communications security as primarily an issue concerning the network provider:

> "we use a VAN network, that takes care of any abuse of data"
>
> "the VAN is an almost 100% guarantee against fraud"!

This perception of security issues was particularly true of those companies without interchange agreements. Such faith in the role of the network provider would not seem to be shared by the network provider's themselves, who "do their best to minimise their commercial exposure".[146]

---

[142] Tedis, op.cit supra n.99, at Art.9(2).

[143] Eg. Canada op.cit. supra n.125, at Art. 6.03. See also Savage, op.cit. supra n.108, at p.68; where a draft `terms agreement', for incorporation into the communication agreement, is provided.

[144] See Chapter 5, at 5.2.3.

[145] See Appendix B3.

[146] Draper, J., "Technical Solutions", p.110, in Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989. See further section 6.5.3. below.

The level of protection required will obviously depend on the nature of the information involved; for example, encryption may be deemed necessary for payment messages, but could be seen as an unnecessary requirement for invoices[147]. Encryption was stated as an option by only a few respondent companies, which would suggest either that companies are unaware of such techniques; or that companies are not, or do not perceive themselves, as currently exchanging high value messages[148].

In all the agreements, the parties agree that they shall:

> "take all appropriate steps and establish and maintain such procedures so as to ensure that as far as reasonably practicable Messages are properly stored, are not accessible to unauthorised persons are not altered, lost or destroyed, and are capable of being retrieved only by properly authorised persons."[149]

In the majority of agreements, reference is usually made to the User Manual/Technical Annex as being the place where such security procedures are detailed and with which the parties must comply[150].

The Australian Agreement includes an additional provision requiring a party that becomes aware of a security breach, such as an unauthorised access, to immediately inform the other parties and then report the results of any subsequent investigation. Such a clause would seem judicious, bearing in mind the potential damage created by a virus inserted into a network, as well as operating against the natural desire of companies to try and keep all breaches of security confidential[151].

Where no explicit requirements are contained in the technical manual, or where the sender desires a particular message to be given additional protection, a provision could provide that the level of security can be set by the message sender and it must be maintained by the recipient in any further onward transmissions[152].

---

147 The FINPRO, op.cit. supra n.134, at 11.3, requires that a code and cryptokey be used as a security device.

148 This is also a factor of the cost of using such security methods.

149 SIA, op.cit. supra n.96, at 3.1.1. Note the similarities with Principle 8 of the UK Data Protection Act, see Chapter 4.4.2.

150 Eg. Eastman Kodak Company Agreement: Electronic Data Interchange (US), at Section III: `To provide for continuous and trouble free operations..'.

151 Australia, op.cit. supra n.123, at 7.4. See also section 6.5 on liabilities below. In most legal systems, there is an implied duty between contracting parties to communicate "any information likely to permit the other party to effectively exercise his rights". This could be seen to apply to actual or potential security breaches discovered by either data users or the network operator. See `The Liability of Electronic Data Interchange Network Operators', p.38, Tedis final report, July 1991.

152 Eg. SIA, op.cit. supra n.96, at 3.2.

Where the parties wish to place positive obligations upon each other for the implementation of appropriate security procedures (detailed in the technical manual), it is also important to consider monitoring procedures to ensure continuing compliance:

> "Once a year each party shall engage an independent expert to evaluate whether that party and its VANS are maintaining and operating the part of the EDI Network under their control in accordance with the requirements of this Agreement. The expert's report shall be made available to the other party within a reasonable time."[153]

`Acknowledgement of receipt of messages'[154] and `confirmation of content'[155] are procedures which the parties could adopt, to provide for a higher degree of security. Acknowledgement of receipt is an automatic aspect of certain data communication networks, and it can be expected to become an increasingly common feature as systems mature. In the absence of such a technical feature, the contractual agreement could state that an `acknowledgement of receipt' message will be sent by the recipient, where requested by the sender; or alternatively, the clause could place a duty on the recipient to send an acknowledgement for all messages received:

> "Each party [shall review at or about .... am. and ... pm. all Documents received by it since its last review of Documents received and] shall promptly acknowledge receipt of each Document received by it."[156]

It is usually agreed by the parties that an `acknowledgement of receipt' will be in the form of an EDI message.

The UN/ECE WP.4 group, studying EDI legal issues, is currently considering the inclusion of a clause in interchange agreements that would state that electronic messages that have not been acknowledged by the recipient would have no legal value and/or consequences[157].

Even where the parties do not require the transmission of a `functional acknowledgement message', a number of the agreements have specified what, in terms of interchanged data, will be considered to be `proper receipt':

---

153 Australian, op.cit. supra n.123, at 9.1.

154 See UNCID, op.cit. supra n.7, at Article 7.

155 Ibid., at Article 8.

156 Canada, op.cit. supra n,125, at 4.03. It has been noted that "an acknowledgement of receipt serves to eliminate many of the problems that have long been debated when contracts have been concluded by distant parties", p.13, `Electronic data Interchange: Preliminary study of legal issues related to the formation of contracts by electronic means', A/CN.9/333, 18 May. 1990.

157 Ritter, J.B., "Electronic commerce and international law: a tapestry in the making", pp.117-126, Proceedings of the 3rd International Congress of EDI users, 3-6 September, 1991, Brussels.

"Documents shall not be deemed to have been properly received, and no Document shall give rise to any obligation, until accessible to the receiving party at such party's Receipt Computer designated in the Appendix"[158]

A `confirmation of content' clause would place an obligation upon the recipient to read the message, within a certain period of receipt, and confirm to the sender that it appears to be correctly formatted; for example, the Canadian Agreement states:

"5.04 **Reasonableness Testing**
Upon receipt of a Document that contains an offer to enter into a new Contract, the Receiver shall promptly review it and notify the Sender of any apparently unusual terms"

This would provide for an extremely high level of security, but would usually require some form of manual intervention, thereby losing some of the benefits of electronic trading. The introduction of some form of `expert system', between the point of receipt and entry into the specific application, to interrogate incoming messages for unusual terms, would perhaps be an alternative technical solution[159].

The Chairman of the sub-committee that drafted the CMI `Rules for Electronic Bills of Lading'[160], states that the committee considered the possibility of including provisions covering both `acknowledgement of receipt' and `confirmation of content', however, it was concluded that "this distinction, it was thought, would not be readily understood by the parties"[161]. The final CMI Rules only deal with `confirmation', to the extent that it "appears to be complete and correct, without prejudice to any subsequent consideration or action that the context may warrant"[162].

It should be clearly expressed that such actions, `acknowledgement of receipt' and `confirmation of content', are not to be considered as `acceptance' in the contractual-legal sense, and therefore will not have an impact on the place or moment of contract formation.

---

158 TPA, op.cit. supra n.97, at 2.1.

159 An expert system, based on an `if...then' methodology, can be written fairly easily for each trade specific application; for example, it could analyse a contractually-binding message to ensure that it falls within certain pre-defined parameters/tolerances regarding costs and quantity etc. The parties could then agree that the point at which the message is approved by the recipient's expert systems is the point at which the recipient agrees to have contractually accepted the order.

160 The CMI Rules, op.cit. supra n.134.

161 Ibid., at p8.

162 Ibid., at Rule 2(e).

Confidentiality is a critical aspect of all business relationships. Within EDI interchange agreements, confidentiality has been treated in three different fashions:

(a) Catch-all confidentiality clauses:

> "Contractor shall not at any time....use or disclose to any person for any purpose other than performance..any information it receives.."[163].

Such an approach has only been adopted in certain company-specific agreements, not in any general Association/model agreements. This probably reflects general business conservatism and fear with regard to the use of all company-related information.

(b) General non-confidential clause:

> "No information contained in any Document or otherwise exchanged between the parties shall be considered confidential, except to the extent provided in Section 1.5 [Signatures], by written agreement between the parties, or by applicable law"[164]

(c) Sender-specified confidentiality:

> "ensure that any Message containing confidential information as designated by the sender of the Message is maintained by the recipient in confidence..."[165]

Both (b) and (c) presume that in the majority of cases, the parties are likely to specify in advance of EDI trading which categories of information are to be considered `confidential'; however, in (c) the sender is given greater flexibility to classify confidentiality on a message by message basis. Indeed, where possible, the User Manual could state that where a particular code is used within an message, then that message is to be treated as `confidential'.

As in standard trading contracts, the scope of the clause generally extends to uses other than that necessary for carrying out the contractual obligations, such as the communication to third parties. Exemptions are provided for when the information is already in the public domain, or has been legitimately received from a third party.

---

[163] IBM, op.cit. supra n.133, at Attachment A: EDI Purchase Order Terms and Conditions.

[164] TPA, op.cit. supra n.97, at 3.2.

[165] SIA, op.cit. supra .96, at 3.1.2.

If the EDI messages are likely to contain personal data, and therefore the transmission of such data to a third country could breach the provisions of the data protection legislation of the home country, then an appropriate clause should be included. For example:

> "Where EDI messages containing personal data are sent or received in countries where no data protection legislation is in force, each party agrees as a minimum standard, to respect the provisions of the Convention No.108 of 28.01.1981 of the Council of Europe on the protection of the individual with regard to the automatic processing of personal data"[166]

In certain agreements, an additional duty has been placed upon the recipient to notify the sender if a message has been mistakenly received:

> "If the recipient of a transfer reasonably understands that it is intended for someone else, the recipient shall take all reasonable action as soon as possible to inform the sender and shall delete the information contained in such transfer from the recipient's computer system, apart from the trade data log."[167]

However, maintenance of a record of the receipt of such a misdirected message may be critical in any subsequent dispute concerning theft of commercial trade secrets.

Authentication

> "la procedure par laquelle l'Emetteur ou le Destinataire confirme son identification"[168]

Authentication is a particular aspect of data security, enabling the recipient to have certainty with regard to the origin of the message. Authentication is closely related to the legal concept of `signature', and therefore the method of authenticating electronic messages will usually be considered to satisfy any statutory requirement for a signature.

In the reviewed agreements, the issue of authentication is usually covered either as part of any designation of a signature requirement:

---

[166] Tedis op.cit. supra n.99, at Art.11. See generally, Kerkau, H.J., "Data Protection and Telecommunications", pp.75-77, Proceedings of *EDI - 1992 and beyond*, Brussels, September 1989, and Walden, I., "How data protection complements and complicates EDI", pp.20-22, Privacy Law & Business, No.10, May 1989.

[167] New Zealand, op.cit. supra n.124, at clause 7(d).

[168] Le Centre International de Recherches et d'Etudes du Droit de l'Informatique et des Télécommunications (CIREDIT): Contrat-type d'interchange EDI (France), at `Défintions' (g).

"Each party agrees that any Signature of such party affixed to or contained in any transmitted Document shall be sufficient to verify such party originated such Document"[169];

or within provisions relating to the security of EDI messages, and referenced to the User Manual for specification (eg. digital signatures):

"..the parties shall agree on procedures or methods to ensure message verification. Message verification includes the identification, authentication and verification of integrity and origin of a message by use of an authentication mechanism..."[170]

Obviously, the nature of the authentication process will alter according to the type of message involved and the purpose/s for which the `signature' is intended to serve[171]; therefore the ability to make use of higher levels of authentication should also be agreed between the parties in advance.

The parties might wish to identify, in the appendices to the agreement, the specific company officers within their organisation who are authorised to send, and are therefore responsible for, all electronic messages sent.

Recipient obligations

The parties might wish to determine in advance the actions of the recipient once the message has been delivered:

"The parties undertake to process or ensure that their system processes the EDI messages within any time limits specified in the Technical Annex, unless otherwise agreed by the parties"[172]

For example, it might be agreed that the recipient has a duty to empty his electronic mailbox within specified hours, eg. 3-5pm every day. In addition, it might be deemed necessary to require the recipient to process the message within a certain time-frame, or "as soon as

---

169 TPA, op.cit. supra n.97, at 1.5.

170 Tedis, op.cit. supra n.99, at 6.2.

171 Baum, op.cit. supra n.84, at p.61, notes that a signature can be used for a number of purposes, including to (1) evidence who created and sent a message; (2) verify the accuracy of message content; (3) demonstrate contractual intent; (4) prevent the sender repudiating the message. In a US survey of EDI users, the following were used as legal signatures: a buyer code, a DUNS number and suffix, a password, a message authentication code, an account number, an ID/password combination and functional acknowledgements - see Legal and Business Controls Task Group, Accredited Standards Committee X12, 1990 Survey.

172 Ibid., at Art.5. A time limit may be critical within a `Just-In-Time' manufacturing environment.

possible"[173]. The parties might even wish to agree the frequency with which messages will be sent.

As discussed previously, however, before such provisions apply, the recipient may be required to send an appropriate `acknowledgement of receipt' or `confirmation of content' message to the sender.

Storage and Evidence

Article 10 of the UNCID Rules[174] states that EDI users should maintain a `trade data log' as a complete historical record of all messages sent and received. The primary purpose of such a `log' is to act as a record for evidential (eg. determine the sequence of events) and audit purposes. The parties can agree upon the exact content of such a record, since within an EDI communication there are two general categories of data: "the commercial transaction itself... and the details relating to the transmission and processing of the transaction (the envelope)"[174a] . In terms of data security, user should retains records of any messages that were misdirected, or any messages sent without adequate authorisation:

> "`Transaction Log' means the record of all Documents and other communications exchanged between the parties via the EDI Network [and a summary of the contents thereof, including all material particulars of the Contracts formed between the parties]."[175]

The records can obviously be maintained in an electronic form, as long as procedures exist for them to be recovered in an unmodified, readable format, as required. The record should also be maintained for a period of time agreed by the parties[176], or as prescribed in legislation and statutory regulations (eg. VAT)[177].

Under the UK Civil Evidence Act 1968, s.5, it states that in order for computer evidence to be admissible as hearsay, a certificate should be supplied stating that the system was functioning correctly when the evidential record was generated. This certificate must be produced by a person "occupying a responsible position in relation to the operation...or the

---

[173] SIA, op.cit. supra n.96, at 6.3.

[174] UNCID, op.cit. supra n.7.

[174a] List, W., "International EDI - the implications for record keeping", p.476, Proceedings of the 3rd International Congress of EDI Users, Brussels, 4-6 September, 1991.

[175] Canada, op.cit. supra n.125, at 1.01 (k).

[176] Eg. ICL: Electronic Data Interchange Agreement, at 7.3 "..for a period of at least six years from the date of creation...". UNCID, op.cit. supra n.7, at 10(c) states that the log "should be stored unchanged.....in the absence of any requirement of national law or agreement between the parties, for three years".

[177] One proposal has suggested that the record-keeping standard for electronic accounting information should be that the record be "instantaneously printable on paper for one year after expiry of the financial year...", but should be readable for at least 10 years. See Fresse, Jan, "EDI and National Legislation" - Teresa (86) Draft Report, p.13, ICC Doc. No. 460-10/Int.38.

management of" the computer system[178]. The interchange agreement should therefore ensure that each party has implemented procedures to satisfy such evidential requirements.

In the majority of the other agreements, each party is usually required to appoint a person(s) who will be "responsible for the systems and procedures relating to the compilation and custody of the Transaction Log"[179]; who would presumably fulfil the role of `internal record-keeper'[180]. One survey respondent[181] depended on the network provider to maintain their records, an appealing option, especially for small companies. However, it is an acceptable option only if any potential dispute is not likely to involve the network provider directly!

Some agreements have dealt with the issue of `storage of data' separately from that of evidential admissibility and, to avoid the potentially stringent statutory admissibility requirements, the parties have agreed a clause stating that:

> "In the event of a dispute, the parties shall not bring into question the admissibility as evidence of messages exchanged and stored according to the provisions of this agreement"[182]

However, such a clause will obviously not prevent any objections being raised in a claim from a third party, such as a regulatory authority.

Where one EDI trading partner is in a dominant position, they could get the other party to agree to accept the data log of the dominant partner as the correct record of events; this approach has been particularly adopted in electronic payment systems, reflecting general banking practice:

> "the Bank's master log shall, in the absence of manifest error, be conclusive proof and evidence of the messages and payments sent, received or made by the Bank in connection with...the Service."[183].

Recently, proposed regulations for EDI have been drafted by the Swedish Federation of Industries. With regard to general evidential issues, the proposals state:

---

178 See Chapter 5, at 5.3.2.

179 Australia, op.cit. supra n.123, at 8.1,

180 See Wright, B., "Authenticating electronic contracts: the case for international recordkeeping", paper in proceedings of EDI and the Law'91, Conference, Washington, February, 1991.

181 See Appendix B3.

182 Tedis, op.cit. supra n.99, at Art.10; Odette, The Guidelines for Interchange Agreements, prepared by the Organisation for Data Exchange Through Teletransmission in Europe, 1990, at Clause 8; and Canada, op.cit. supra n.125, at 7.04. The UNCITRAL 1991 report, op.cit. supra n.132, at p21, states: "It now seems to be widely conceded that under both common law and civil law systems, such private commercial agreements on admissibility of evidence are valid, or, at least, that they are not faced with a general prohibition."

183 Barclays EDI Trading Master Interchange Agreement, at clause 10(b); see also National Westminister Terms and Conditions for Bankline Interchange, at 14; and British Aerospace EDI Agreement, at 6.

"Any party not complying with the requirement to keep a data log, or breaking other security requirements in relation to the claim in question, should have the burden of proving that the claim is invalid"[184]

Network Provider

Most EDI trading partners communicate via a third-party network provider (VAN). It is therefore necessary to specify the responsibilities of the trading partners for the actions of such intermediaries. The basic rule, taken up in all the reviewed agreements, is that the message sender is liable with regard to his trading partner for the actions of the network provider; for example:

"...that party shall be responsible towards the other party...for any acts, failures or omissions by that intermediary in its provision of the said services....and for the purposes of this Agreement the intermediary shall be deemed to be an agent of that party."[185]

In recognition of the fact that the EDI network adopted by a company may be dictated to it by its trading partner, the SIA includes an additional clause stating that where a Service Provider is imposed, the dominating partner is responsible[186]. In many agreements, specific reference is made to the fact that each party is responsible for its own costs relating to the use of the third-party[187].

If the parties do not include a clause, stating that the message sender will be responsible for the conduct of the network provider, then no contractual liability will exist "except where such conduct is attributable to either party and causes such party to breach the provisions of the Agreement"[188].

The exact nature of the relationship between the message sender and the Service Provider will obviously be determined by contract, and is discussed in Section 6.4 below.

---

184 Presse, op.cit. supra n.177, at p.21.

185 SIA, op.cit. supra n.96, at 8.1, and TPA, op.cit. supra n.97, at s.1.2.3. For EFT transfers, in the US, the UCC, art.4A-206(a) (1989) states that: "If a payment order addressed to a receiving bank is transmitted to a funds-transfer system or other third-party communication system for transmittal to the bank, the system is deemed to be an agent of the sender....". In contrast, Katus, op.cit. n.1, at p.93, believes that where the parties agree to use a particular network provider that "senders and addressees share equal responsibilities".

186 Ibid., at 8.2.

187 Eg. Australian, op.cit. supra n.123, at 5.2 and TPA, op.cit. supra n.97, at 1.2.2.

188 O'Brien, Kevin O., "Global Value Added Network Providers: Contractual Analysis of Legal Liability Issues", p.2, paper presented at the 4th EDI Electronic Data Interchange Conference, USA.

Appendices

A number of interchange agreements make provision for the substantial use of appendices, attached to the main agreement. The number of such appendices often reflect the perception of a closer relationship between the use of EDI, as a mode of communication, and the underlying contracts for goods and services; such as in the ABA Agreement.

The User Manual is often included within the appendices, which seems suitable, since it contains the `technical security' procedures for effective data communications that complement the `legal security' provisions contained within the interchange agreement. The two documents are intimately linked[189].

Other issues often covered in the appendices are: message types to be exchanged; identifying the third-party EDI network provider and allocating the associated costs; industry/trade specific guidelines or codes of conduct that impact on either the use of data communications (eg. data protection) or the general trading relationship. The most common appendix contains a copy of the standard terms and conditions upon which the commercial relationship is based[190].

Miscellaneous

(a) EDI specific terms:

The User Manual, containing the technical specifications, could give rise to disputes with regard to the interpretation of certain requirements, therefore, some agreements have included a clause appointing an expert independent authority to resolve such disputes:

> "Any question relating to the interpretation of the User Manual may be referred by the parties to the body responsible for the publication of the User Manual or the Council of the EDI Association as may be applicable acting as experts and not arbitrators, whose decision shall be final and binding on the parties making the reference."[191]

The market for information technology products and services develops extremely rapidly, therefore, the parties could impose an obligation to inform the other party when new

---

189 See Thomsen, H.B., "Interchange Agreements", p.81-82, in Walden, op.cit. supra n.146.

190 See in particular the TPA, op.cit. supra n.97; the Kodak, op.cit. supra n.150 and the Australian, op.cit. supra n.123.

191 SIA, op.cit. supra n.97, at clause 10. The Dish Pilot Project Interchange Agreement refers such questions to the management committee of the project, at clause 12.

hardware, software or communication products are to be implemented, that may impact on the data communications between the trading partners[192].

As stated in the definitions, the parties may wish to run the EDI system on a trial basis for a certain period of time, before `live' electronic trading is contemplated. Where this is the case, the interchange agreement should include a provision covering such trials, and any subsequent and continuing test procedures agreed between the parties[193]. Such provisions may specify the status of the electronic messages sent during the test period, vis-a-vis the continuing paper-based communications.

(b) Standard commercial contractual provisions:

Disputes are inevitable in any commercial relationship. However, resolving disagreements through the courts is time-consuming and expensive and since no direct case law exists in the field of EDI (to date), these factors can be expected to multiply. In addition, the investment in time and money to establish EDI communications with your trading partner means, in commercial terms, that any dispute is to be strenuously avoided.

The parties may, therefore, wish to include a clause stating that the parties agree to go to arbitration or some other means of alternative dispute resolution[194], rather than use the court system. This is the position adopted in the vast majority of agreements:

> "In the event of any disagreement or dispute between the parties as to any matter arising from or related to this Agreement and which the parties are unable to resolve after good faith negotiations, the matter shall be referred to and determined by arbitration.."[195]

Article 11 of the UNCID Rules[196], provides that all questions of interpretation with regard to the "correct meaning of the rules should be referred to the International Chamber of Commerce". Such a provision was intended to ensure that the rules were adopted in a uniform manner, an importance basis for their international acceptance.

The use of appropriately chosen arbitrators should substantially enhance the `legal security' of the provisions within the agreement which are intended to provide for legal certainty in electronic trading, such as contract formation issues.

---

192 Eg. DIN (German National Standards Body) draft EDI Agreement, at clause 9.

193 Eg. Canada, op.cit. supra n.125, at 3.02.

194 Eg. Mini-Trials, Mediation or Conciliation; see Schiffer, R.A., "The use of `alternative dispute resolution' in resolving disputes involving EDI", p177-188, in Walden, op.cit. supra n.146.

195 Canada, op.cit. supra n.125, at 10.01.

196 op.cit supra n.7.

It is important that certain elements arising out of the interchange agreement, such as confidentiality obligations and maintenance of a `data log', are maintained for a period after the formal trading relationship has come to an end. Any contract termination clause should therefore specify such responsibilities.

The ability of commercial parties to `assign' a contract to a third-party is usually fairly restricted. Within an EDI context, it would seem particularly pertinent to include a provision denying the right of the parties to assign their contractual rights and obligations with respect to the interchange agreement. Since authentication is a critical component of data communications security, an assignment could severely compromise such security procedures[197].

Most contractual agreements identify the jurisdiction and applicable law upon which an arising dispute will be settled[198]. In an EDI context, where the communications network is likely to extend over a large number of legal jurisdictions, the resolution of such questions by prior agreement would seem particularly imperative.

6.3.4 CAD/CAM Agreements

The exchange of computer-aided design and manufacturing information is a particular form of electronic data interchange. The major difference between exchanging standard business documents, such as invoices, and the exchange of CAD/CAM information is the complexity of the information involved. However, the complexity and current lack of technical maturity in this sector has legal consequences that need to be considered when drafting an appropriate communication agreement[199].

As discussed in 6.5.2 below, the standard liability provision in all modes of communication is that the message sender is responsible for the accuracy of the message. However, what liability provisions should exist in a CAD/CAM environment, where an element of inaccuracy is a recognised facet of the electronic communication? The parties will need to carry out prior test exchanges to determine the level of accuracy of certain features, such as annotations and symbols[200], and draft a liability clause accordingly; eg.:

---

[197] Thomsen, op.cit. supra n.189, at p.87, para. 6.9.14.

[198] See Section 6.1.2 above.

[199] See Chapter 2, at 2.2.3.2. See also "Report on the potential legal issues arising from the implementation of CALS by the DoD", Prepared by the US Legal Issues Committee of the Acquisition Task Group, CALS/CE Industry Steering Group, 10 November 1991.

[200] Ibid., at p.8, parties need to test "how each system maps its entities to the neutral format [eg. IGES] and from the neutral or native format back". Following such tests, CAD/CAM drafting practices can be altered to avoid the use of non-transferable entities and features (p.12).

"Both parties shall use all reasonable endeavours to ensure the accuracy of data exchanged and will accept no responsibility for any consequences arising out of any inaccuracies or omissions unless such inaccuracies or omissions are the result of negligence on the part of that party"[201]

An additional legal issue, is the fact that engineering drawings are deemed to be classified as `artistic works' and are protected under copyright legislation[202]. However, the communication process will change the data that compose the work, such that the sender will need to ensure that the recipient acknowledges that the received data represents a legitimate `copy' of the work[203], and that all rights of ownership remain with the original party .

The CAD/CAM data will generally take three forms: the data held by the sender; the data in neutral format[204] during communication and the data as received and translated into the recipient's format. The parties therefore need to agree whether copies of all three file formats should be archived for a certain period after the exchange occurs, and explicitly state who holds the `master' data in the event of a dispute.

6.3.5 Comment

There has recently been criticism of the nature of communication agreements as outlined above. It has been suggested that such agreements are primarily suited to a closed data communication's environment, where electronic messaging is limited to an industry group or particular sector; "with the advent of open EDI systems, existing interchange agreements may become obsolete"[205]. It is believed that as commercial entities come to communicate completely by electronic messaging systems, the need to sign an agreement will no longer be practical within such a fast-moving environment.

As an alternative to such agreements, two alternative proposals have recently been promoted. The first, `interchange profiles', would be based upon "a pre-defined legal scenario which smoothly combines legal, security and technical considerations to suit pre-determined EDI relationships"[206]. Such profiles would consist of standard terms, drafted by neutral

---

201 CADDETC, *The Exchange Agreement: Guidelines for the successful exchange of product data*, 1990, at p.20.

202 See the definition of `artistic works' in the Copyright Designs and Patents Act (CDP), s.4.

203 CDP 1988, s.17(2), defines copying as `reproducing the work in a material form' including `storing the work in any medium by electronic means'.

204 "An intermediate file format which aids the transfer of product data between dissimilar CAD/CAM systems" (eg. IGES etc.), CADDETC, op.cit. supra n.201, at p.18.

205 Piette-Coudol, Thierry, p.1, "From Interchange Contracts...To Interchange Profiles", ICC Document No. 460-10/Int.34.

206 Ibid., at p2.

organisations such as trade associations, and converted into codes, similar to United Nations Standard Messages (UNSMs)[207]. When a data user decides to communicate with a new trading partner and establish a legal relationship, such as a purchase order for goods, then the user would insert the relevant `interchange profile' into the EDI purchase order message. The recipient would then be able to reference the code to a particular set of terms: both legal and technical.

The major practical disadvantage of such a scheme is the fact that it requires the creation of a vast code system, probably held on a database, to cover all the potential types of legal relationship. Such standard-making would take a considerable time to construct[208].

The second suggested arrangement would be the drafting of a set of EDI standard legal terms, similar to those that currently exist for international trade: INCOTERMS[209]. Such terms could then be stated by the sender as the conditions under which he is prepared to trade electronically. This is analogous to reliance on the UNCID Code of Conduct[210], except the terms, as stated, would form complete and explicit contractual conditions.

Indeed, the similarity between an `EDITERMS' solution and the `code of conduct approach' has led to calls for a revision of UNCID, to take account of the emergence of the open systems environment. The comparison with Incoterms, however, illustrates the problem of this approach: The Incoterms were primarily an quasi-legal codification of existing practice in international trade; whereas, any EDIterms would have to anticipate such practice. As in other areas of information technology law, such anticipation can lead to unnecessary restrictions and/or unrealistic requirements.

As stated previously, at the initial phase of the development of the UNCID rules, the Nordic Legal Committee circulated a proposal for `Uniform Rules for Communication Agreements'[211]. This style of proposal was rejected in favour of a code of conduct, because it was felt that it would be impracticable:

---

207 See Chapter 2, at 2.2.3.2.

208 Current UNSM's take around 4-5 years to be agreed upon.

209 See Brousse, Pascal, "Towards a more suitable interchange contract", ICC Document No.460-10/Int.32; and Bertrand, A.R., "Le Contrat d' Interchange dans une perspective historique: Vers des Incoterms E.D.I.", pp.107-114, in Linant de Bellefonds, Xavier, *Le Nouveau Droit Des EDI*, Editions des Parques, 1991. See also ICC Publication, Incoterms, 1st July 1990; and at Chapter 5, at 5.2.5. Similar suggestions have been made for `Incoterms' covering international data flows; see Bing, J., P. Forsberg, and E. Nygaard, *Legal Issues related to transborder data flows*, DSTI/ICCP/81.9. See further Chapter 3, at 3.4.

210 UNCID, op.cit. supra n. 7.

211 See ECE document TRADE/WP.4/R.300 and in ICC document No.374/1.

"...the details and form of communication agreements differ according to the size and type of the user groups. The agreement may be included in a protocol or form a separate document. It may contain additional rules...It is therefore not practical to formulate a standard model"[212]

Initially, the code of conduct was seen as a lower achievement, by the drafting group, than that of a model agreement, since it was not directly binding on users. However, it was also recognised by the drafters that codes of conduct can "have a wider field of application, to the extent that they are found acceptable by the courts"[213].

However, since that decision to avoid the complexities of drafting model agreements, various user groups (eg. Odette), Customs authorities (eg. New Zealand), national (eg. UK EDIA[214]) and international (eg. Tedis) organisations have drafted such model agreements. Indeed, by 1991, when the UN/ECE WP.4 adopted a new legal work programme in the area of electronic trading, which included the need to establish a `truly international interchange agreement', it was felt that the existing range of agreements:

"...present in many instances different solutions with respect to the topics addressed and often address concerns of specific relevance to the identified needs within the sponsoring industry, organisation, country or region. As a result...there is a possible barrier to international trade arising from the absence of an internationally acceptable form of agreement which may be adopted for use in commercial practice."[215].

One issue that requires consideration, therefore, is whether such an international model agreement is relevant to users needs, and whether the complete shift in focus from a `code of conduct'[216] solution to a standard contractual agreement was either correct or necessary.

---

212 UNCID, op.cit. supra n.7.

213 Thomsen, at p.155, in Thomsen, H.B., & B.S. Wheble, *Trading with EDI: The Legal Issues*, at p.155, IBC Financial Books 1989. Hans Thomsen was co-chairman of the UNCID drafting committee.

214 Unlike most agreements, the SIA is intended to be used without modification.

215 "To ensure reasonable harmonisation of interchange agreements and the development of an internationally accepted version for optional use", see `Commercial and legal aspects of trade facilitation - detailed action programme', TRADE/WP.4/R.697, 15 March 1991. A more detailed programme was adopted on 20 September 1991; TRADE/WP.4/R.781. For a general discussion of the work programme, see Wheble, B.S., "ECE WP.4 - EDI Legal Group Work Programme", paper presented at EDIFORUM, Pisa, Italy, 5 November 1991. See also Boss, op.cit. supra n.97, at p.541, who states that, until the WP.4 model is produced, users need to review "the compatibility of the goals of the model agreement and the needs of the user". However, this would seem to be sound legal advice for <u>any</u> agreement!

216 A code of conduct "may propose new laws, compile old laws, state general principles or elaborately present rules and regulations"; see Brown, R.W., "A Model Code for Transnational Commerce?", p117, Transnational Data and Communications Report, Vol.VII, No.2, 1984.

A review of the types of contractual provisions that exist within interchange agreements suggests that six diverse elements are currently present; and enables us to more accurately assess the relevance of such agreements[217].

When UNCID was drafted, it was seen as a `solid basis' upon which to draft interchange agreements. However, it was also described as:

> "a `bridging operation' while the relevant international organisations identified the required adjustments to national and international law, brought them to the attention of the politicians and secured action."[218]

Such statements, from the co-chairman of the drafting group, would suggest that when legislation has been amended to accept the use of electronic communications, then interchange agreements would no longer be necessary.

The review of existing interchange agreements, however, shows that only certain provisions relate to such `legal insecurities' created by statutory requirements; for example,

- Terms that redefine `writing' to include electronic messages, or where the parties agree not to challenge the validity of a message based on the absence of a paper document;

- agreement not to challenge the evidential admissibility of electronic records in a dispute.

When, at some future point, the law is appropriately amended, such provisions would seem to become unnecessary; although the need for the other elements would appear to be unaffected.

A second distinct element of interchange agreements covers the security concerns of the parties, such as acknowledgement of receipt, confidentiality and authentication provisions. It has already been noted, however, that the primary documentary source containing the specific technical security procedures should be the `User Manual'[219]. As already noted, where an `acknowledgement' is an automatic feature of the system, then such a term would seem to be superfluous.

---

217 Baum, op.cit.supra n.84, at p.55, distinguishes three broad categories: (1) contract formation issues; (2) requirements to operate EDI facilities etc., and (3) general contract considerations.

218 Wheble, B.S., "Creating Legal Relationships with Trading Partners", p.133, *The EDI Handbook* (ed. M.Gifkin and D.Hitchcock), Online Publications, Middlesex, 1988. See also Thomsen, H.B., "Interchange Agreements", p73-89, in Walden, op.cit. supra n.146.

219 See Section 6.3.2 above, and the SIA, op.cit. supra n.96, at p.1 of the `Explanatory Commentary'; the User Manual is also seen as "a suitable place to set down the legal requirements associated with the specialist, trade-specific messages".

In addition, the inclusion of `confidentiality' clauses could be seen as unnecessary, since it is an issue that would usually be dealt with in the underlying commercial contract, or, as in other forms of communication, not dealt with by prior agreement at all[220]. In the US, where `confidentiality' is not generally covered in standard trading terms, "a considerable majority of the...EDI community takes this position in its TPAs"[221].

As discussed in Chapter 2, modern data communications systems can be an extremely secure form of communications, particularly when compared to existing paper systems. It could be that the current inclusion of security provisions within the interchange agreement reflects a unrealistic trepidation with regard to the technology and the nature of the risks that can arise. It is possible, therefore, that as non-technical business users, and indeed the legal profession, gain greater trust and recognition in the inherent security of such communications systems, then such terms will disappear.

A third strand within the reviewed interchange agreements concerns the obligations imposed upon the recipient, usually specifying the actions of the recipient upon message delivery; for example, stating that the mailbox must be accessed at certain times, and the message processed within a certain period. Such obligations need to be decided within the specific trade/industry in which the communication occurs and therefore an international agreement would seem unable to comprehensively cover these issues.

A fourth recognisable element, covers clauses by which the parties agree to obligations designed to facilitate the relationship, such as maintaining a log of all messages sent and received. Such a provision is primarily an explicit recognition of the mutual need for security. In the absence of such a clause, both parties could still be expected to maintain some form of data log, as a normal procedure within any corporate data security policy. In the event of a dispute, if one party failed to maintain a record of messages sent and received, then they would be placed at a significant disadvantage[222].

The inclusion within a contractual agreement of terms that are primarily designed to facilitate a business relationship, rather than simply establishing enforceable obligations, is common. However, such issues could also be effectively dealt with through the parties explicitly or implicitly agreeing to abide by a code of conduct, such as UNCID.

---

220 Boss, op.cit. supra n.97, at p.551, states that "there is a quantitative difference in the electronic arena, where the parties possess the ability to rapidly access, consolidate and manipulate data". Note that a similar point was made by the UK government when it introduced the Data Protection Act 1984, which only applies to computer data; see further Chapter 4.

221 Baum, op.cit. supra n.84, at p.83.

222 Note, that the FINPRO, Odette and New Zealand agreements do not address the issue of evidence.

The fifth recognisably distinct element within such agreements deals with liability[223]. The general assumption in all the agreements is that the primary form of liability, arising from the trading relationship, will be dealt with in the underlying commercial contract for the goods and services. The sender is stated as being responsible for the accuracy of the message. However, this is inherent for any mode of communication, and could therefore be seen as an unnecessary statement. The only critical provision allocating risk within existing interchange agreements seems to concern the parties agreement to regard the actions of the third-party network provider as the responsibility of the message sender.

The sixth element within interchange agreements are the standard contractual provisions, such as force majeure and dispute resolution. A force majeure clause would seem an unnecessary repetition of what should appear in a standard underlying commercial contract, unless perhaps a qualifying provision is also included, whereby the parties agree to use alternative means of communication, in the event that the data network is unavailable. However, this would also seem to be a sensible security procedure which could be placed within the User Manual.

With regard to interchange agreements, it has been noted that:

> "..the use of a model interchange agreement can eliminate most questions as to the legal principles applicable to the transaction."[224]

However, as the previous analysis has noted, the amount of substantive legal principle established within the reviewed interchange agreements is not significant. In addition, it should be reiterated[225], that there remains uncertainty as to whether parties can contractually resolve certain legal insecurities arising in statute, such as the requirement for a `writing': For example, the EDI Council of Canada states, in its commentary to its model interchange agreement:

> "[I]t is not clear whether parties to an agreement may waive the requirements of the statute of frauds provisions of an applicable Sale of Goods Act for the purposes of litigation, or arbitration."[226]

---

[223] See further Section 6.5.2 below.

[224] Boss, op.cit. supra n.97, at p.540.

[225] See 6.1.3 above.

[226] Canada, op.cit. supra n.125, at p.13.

An interchange agreement will not bind a court when deciding questions of legal principle, nor the actions of a third party.

Overall, it can be submitted that only three of the six elements currently dealt with in existing agreements (ie. statutory requirements, recipients obligations and the liability of intermediaries) particularly benefit from a contractual arrangement. However, these issues could be placed within the underlying commercial terms and conditions[227] or the User Manual, rather than in a distinct communication agreement. While the other elements, could be dealt with through adoption of the UNCID code of conduct, or by following, during implementation, some form of checklist or guidelines[228].

6.4 Network provider contracts

When a company decides to communicate electronically with its trading partners, the current tendency, within the UK, is to make use of a value-added network provider (VAN)[229]. Therefore, as electronic messaging develops to cover a wider range of business communication functions, the contract with the network provider will assume greater significance in terms of ensuring `legal security'[230]. This section is concerned with the contract made between the network provider and its customer, the data user.

The following is an analysis of network provider contracts, based upon a survey of 26 such service contracts, from both Europe and the US[231]. The focus of the analysis will be on the range of `legal security' issues that should be considered by trading companies when negotiating the establishment of such a contractual relationship. The review will not, therefore, give detailed consideration to provisions which occur as standard contractual

---

227 In the US, one company simply includes a statement on its standard corporate purchase order: "All EDI transactions shall be as enforceable as if done using paper documents.", quoted in Baum, op.cit. supra n.84, at p.51, fn.67; see also Ford Motor Company's opinion, at p.102, fn.155. The ABA draft Model Electronic Payments Agreement (Working Draft 1.4, March 6, 1992) states that the agreement is designed to be `stand-alone', but could also be "extracted for use as an amendment to an existing Business Agreement, or incorporated as an integral part of a new Business Agreement", at p.3, para.9.

228 The Article Number Association (ANA), the largest UK EDI community, believes that the "functionality of an interchange agreement is dubious", and therefore does not recommend that its members use such agreements - Conversation with Tim Pryce, Tradacoms Executive, ANA; 13/03/92. The ANA is currently drafting a set of implementation guidelines for members: `Guidelines for establishing an Electronic Data Interchange Trading Relationship' [Draft], April, 1992.

229 See further Chapter 2. In France, the tendency has been to communicate directly via the public data network, see Moyse, Malcolm, "No room left for the middle-man", p.10, Financial Times, 8/8/90.

230 The security implications arising from dependency on a single network provider for data communications has lead some commentators to suggest `dual sourcing' as part of a security policy; stated by Adrian Stirrup, Ernst & Young, EDI 92 COMPAT, Paris, 2 June 1992.

231 See Appendix D1 for a list of the contracts, covering Email, EDI, database and general communication services. Appendix D2 contains a copy of the PMS DIALnet contract, as an example. Such communication contracts deal with many of the same issues arising in `Facilities Management' (FM) arrangements for computer services; see generally, Cook, Trevor, "Facilities Management and Other Computer Services Contracts", pp.130-141, in Edwards, C., N. Savage & I. Walden (eds.), *Information Technology and the Law* (2nd edition), Macmillan 1990.

issues. As with interchange agreements, issues of responsibility and liability will be considered primarily in Section 6.5.

6.4.1 Drafting Considerations

The Service[231a]

When planning the introduction of electronic messaging into a company, it is obviously important to have a clear perception of the intended role of data communications in the business, both current and in the future; and therefore the services that you would like the chosen network provider to offer.

Some of the trading partners with which the company communicates may be using either a different network provider, communication protocol[232] and/or a different message protocol[233]. The data user might therefore require the network provider to be able to interconnect or translate particular messages accordingly. The data user needs to consider the extent to which such services are guaranteed by the network provider. A provision should also specify the extent to which, and procedures whereby, the data user may modify specific message formats[234].

In addition to the communication service, the network provider usually provides associated services, such as support staff to assist the data user during the initial stages of implementation:

> "The Company [Network Provider] will at any time within a period of three months from the Contract Date make available at the Company's premises or....at the Client's Site an implementation support representative"[235]

After this period, the data user can usually obtain such services upon additional payment of consultancy fees. Many of the network providers also offer `fault reporting desks', coupled with a guaranteed response time[236]. The data user needs to consider whether the scope of this service will realistically complement the company's planned implementation; for

---

231a See generally "Comparison of major VANs", p.12-13, *Electronic Trader*, May 1992.

232 Eg. X.25, X.400 and C03.

233 Eg. EDIFACT, Tradacoms and ANSI X.12.

234 See further Chapter 2, at 2.2.3.2.

235 Istel Computer Services Agreement, at clause 2.3.

236 Ibid., at 2.5.

example, if the system is intended to operate 24 hours a day, will such assistance be provided outside of normal working hours[237].

Within the competitive data communications market, network providers will be concerned to offer the most efficient and up-to-date service. As a consequence, this has meant the inclusion of the following type of clause in some contracts:

> "The Company [Network Provider] reserves the right to withdraw or modify any particular service in the interest of maximising the effectiveness of its services"[238]

However, maximising the effectiveness of the network service as a whole might be of disadvantage to the data user's business, which has a particular need of the service that is to be withdrawn. These clauses do not usually provide for a period of notice before such actions are taken. Data users should, therefore, obtain some guaranteed notification period; otherwise, in data security terms, the modification to the service could seriously impact on the availability of communication links to the business. A notification period is also necessary to enable the data user to choose whether to remain with the network provider or move. Similar considerations also arise with respect to the notification of price adjustments.

Another means by which the network provider may control or vary the quality of the service, is through the periodic imposition of instructions concerning the use of the service. In some contracts, such instructions, when issued, are deemed to form part of the contract[239].

Where the data user and the network provider are multinational, restrictions may be placed on the use of the service by the data user outside of the national jurisdiction where the agreement was made. However, such use is usually permitted upon written application[240].

One network provider agreement specifically restricts the types of uses made of the data sent via the network:

> "..it [Data User] will use the services provided by the Company hereunder essentially for data processing and that any use of said service for communications shall be incidental to and an integral part of such data processing."[241]

---

[237] Eg. IBM's General terms and conditions for information network service [RNS], Annex X, Clause 2(c): "If desired, the Help Desk Service can be made available for longer than provided for in the RNS Service Description by special arrangement on a case-by-case basis."

[238] GE Informations Services Multinational Access Agreement (MNA), at clause 2; and Agreement for Computer Services (US). See also Control Data Co. Data Services Agreement, Schedle AA7775, at clause1.

[239] British Telecom Dialcom Service, at clause 3.

[240] Geisco (US), op.cit. supra n.238.

Such a clause is designed to prevent the use of the service for Email, free format, style communications, instead of pure EDI computer-to-computer applications.

When choosing a data communications strategy, data users need to bear in mind that direct data communications with trading partners, via the public data network, is a potentially viable alternative to the use of a third-party value-added network provider, and can be significantly cheaper[242]. It is therefore important that data users are clear of what real `value-added' services are provided in the contract for the cost[243].

Data user obligations

Most of the network agreements place primary responsibility for the accuracy of the information, submitted by the data user to the service, upon the data user:

> "The User shall be responsible for the accuracy of the data and addressing and proper use of passwords within the Transmissions..."[244]

One network provider states that it can give no assurances as to the accuracy of the messages "since errors or omissions may occur during transmission of a message through the Networks over which the Company has no control".[245]

As part of the data user's responsibility to correctly address the messages, he may have to "establish and maintain a list of Trading Partners with whom it has agreed to exchange Transmissions", for the network provider[246]. Such a clause could militate against the development of `open-EDI', where a data user is able to establish a commercial relationship with a data user with whom he has had no previous contact[247].

---

241 Geisco (MNA) op.cit. supra n.238, at 5.

242 It is estimated that use of the public data network can cost 40% less in set-up and running charges to that of a VAN service. see Moyse, op.cit. supra n.229 The retail group, WH Smith, send all their intra-company EDI invoices, for one division, via one magnetic tape per month, at a cost of about £12: Interview with Philip Holt, Senior IT Consultant; 25/09/90.

243 See Snyder, D.M., "Service level agreement in network services", p.93-101, in Proceedings of `Networks 91: Current Issues', Birmingham, June 1991.

244 INS Tradanet UserContract, at 4(a).

245 One-To-One Co. Standard Terms and Conditions, at 6(H)(b).

246 British Petroleum EDI Network Services Contract (draft), at Schedule A.3.

247 See further Chapter 2, at 2.2.4.

The content of the message may also be the subject of contractual provision, for example, in certain Email services where the messages are human-readable. The data user may be required to ensure that the service will not be used:

> "for sending to any persons any message or communication which is offensive or abusive or of an indecent obscene or menacing character.."[248]

Such harassment can also extend to the persistent sending of messages for the purpose of disturbing another person. However, the monitoring by the data user that such a provision implies, could give rise to the types of privacy violation cases that are currently being pursued by employees in the US[249]. In addition, where the network provider provides an information service (eg. an on-line database), then it will often exclude liability for the accuracy of the information contained within the database[250], and/or even attach conditions to the use of such information[251].

When a company establishes data communications, it may require the purchase of dedicated equipment, hardware and software. Communications and messaging software will usually be obtained either from the network provider; a software house, or can be developed in-house. In a number of the contracts, the use of all data user-provided equipment might require a process of validation before connection, to ensure compatibility:

> "BT's acceptance of the Customer's order is subject to the testing of the Customer's EDI Translation and Communications software by BT."[252]

In some agreements, the cost of such validation is borne by the data user.[253] The network provider will also usually require notification of any changes in the equipment used.

Where the service includes the provision of equipment by the network provider, then the network provider will usually reserve the right to enter the data user's premises to attend to such equipment. However, due to possible commercial sensitivity, as well as inconvenience, such access may have to be qualified by a notification period.

---

248 Dialcom, op.cit. supra n.239, at 4(1)(a); see also AT&T Messaging Service Agreement, at 4(c). See also *Cubby v CompuServe*, 776 F.Supp. 135 (SDNY 1991).

249 See Chapter 4: Data Protection, at 4.6.1.

250 Eg. Control Data, op.cit. supra n.238, at 7: "..makes no representations or warranties as to the accuracy, content or availabilty of the information contained in any data base made available..".

251 Eg. CCN Systems Ltd: Terms and Conditions, at 7(a): "Information provided by CCN to the Client must not be used as the sole basis for a business decision of the Client".

252 BT's Terms and Conditions for EDI*Net Service.

253 INS, op.cit. supra n.244, at clause 4(a).

Once electronic messaging has been implemented and run successfully for a period of time, as with information technology generally, the business usually recognises other areas of the business that could benefit from such communications. Obviously, such additional uses could significantly alter the volume of messages sent and received, and the network provider might require adequate notice of such volume changes; for example:

> "The User shall give INS as much notice as is reasonably possible of any significant change which he expects to make in the average volume of data per calendar month which he submits to the Tradanet Service."[254]

Finally, a number of the agreements make reference to the fact that the network provider is operating under licence from the national government or appropriate telecommunications authority. The data user is therefore required to either abide by any relevant licence conditions, or to ensure that they do not act so as to endanger the network provider's authority to operate.[255]

System access and ownership

The availability of information and processing resources is one of the major elements of data security: are the resources available when they are needed? It may be critical to the data user to obtain, in advance, detailed specifications regarding the form of access and availability to the network, guaranteed by the network provider. Whether the network offers 24 hour up-time, for example, may be of critical importance to some types of data users, such as those involving electronic funds transfers; while for some SMEs, sending invoices and purchase orders, a guaranteed minimum number of hours (eg. 9am-5pm), may be satisfactory for their purposes:

> "The Company warrants that the Service will be available during the specified transmission times....except during periods of preventative or emergency maintenance.."[256]

Network availability should be sub-divided into:

- Service hours, ie. general operating periods, and

---

254 Ibid., at clause 4(e).

255 Eg. British Petroleum Co. Plc.: EDI Network Services Contract, at A.8: "The User shall not do any act or thing which might cause the Network not to be able to comply with the General Licence issued under section 15(1) of the Telecommunications Act 1981...."; Control Data (US), op.cit. supra n.238, at 5(a): "Customer agrees to abide by the rules and regulations of the International Telecommunications Regulatory Agencies...".

256 Istel, op.cit. supra n.235, at 6.2.

- System up-time, ie. the availability of the network during service hours (network capacity)[257].

System up-time specifications are often detailed in attached schedules, detailing the service. Where the network provider fails to provide the contractually specified up-time, the data user may be offered a reduction in charges[258].

The network provider obviously has a significant amount of control over the data once it has been placed in the network, ie. the route through the network(s), any translation the message may undergo and the point at which it is sent to the receiving mailbox. In some agreements, it has been thought necessary to explicitly state that the network provider has no ownership over the data sent by the client:

> "All data submitted to the Tradanet Service by the User shall remain the sole property of the User..."[259]

One of the value-added services offered by the network provider might be to maintain an archive record of all data sent and received by the EDI user[260]. If this is the case, the data user may demand that a clause be included in the contract requiring that any such records be kept under certain conditions, such as being stored separately from that of other clients; for example:

> "all records, data and files stored by the Service Provider as archives of Customer's data, including the media on which they are stored, are the exclusive property of Customer, and Service Provider may assert no lien on or right to any of the same. Service Provider will conspicuously mark all such archival storage media as Customer's property. At Customer's request, Service Provider will, for [a certain fee], promptly deliver the same to Customer."[261]

The network provider, in addition to its communication service, might offer gateway access to various international database services, such as Reuters `Textline' or its own information

---

257 See `The Liability of Electronic Data Interchange Network Operators', at p.87-89, Tedis final report, July 1991.

258 Eg. Geisco MNA, op.cit. supra n.238, at 8: "the total charge to Customer for the month....will be reduced by a percentage derived from a ratio the numerator of which is the number of hours by which the available hours was less that the specified system up-time, and the denominator of which is the specified system up-time."!

259 INS, op.cit. supra n.244, at 6(a).

260 Eg. SWIFT maintains all messages in an on-line retrievable state for four months after being sent. Source: van Leeuwen, D., "SWIFT initiatives for EDI and cross border payments", paper presented at *1992 Progress in Electronic Trade Payments*Conference, 7-8 July 1992.

261 quoted in Wright, B., op.cit. supra n.106, p.39.

service, and therefore the data user will require the right to access and use such information, in addition to any copyright aspects.[262]

Confidentiality and Security

> "It is a common misconception that making the network private, as with VANs, makes it more secure"[263]

The quote above appeared in an article describing the use of data communications in France, where most companies transmit data over the public data network rather than make use of third-party value-added network providers. The technical reality behind the assertion is the fact that the primary aspect of control over transmitted data is through elements built into the communication protocols and messaging standards, integral to the transmission process, and potentially independent of the network carrier[264]. The security procedures offered by third-party network providers, therefore, tend to be external controls over the data.

The maintenance of data confidentiality will be an obvious area of concern for both the data user and the network provider. Nearly all of the information sent via the network will concern the data user's business, as well as his clients, and therefore the network provider should be required to maintain all such information in confidence.

In the United Kingdom, there are statutory requirements placed upon the network provider to take "all reasonable steps to safeguard the privacy and confidentiality of any Message conveyed for a consideration"[265]. In addition, under certain licences, the network provider is expected to abide by a code of practice regarding the confidentiality of client information, and pass it on to the user[266]. In the US, the Electronic Communications Privacy Act[267] covers any communication service which provides "wire or electronic communication services for computers"[268]. The Act creates a federal criminal offence of access to a system without authorisation, or by acting beyond existing authority. In addition, service providers

---

262 Eg. PMS Communications: DIALnet User Contract (see Appendix D2), at 2.3: "PMS grants the User a non-transferable right to obtain access to, process and use for its own internal purposes information provided via the DIALnet, which may be made available to it by PMS from time to time".

263 Moyse, op.cit. supra n.229.

264 See further Chapter 2.

265 Condition 19 of the Branch Systems Licence and Condition 7.1 of the UK VADS licence; see also Chapter 3, at 3.3.2.2.

266 Ibid., at Condition 16 of the VADS licence. OFTEL has published a model code of practice on confidentiality which must be adopted, unless the licensee drafts its own version and obtains OFTEL approval for it.

267 18 U.S.C. § 2510-21.

268 Ibid., at § 2701 *et seq.*

can not knowingly divulge the contents of a communication stored or processed electronically unless permitted by contract.[269]

The parties should also be aware of any other legislation which should be taken into account, such as obligations brought under data protection legislation:

> "The Company undertakes to comply so far as is necessary with the Data Protection Act 1984, and shall procure that its personnel, sub-contractors and agents shall observe the provisions of that Act"[270]

It would be up to the parties to the agreement to decide whether detailed procedures regarding confidentiality and security are to be included in the contract; for example, one network provider in the US requires that EDI users mark all data which is to be considered confidential[271]. Another agreement requires the data user to designate all confidential information `in writing'[272]. However, these requirements may be felt to be too onerous a responsibility for the user, who would prefer a general `catch-all' confidentiality clause.

The corollary of the data user being responsible for the accuracy of the data, is an obligation upon the network provider not to alter the submitted data, except perhaps "to the extent necessary for performing conversions of protocol or of data structure....so as to make such data available to its intended recipient in a standard and acceptable format"[273]. An additional obligation concerning data alteration, designed to protect data confidentiality, is for the network provider to guarantee that data will not be converted, at any time, into a `human-readable' format[274].

---

269 See Nimmer, R.T., "Legal obligations of the EDI Service Provider", p.8, paper presented at EDI & the Law, Washington, Feb. 1991.

270 Istel, op.cit. supra n.235, at 3.6(b). See Section 6.2.3. above. See also Article 7(1) of the European Commission's "Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and public digital mobile networks" (SYN 288), which imposes a duty of confidentiality on telecommunications organisations.

271 Comment made by Carlsen, R.C., "Network and User Responsibilities: A contract perspective", paper presented at EDI: Letters of the Law, Dallas, Texas, 15-16 February 1990. The confidentiality of a message can, in effect, be flagged to the network provider within some communications protocols by the use of certain forms of `enveloping'; see further Hill, op.cit. supra n.111.

272 McDonnel Douglas Co., EDI*Net Communication Services Agreement, at X(E). Baum, Michael S., Henry H. Perritt, JR., *Electronic Contracting, Publishing and EDI Law*, p.125, Wiley Law Publications, New York, 1991, states that most service provider agreements require confidential information to be designated, this is not the case within the UK agreements reviewed by the author.

273 INS, op.cit. supra n.244, at 6(c).

274 Ibid., at 6(d), "save to the extent necessary to facilitate recovery from a failure in the Tradanet Service, by producing a computer store dump or disk dump or store print with the User's permission". See also the Council of Europe `Draft recommendation on the protection of personal data in the area of telecommunications services, with particular reference to telephone services', final activity report of Working Party No.9, February 1991 (CJ-PD (91) 2): Article 10.1 states that "Unless authorised for technical storage or message transmission reasons...authorised by the subscriber, any interference with the content of communications...is prohibited".

The parties will probably agree obligations regarding the maintenance of back-up data and its reconstruction in the event that data is lost during some part of the transmission. The cost of retransmitting the message will usually be borne by the network provider, if they are responsible for the failure. The data user might be required to maintain copies of all messages sent until their correctness has been verified:

> "The Customer agrees to maintain a duplicate copy of every EDI message sent using the Service until it has been successfully received by the intended recipient"[275]

Alternatively, the network provider might be able to restore a particular message from archive records[276]. If, for reasons of data confidentiality, the data user wants the network provider to erase all data sent by the user, then the timescales for this process will have to be agreed, and it might be felt necessary to outline what `erase' means in terms of the network[277].

Some of the agreements make explicit recognition of the viewpoint that no security policy can prevent all losses or alterations to data, particularly through unauthorised access, and although warranting that security measures have been implemented to safeguard against such occurrences, no guarantees can be made:

> "INS warrants that it has built into the computer programs....checks and controls designed with a high degree of professional competence to detect and prevent unauthorised access to User data...INS does not, and cannot, guarantee that a third party could not gain such unauthorised access.."[278]

Access to the network will be through some form of identification system. The parties will therefore be concerned with the distribution of such access codes, and the subsequent protection given:

---

[275] BT, op.cit. supra n.252, at 2.2. A more stringent clause is imposed under IBM's General terms and conditions for information network service:

> "20. The Customer is responsible for developing and/or maintaining procedures, external to the Service, to safeguard its programs and data, and for the back-up and reconstruction of lost data, programs or procedures."

Baum, op.cit. supra n.84, at p.128, states that in the US most service providers do not expressly impose data retention obligations on customers.

[276] Eg. Geisco copy "every document that is sent into a second file which cannot be altered.", p.4, Hunter, B.E., "Legal Responsibilities of EDI Service Providers: A Service Provider's Perspective", paper presented at EDI & the Law, Washington, Feb. 1991.

[277] See Wright, op.cit. supra n.106, at p.41: "`Erase' means to render the relevant data unrecoverable by all means.

[278] INS, op.cit. supra n.244, at 6(f). Control Data, op.cit. supra n.238, at 5(c) states that although "Reasonable precautions have been taken", they "cannot guarantee their [programs and data] integrity and security"; likewise with CompuServe: Computer Services Agreement (US), at 4(b).

"IBM will provide USERIDs to enable access to the Services. The Customer is responsible for the control and distribution of its USERIDs to its end-users. IBM shall have no liability for any misuse of the USERIDs by any party not under IBM's control...."[279]

Obviously, the degree of security required depends primarily on the nature of the information being sent. However, the data user might wish to have some guarantees laid down regarding the effectiveness of the security procedures carried out by the network provider. In the UK, for example, the Department of Trade and Industry has recently established a new national scheme for the security evaluation and certification of IT systems and products[280]. The data user might request that the network provider obtains such a certificate to the operation of the network.

Audit

"An audit is the examination of an activity...and the expression of an opinion on the quality of performance of the activity, conducted by people who are independent of the staff responsible for the performance and supervision of the activity."[281]

The data user is likely to want to see a system audit record of the network provider's network during the initial process of choosing a particular communication service, in order to assess the security and confidentiality function of the specific network. Most network providers offer such a document as part of their marketing strategy.

Audit records will usually form, therefore, part of the pre-contractual negotiation stage for the service. However, the data user may also want to include a clause in the service contract stating that the network provider will provide details of any subsequent, or periodic (usually annual), audit carried out. For additional security, the data user may even demand the right to nominate a particular external auditor[282].

---

279 IBM, op.cit. supra n.237, at Art.7.

280 See DTI Commercial Computer Security Centre, "Commercial Systems Integration - A Technical Discussion", Version 1.0, 27 May 1992. See also Chapter 2, at 2.3.4.

281 List, W., "Audit", p72, Proceedings of the EDI and the Law Conference, London, 4 July, 1990. See also Goetzman, J., "Audit and Security Responsibilities: An EDI Service Provider's Perspective", paper presented at EDI: Letters of the Law, Dallas, Texas, 15-16 February 1990.

282 See "Audit - Problems facing users of networked services", pp.32-46, in `A Service Infrastructure for EDI Security', TEDIS final report, December 1991.

Recent legislation in France, has permitted companies to send electronic invoices to the tax authorities[283]. As part of the approval process, the authorities reserve the right to `audit' the communication system of the data user. However, this has been widely defined to include the data user's network provider. In such circumstances, the network provider contract could establish some form of contractual recognition of this obligation. The carrying out of such an audit would be particularly problematic where the network provider is based in a different country[284].

Contractual provision for system/security audit records do not appear in any of the reviewed agreements; probably reflecting the network providers' generally cautious commercial perspective. However, the requirement might be suitably placed within the general service description, attached to the body of the agreement as either a schedule or appendix[285].

Related to the issue of system audit, it can sometimes be difficult for the data user to verify his network bill, especially if the service is charged on a per number of characters basis. The data user could therefore require the provision of appropriate software/equipment that can provide an independent record of charges that have accrued. Obviously, in the event that the network provider's summary statement of charges and invoice does not equate with the data user's internal record, then there will have to be provision for resolving such issues.

Internetwork Connections

Obviously, as the use of data communications expands into all aspects of business communication, data users will increasingly submit messages to their network provider, to be passed onto the recipient, via a different third-party network provider; indeed potentially through many such third-party intermediaries, particularly in international trade[286].

Such internetwork traffic raises some important legal security issues, in terms of the legal relationships that exist between the network providers, and between the data user and the

---

283 Loi de finances rectificative pour 1990 (No.90-1169 du 29 décembre 1990), Journal Officiel du 30 décembre 1990 on 31st December 1991.

284 Eg. the IBM and Geis networks are based in the Netherlands.

285 Both INS and IBM conduct an annual audit of network performance, which is made available to customers within the marketing materials, or upon request. It would appear from conversations with industry members that such an informal arrangement is the norm.

286 Currently in the UK, there has only been interconnection between INS and Geisco, since 1988, and INS and Istel, since 1989 (for only one customer!). The VANs have claimed that there is no real demand from users for such interconnections; however, the six main UK X.400 service providers have recently announced plans for an interconnection service: "X.400 aims for easy messaging", p.2, Computing, 13 Feb. 1992. For the current state of interconnection in Europe, see "Service Providers Cooperate on X.400", Telecommunications, p.15, April 1991. In the US, the range of interconnections is considerably wider; see `X.400 Interconnect Matrix', Electronic Messaging News 7, Jan. 23, 1991. The European Electronic Mail Association (EEMA) issued a draft `Memorandum of Understanding' at a meeting in The Hague in November 1990, which requires signatories to "complete specifications for the interconnection of message handling systems".

remote network providers. Such developments could mean the creation of a complex nexus of legal agreements between all the parties. The European Commission, under the Tedis programme[287], has recently awarded a contract to establish a EDI interconnectivity service for all the European network providers[288]. If such a scheme succeeds, then network providers may only need to contract with the provider of the central communications hub.

However, if data users perceive the need for internetwork traffic, then they need to ensure that the network provider with whom they are contracted, has established adequate contractual relations with the other network provider, to cover such issues as:

- guaranteeing that security procedures, such as encryption, are maintained throughout the communication process[289];
- liabilities and indemnities with regard to the actions of remote networks[290];
- error identification, notification and resolution;
- acknowledgements[291];
- and the implications for the audit trail.

The data user may require that they receive a copy of the interconnection agreement, under which such arrangements have been made, as part of the system documentation.

Miscellaneous

(a) EDI-specific clauses

In the event of a dispute, the data user may wish to submit certain records held by the network provider as evidence. In such circumstances, the network provider might be required to produce an appropriate certificate establishing that, at the time the record was produced, the network was functioning correctly[292]. The ability to produce such a certificate could form a contractually agreed obligation[293].

---

287 op.cit. supra n.98.

288 "Interconnectivity contract placed", p.4, Electronic Trader, Vol.II, No.IV, February 1992.

289 An Istel spokesman, at EDIA's Oil Industry Section Open Day [24 April 1990], stated that when messages were sent between Istel and INS, all encryption protection was removed. In the US, this is described as the "dump and pray" technique; see EDI News, Vol.6, No.5, March 9, 1992.

290 Eg. BT's Dialcom, op.cit. supra n.239, at 12(2) states: "BT undertakes no liability whatever....for the acts or omissions of other providers of telecommunication service outside the United Kingdom...".

291 See Baum, op.cit. supra n.84, at p143 - Acknowledgements can be (i) negative: when a problem is discovered; (ii) a positive delivery report; (iii) an end of transmission notification, or (iv) an interconnect mailbag acknowledgement (eg. the EDI Mailbag, X12.56 standard, for moving transactions between networks).

292 See Chapter 5, at 5.3.2 .

293 Eg. BP, op.cit. supra n.255, at B.2: "...It is expressly agreed that the Network shall, being aware that the provisions of section 10 of the Finance Act 1985 apply in respect of any computer user for transmission of invoice data,....provide a certificate in accordance with Part 1 of the Civil Evidence Act 1968 if so required by the Commissioners of HM Customs and Excise".

In addition, in a dispute, the data user might have to show the court what the service was composed of, and its detailed functionality. The data user should therefore ensure adequate access to all the service providers system documentation:

> "Company will provide Customer with manuals, instruction books, and other relevant documents in accordance with Company's current Price Schedule"[294]

Such a documentation clause should, of course, cover any relevant versions of the system documentation that might enable the data user to determine the functioning and reliability of the network.

The data user might also want to restrict the use of its name in any promotional material produced by the network provider:

> "The Company shall not disclose the making of any agreement between itself and the Client, in any journal, magazine, or publication, list of customers or otherwise with the prior written consent of the Client"[295]

(b) Standard contract terms

Certain elements of the communication system, such as the software, and certain data sent via the network, will the subject of intellectual property rights, primarily copyright or patent. It is usual for the network agreements to cover such issues in two ways:

- The parties agree not to act in any way so as to challenge or infringe any rights held by the other party, with respect to the components of the service or the information exchanged;

- the parties will indemnify the other party against any actions brought by a third-party, arising out of the use of information or equipment provided to it by the other party.

It is also important that the parties include rules within the contract to deal with the termination of the service, such as ensuring that confidentiality procedures are maintained and audit records returned. Some US agreements state that, where a contract is terminated,

---

294 Geisco MNA, op.cit. supra n.238, at 17(c).

295 INS, op.cit. supra n.244, at 7.10.

the network provider reserves the right to dispose of any of the data user's information still held in the network providers system, unless alternative prior arrangement are made[296].

6.4.2 Comment

All but one of the reviewed contracts represent the standard terms and conditions upon which the network providers offer the service; they are therefore clearly drafted from the perspective of their concerns. Unlike with most interchange agreements, none of these contracts were drafted by independent organisations. As with much IT purchasing, purchasers tend to be primarily concerned with choosing the right products and services and, once the decision has been made, they tend simply to accept the suppliers terms and conditions[297].

As in any contractual relationship, the ability of the parties to influence the terms and conditions under which the service operates will be a factor of their respective bargaining strengths. From the data user's perspective, such strengths can be substantially enhanced if the approach to the network provider is made through membership of an industry group, or an established set of trading partners. In the US, for example, the Aerospace Industries Association (AIA), in 1988, informed the eight main EMail service providers that:

> "if they did not provide timely, standardized (X.400) interconnections among themselves to enable their customers to communicate with one another, AIA members would independently interconnect and terminate their respective TPSPAs [Third Party Service Provider Agreements]"[298]

Such a strategy met with complete success!

6.5 Responsibilities and liabilities

6.5.1 Background

Commercial relationships usually give rise to obligations and responsibilities on behalf of the business. In data communications, there are three primary parties typically involved upon

---

296 Eg. Control Data, op.cit. supra n.238, at 6(d).

297 See Kemp, Richard, "Public Sector IT Acquisition", The Journal - Local Government, Spring 1991.

298 Baum, op.cit. supra n.84, at p.110.

whom responsibilities devolve: the message sender, the network-communications provider and the recipient of the message[299]. These parties will be concerned with four major risks:

- The transmission of incomplete or falsified data to the recipient;
- the transmission of the data to an erroneous recipient;
- the transmission of the data by an unauthorised sender;
- delay in the transmission of the data.[300]

This section briefly reviews the kind of liabilities that can arise from these risks, with specific reference to the forms of contracts already discussed in this chapter.

Under English common law, the message sender will be responsible for ensuring that all messages are properly authorised. If the sender provides an employee with ostensible authority to act on behalf of the company, such as initiating an electronic funds transfer, then the sender will be liable at common law for any subsequent fraud committed by that authorised employee[301].

The message sender is also responsible for ensuring that the contents of the message is correct, since a mere mistake will not render a contract void[302]. Where the message received is substantially different from that sent, and neither party is aware of the corruption, the mutual misunderstanding will prevent an enforceable contract from arising[303].

Two main categories of damage are usually distinguished as resulting from a breach of contract: direct and consequential[304]. Due to the potentially unlimited and unforeseen nature of consequential damage, companies tend to expressly exclude responsibility for such damages, and often place limits on the amount of damages available under the former category.

---

299 The contractual nexus of responsibilities and liabilities in data communications is obviously much wider, covering for example the supplier of the communications software, but such aspects are beyond the scope of this thesis.

300 Elias, Lieve, "Data security and formation of contracts", paper presented at `Data Security in Computer Networks and the Legal Problems' Conference, Hannover, 23-24 September, 1991; see also Chalton., S., "The Authentication of the Origin and Content of Paperless Transactions, and Questions of Liability in Common Law", p103, Proceedings of CELIM Conference: `Paperless Trading & the Law in the EEC', Brussels, March 17-18, 1986; Mosteshar, S., "Liability Issues in EDI", pp.49-55, in Walden, op.cit. supra n.146; Tapper, C., "Liability Issues", pp.95-102, in Proceedings of `Data Security & the Law' Conference, London, July 1991; Linant de Bellefonds, Xavier, "Les EDI: questions de responsabilité", pp.115-130, in *Le Nouveau Droit Des EDI*, op.cit. supra n.209; and Allen, Thomas, "Electronic Data Interchange, computer ordering and the formation of contracts", pp.10-13, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

301 *Lloyd v Grace Smith & Co.* 1912 AC 716.

302 The message sender may be able to avoid the contractual obligations, where the recipient is aware of the mistake and yet decides to act upon it; see *Hartog v Colin & Shields* 1939 3 All ER 566.

303 *Raffles v Wichelhaus* 1864 2 H&C 906. Where a mistake is made by an intermediary, such as a network provider, English case law suggests that the offeror may not be bound; see *Henkel v Pape*, (1870) LR 6 Ex 7., where the court held that the buyer was not responsible for a mistake made by the telegraph company.

304 Also referred to as `indirect' or `incidental' damages. The damage is often in the form of lost profits.

In certain circumstances, the court may declare that a particular contract has been `frustrated', and will terminate the contract without attributing fault or liability[305]. Frustration is usually said to occur when an intervening event, such as a destruction of the subject matter[306], removes the purpose of the contract. Supervening illegality could also be a cause of contract frustration, for example, if a company contracted to send personal data to a US company, but was then prevented from doing so by the Data Protection Registrar, the contract could be frustrated. This would not be the case, however, if the Registrar simply required certain conditions to be fulfilled, which would make the contract more expensive or difficult to carry out[307].

6.5.2 Communication agreements

The survey respondents[308] were asked whether any special liability arrangements existed for the use of EDI:

> "As normal. What is special about EDI?"

> "Terms of underlying commercial contract would prevail"

The majority of responses fell into the category illustrated by the quotes above: data communication systems do not give rise to significantly additional liabilities.

However, the scope of any liability clause depends on the perceived nature of an interchange agreement. The SIA does not include an extensive liability clause, since it is assumed that any damage that arises between the trading partners will be due to a breach of the underlying contract, or in tort (through negligence), not through the means of communication[309]. Indeed, as a US study of companies implementing electronic trading noted, companies "did not adopt the technology with an expectation they would introduce substantial risks"[310]. Most interchange agreements have followed this general perspective:

> "this Agreement shall not be used to impose liability for consequential damages or in any other way to increase the liability of either in the event of a failure to perform its

---

305 The Law Reform (Frustrated Contracts) Act 1943 specifies the precise application of loss.

306 Eg. *Taylor v Caldwell* (1863) 3 B&S. 286 Queen's Bench; S&T. 406.

307 Eg. *Davis Contractors Ltd v Fareham UDC* (1956) AC 696; 2 All ER 633, CA.

308 See Appendix B3.

309 SIA, op.cit. supra n.96, `Explanatory Commentary', p.2.

310 ABA report, op.cit. supra n.100, at p.92.

obligations under a Contract, beyond what it would have incurred for a breach of the Sales Agreement.."[311]

However, some agreements have explicitly attributed liability for the direct damage arising out of a failure by one of the parties to abide by the provisions of the interchange agreement:

"The Bank shall be liable to the Customer for actual losses suffered by the Customer as a direct result of the Banks negligent performance of the Service provided that such liability is limited to (i) the actual cost of reprocessing Instructions to correct such negligent performance and (ii) any additional costs necessary to prevent a recurrence of the same..."[312].

The basic aspect of liability inherent in any agreed method of communication is that the sender will be responsible for the completeness and accuracy of any messages[313], and therefore this could be explicitly stated in the interchange agreement for clarity. However, a dominant trading partner could even exclude responsibility for accuracy[314].

Within the UK EDI Association's standard agreement, the only slight qualifications to the sender's liability for message accuracy is

- where the relevant mistake was caused by technical faults[315];
- or where the mistake should have been, in the circumstances, `reasonably obvious' to the recipient[316].

All the agreements require that, in the event of a incorrect/garbled message being received, the recipient must inform the sender as soon as possible, or the sender is entitled to act if the message were correct[317].

The Australian Agreement also imposes severe liability clauses with respect to the implementation of effective security procedures:

---

311 Canada, op.cit. supra n.125, at 8.01. The IBM agreement, op.cit. supra n.133, also states that they will not be liable for damage "caused by the Supplier's failure to perform its security responsibilities".

312 See NatWest, op.cit. supra n.183, at 15. However, such `financial' communication agreements can be seen as unique, to the extent that one of the data users (ie. the bank) views the ability to interchange data as a service in itself, rather than simply as a adopted mode of communication. However, see also CCC `Guidelines Concerning Customs-Trader Data Interchange Agreements and EDI User Manuals', at p.19, para. 3.12.

313 Mosteshar, op.cit. supra n.299, at p.52, para. 4.2.2.

314 British Aerospace Agreement, at clause 6.

315 SIA, op.cit. supra n.96, at 5.2 "...unless such Messages can be shown to have been corrupted as a result of technical failure on the part of machine, system or transmission line".

316 Ibid., at 5.4: "...the sender will not be liable for the consequences of an incomplete or incorrect transmission if the error is or should in all circumstances be reasonably obvious to the recipient. In such an event the recipient must notify the sender thereof."

317 Eg. TPA, op.cit. supra n.97, at 2.4.

"7.2 Each party shall be responsible to the other to prevent unauthorised access or transmissions and shall be liable for any costs or consequences which flow therefrom"

Since no security measures are considered to be absolutely secure, such a provision seems excessively harsh and goes against the general trend to require `adequate' or `appropriate' security measures[318]. In the ABA draft `payments agreement', liability for consequential damage is excluded except when arising from a breach of the confidentiality or the security provisions.[319]

If no new liabilities are seen as arising under EDI, then the logical consequence is that there should be no need to make special insurance arrangements. However, as with the use of IT in business generally, it has been suggested that data users should insure against the following possibilities:

"1. Additional costs and business interruption caused by
   - property damage to receiving/processing equipment..
   - errors/defects in receiving/processing software..
2. Reconstruction costs for data and programs..
3. Intentional illegal enrichment.."[320]

The UK's SIA recommends that EDI users inform their insurers of their intention to engage in EDI transactions so that they are aware of the situation[321]. Indeed, if a company can convince its insurance company that the use of data communications will lead to a reduction in commercial risk, due to factors such as fewer keying-in errors, then lower premiums may be negotiated! Some agreements include an insurance-related clause, imposing a positive obligation to ensure that suitable insurance arrangements have been made[322].

A `force majeure' clause is common in most contracts, stating that neither party will be responsible to the other for loss arising from what is often termed an `act of god', ie. a disruptive factor which is considered to be outside the control of the parties, such as floods. A clause might be included in the IA, imposing a duty on the party which has suffered an `act of

---

318 See Chapter 4, at 4.4.2,

319 MPA, op.cit. supra n.227, at §.7 and §.8.

320 Rettig, Dr. and Dr. Otto, "Insurance Coverage and EDI", p.3, paper presented at `*Data Security in Computer Networks and the Legal Problems*' Conference, Hannover, 23-24 September, 1991; Davies, David, "EDI Insurance - The `Red Herring' Theory Examined", in Proceedings of the *6th Annual Canadian Law Conference*, London, 1 November 1991; and Neilson, A., "Insuring against the inevitable", pp.195-200, *Data Security & the Law* Conference, 8 May 1992. See for example, `Electronic and Computer Crime: A Program of Insurance', by Underwriters at Lloyd's, 1983.

321 SIA, op.cit. supra n.96, at `Explanatory Commentary', p.2.

322 NHS (UK) Draft Interchange Agreement, at clause 20.

god', preventing EDI communication, to use a reasonable alternative means of communication:

> "In the event of a breakdown in or interference with the agreed means of communication the parties to this agreement shall immediately use every endeavour to communicate by other expeditious means"[323].

As mentioned in Section 6.3.3, in all the reviewed agreements, the parties are held to be liable for damages arising out of the actions of the third party EDI network provider.

6.5.3 Network provider contracts

> "The Company gives no warranty or representation as to the fitness of the service nor the software for any purpose nor as to performance, or quality of either of them."[324]

The above clause is representative of the current trend in such value-added communications services, and is based on the fact that the basic network providers (eg. the national PTTs) have historically had the statutory right to do likewise[325]. It is also justified on the grounds that the value of the transaction message is outside both the knowledge and control of the network provider, who therefore has little ability to assess his potential liability and make adequate provision for it through insurance. The data user should be able to assess the potential damages that could arise and has the responsibility and ability to mitigate against such losses through the implementation of appropriate control procedures.

All of the agreements reviewed stated that the network provider would be liable for direct damages, although the maximum amount available is usually specified. The only company not even willing to offer compensation for direct damage is Ordernet (US), who state at clause 7(d):

---

323 New Zealand Customs, op.cit. supra n.124, at 10(c); see also Thomsen, H.B., "Interchange Agreements", p.87, para. 6.9.13, in Walden, op.cit. supra n.146.

324 Istel, op.cit. supra n.235, at 6.2.

325 Some public telecommunication operators are exempted from all liability by law, eg. Belgium, Greece, Denmark; others are limited to refund "the price paid for the failed circuits provided the circuit is out of order for more than 60 minutes" [CCITT recommendation]. In Italy, the Constitutional Court decided that total exemption of liability was unconstitutional [March 17, 1988, decision 303/December 20, 1988, decision 1104]. See generally Petre, Blanche, "Network Providers", p.11, Computer Law and Practice, Vol.7, No.1, Sept-Oct. 1990 and `The Liability of Electronic Data Interchange Network Operators', pp.69-82, Tedis final report, July 1991.

"..Ordernet Services shall not be responsible for any direct, indirect or special or consequential damages (including but not limited to loss of profits or loss of business) suffered by customer as a result of any default by Ordernet Services.."[326]

However, under US law, complete exclusion of liability in service contracts, such as not accepting liability for a refusal to provide the service and accepting no obligations of reasonable effort to perform the service, would not be recognised by the courts as a mutually binding contract.[327]

Under English law, the ability of network providers to exclude liability by contract is governed under the Supply of Goods and Services Act 1982[328], which imposes an implied contractual term upon the network providers to act with reasonable care and skill, and the Unfair Contract Terms Act 1977[329].

With regard to the technical components of the system, the choice of hardware and software used, where the network provider has used standard market products, it is unlikely that he will be guilty of lack of care[330]. It is more likely to apply, however, where the components were designed by the network provider. In certain contracts, the network provider warrants that such equipment will function correctly for a period of time[331]. Care is also required in the operation of the system; lack of care possibly being evidenced by a failure to comply with the express contract. Some of the UK and US agreements give explicit contractual recognition to a duty of care[332].

It should be recognised, however, that the level of responsibility a network provider is prepared to carry could be a matter for negotiation between the parties, based on the data user being prepared to adopt special security procedures and pay the cost of such measures.

---

326 In addition, TranSettlements (US) would seem to exclude direct damages by stating at 5: "In the event of failure of malfunction of the system, TranSettlements' total responsibility will be to use its best efforts to correct any such failure or malfunction."

327 *Sterling Computer Systems of Texas., Inc. v Texas Pipe Bending Co.*, 507 SW 2d 282 (Tex.Civ.App. 1974). See also Nimmer, op.cit. supra n.268; and Wright, B., The Law of Electronic Commerce - EDI, *Fax and E-mail: Technology, Proof and Liability*, Little, Brown and Company, Boston, 1991.

328 S.13 states that "In a contract for the supply of a service where the supplier is acting in the course of business, there is an implied term that the supplier will carry out the service with reasonable skill and care". This is also the position in the US, 17A C.J.S. Contracts § 329 (1963) and *NTA National Inc. v DNC Services Corp.*, 511 F.Supp.210 [DCC 1981].

329 Exclusion of liability under ss. 2 and 3, is only effective if it satisfies the test of `reasonableness' in s.11, where regard should be had to (a) the resources of the party relying on the term to meet the potential liability and (b) how able he is to gain insurance protection (s.11(4)). Statutory requirements, such as those contained within the Value-Added and Data Service (VADS) licence, cannot be excluded in contract.

330 Reed, C., "Contractual and Liability Issues", Proceedings of the EDI and the Law Conference, London, 3-4 October 1989.

331 Eg. MercuryLink, at 13.1: "Mercury warrants that the Equipment is free from defects in design, manufacture or materials except where caused by fair wear or tear and that the Software is capable of fulfilling all material requirements of the functions and specifications set out in Mercury's Service Literature...". This warranty is limited to the first 12 months following delivery (13.2).

332 Eg. AT&T, op.cit. supra n.248, at 5(a): "AT&T will use reasonable care to prevent loss, alteration or disclosure of information or data in your files".

In the US, the First National Bank of Chicago agreed to take additional liability when carrying electronic trade payments for General Motors, if the car manufacturer cryptographically authenticated and encrypted its payment messages[333].

The data user should also distinguish and demand guarantees on service features, such as support of a specific messaging protocol or particular security features, which are seen as being vital to the data user's commercial operations; for example:

> "The Company warrants that subject to the express terms of this Contract 98% of such data will be processed within 15 minutes of receipt at the Company's computer centre...and 100% within 90 minutes"[334]

Such warranties enable the data user to sue for damages in the event that such standards are not met. In this respect, it is important for the parties to distinguish between standards of performance for the physical system and the service itself. One French network provider has recently announced the introduction of an `expert system' into their service provision, which would enable the user to pre-define the level of service that they require from the network and to self-monitor compliance with such criteria[335].

With regard to defects in the performance of the service, one network provider states that if it is unable to correct a particular defect to the service then it reserves the right to terminate the service with no liability[336]. Presumably, the network provider could argue that this covers all events that cause damage, such as misdirecting a message, since this could be classified as a `defect' of the service. The termination aspect of such a clause could obviously have a serious impact on a data user's commercial operations, increasing the level of losses; it should therefore be strenuously objected to.

Other network providers' accept an obligation to correct any errors in the service:

---

333 Wright 1989, op.cit. supra n.106, at p.50.

334 Istel, op.cit. supra n.235, at 2.4. BT-Tymnet state that messages are normally delivered in 2-3 minutes and guaranteed in 2 hours. AT& T, op.cit. supra n.248, at 6.A "warrants that the Messaging Service(s) will perform as described in the Documentation". Alternatively, INS, op.cit. supra n.244, at 11(d) states: "Since INS has no knowledge or conrol over the types or volumes of Transmissions which the User...will submit to the TRADANET Service....INS does not guarantee any specific time for delivery...".

335 Brunet, Christophe, "Artificial Intelligence in EDI", pp.93-101, Proceedings of '91 International Conference on EDI, Korea, 7-8 November, 1991. See generally, van Dijk, J.C., and Paul Williams, *Expert Systems in Auditing*, Macmillan 1990. See also Chapter 2, at 2.3.3.

336 Eg. Geisco EDI*Express System Supplement to MNA, op.cit. supra n.238, at 9: "If Company cannot correct the non conformity or defect within a reasonable time, Company may terminate this agreement. Company shall thereupon have no obligation or liability to Customer...".

"Supplier will, at its expense, correct any data processing errors which are due solely either to malfunction of Supplier controlled machines, Supplier operators, Supplier programmers, or Supplier programs.."[337]

The network provider will usually provide one of two alternative remedy provisions in the case of the service failing to perform to its contractual obligations, and direct damages arising:

- a `limitation of action' clause: "..liability will be limited to Customer's actual damage in an amount not to exceed one month's average charge.."[338]; or

- an `exclusive remedy' clause: "If the Company does not fulfil its obligations with respect to providing system up-time, Customer's exclusive remedy is...."[339].

In both cases, it is important to consider if the amount is reasonable and adequate to cover the potential direct damages. Limitation of liability clauses may also limit the time period within which a legal action must be taken. The data user needs to consider the suitability of the period, depending on the nature of the service concerned; for example, a one year time limit should be sufficient to discover message accuracy, but damage caused by deficient consultancy services may take longer to appear. Alternatively, the agreement may impose upon the data user a duty of notification, where the network provider is thought to have committed an actionable offence[340].

The network provider agreements all include indemnification clause(s), but the exact scope varies considerably. As mentioned in section 6.4.1 above, such clauses are usually included to cover intellectual property rights. The general indemnification clause protects both parties from the "acts or omissions" of the other, depending on their degree of negligence. The US agreements tend to protect only the network provider[341].

In the case of most network providers, both in the US and UK, in addition to the agreement with the data user, the service provider will have a licence and/or contract with the basic telecommunication provider (eg. the national PTTs). The data user should therefore ensure

---

337 BT Tymnet EDI Agreement (US) at F. See also Ordernet Services Inc. (US), at 7(a).

338 Control Data, op.cit. supra n.238, at 8(d). Harbinger (US) has no amount limit for direct damages.

339 Geisco (US), op.cit. supra n.238, at 3.

340 Eg. CompuServe, op.cit. supra n.277, at 6(c): whereCompuServe have acted incorrectly etc. "..Customer shall (i) promptly notify CompuServe of such facts by telephone and shall (ii) further notify CompuServe in writing within ten days of such discovery. The failure to give the foregoing notices shall constitute an irrevocable waiver of all claims...".

341 See O' Brien, op.cit. supra n.188, at p.6. The Ordernet, op.cit. supra n.336, at 7(c), includes such a wide indemnification clause that it would require the user to pay consequential damages!

that a indemnity provision exists to cover situations where a dispute arises between these parties, which results in the loss of the service to the data user[342].

As noted in 6.4.1, internetworking between the network providers can give rise to complex questions of liability which users need to address. Since the user is extremely unlikely to have a direct contractual arrangement with the remote network, he will have to ensure that the network provider with whom he directly communicates has made the appropriate contractual arrangements. In the longer term, as noted by Wright[343], legislation could be enacted which would "set forth the duties of networks in a chain of communication".

In the US, the Federal Communications Commissions is currently examining whether carrier liability rules should be enacted, particularly with respect to network toll fraud[344]. Complaints have recently been filed with the Commission, by various users, concerning the fact that network providers exclude all such liability and yet fail to implement adequate security controls[345].

With regard to satellite communications, the INTELSAT and EUTELSAT Operating Agreements, for use of their satellite services, exclude liability for "loss or damage which may be sustained by reason of unavailability, delay or faultiness of telecommunication services provided or to be provided by them"[346].

In the area of Electronic Funds Transfers (EFT), communication networks between financial institutions are primarily closed user groups, and therefore the allocation of risk is divided more equitably. The agreement governing the SWIFT network[347], for example, states that SWIFT is responsible for any events that occur in the part of the system controlled by SWIFT, while the users are responsible for events that occur in the part of the system under their control:

---

342 Eg. INS, op.cit. supra n.244, at 11(c): "INS shall have no liability for any loss or damage...as a result of the non-availability or failure of the telecommunications line of any duly authorised public telecommunications operator, except where...caused by an act or omission on the part of INS". IBM, op.cit. supra n.237, at Art.22.

343 op.cit. supra n.106, at p.53. A similar such concept already exists in the UCC, § 7-302, for certain connecting transportation carriers.

344 "Network toll fraud involves hackers who dial into a private branch exchange and use a stolen authorisation code to dial out to any destination in the world or who trick voice mail systems into giving them an outgoing line.", p3, Taff, A., "Toll fraud victims tell FCC carriers are unresponsive", Network World, 6 May, 1991. See also Cook, W., "Trends in Network Liability: 1992", pp.213-216, The Computer Law and Security Report, Vol.8, No.5, Sept./Oct. 1992.

345 Ibid.

346 quoted at p.10023, in Saxby, S. (General Editor) *The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990. See also Chapter 3, at 3.3.1.

347 The Society for Worldwide Interbank Financial Telecommunications, incorporated under Belgian law. For further details, see Beker, Professor H.J., and I. Walden, "Electronic Fund Transfer", p.5022-5025, in *Encyclopedia*, ibid.

"SWIFT assumes liability after the message reaches a regional processor, while the sender is liable for line failures between their premises and the regional processor"[348].

The growth of EFT communications between banks and trading corporations, has led to the drafting of legal instruments in certain forums, in order to ensure a fair allocation of the risks. In the US, in 1989, the National Conference of Commissioners on Uniform States Law and the American Law Institute drafted an additional article to the Uniform Commercial Code (UCC) covering `wholesale' credit transfers, which has already been adopted by a number of States[349]. With regard to the liability of the bank for sending the message, it states:

"if a payment order addressed to a receiving bank is transmitted to a funds transfer system or other third party communication system for transmittal to the bank, the system is deemed to be an agent of the sender for the purpose of transmitting the payment order to the bank."[350]

The draft law also states that, where a security procedure is adopted by the parties to detect and/or prevent errors from occurring, in the event that an error arises because such security procedures are not followed, then the loss will be borne by the party that has failed to comply with the procedures.[351]

The United Nations Commission on International Trade Law (UNCITRAL) is currently working on a `Draft Model Law on International Credit Transfers'[352]. The current document differs from the UCC 4a, in that the banks are seen to be liable unless one of the permitted exempting conditions exist.

In international trade, the vast majority of traders make use of documentary credits as the mechanism by which a seller can ensure payment from the buyer. Under the current ICC Uniform Customs and Practice for Documentary Credits[353], the following provision covers bank liability:

---

348 See Appendix B3. See also Petre, op.cit. supra n.324, at p.12, fn.18.

349 Ibid., at p.13, fn.21.

350 Article 4a-206.

351 Prefatory note.

352 UNCITRAL model law, op.cit. supra n.19.

353 5th Edition, 1983, Doc. No.400.

"banks are not liable or responsible for the consequences of any delay and/or loss in transit of any messages, letters or documents or for delay, mutilation or errors arising in the transmission of any telecommunications."[354]

To date, in the absence of legislation, financial institutions have generally been able to exclude liability for most errors that arise in EFT systems[355].

Finally, with regard to general network provider liability issues, data users need to be careful that the wording of a force majeure clause is not too vague, ie. what is `beyond the reasonable control' of a network provider? In Finland, a credit card user was unable to complete a purchase, "due to a non identified disturbance in the data traffic". The credit card company claimed that it was not responsible for such `force majeure' disturbances. The court held that suitable alternative means of communication existed, ie. the telephone, and therefore the company did have to compensate for the card holder's loss[356]. Does the force majeure clause include an obligation on the network provider and data user to take steps to mitigate such occurrences, ie. implement a disaster recovery plan?

6.5.4 Tortious liability

Under common law, liability can arise because one party has been negligent in fulfilling its responsibilities: tortious liability. It often applies in conjunction with other liabilities, arising through statute or contract. Negligent liability, in common law jurisdictions, requires three essential elements:

- the defendant must owe the plaintiff `a duty of care'. Therefore, it must be shown that there exists a sufficiently close relationship between the two parties, ie. it must be reasonably foreseeable that the defendant's negligence could injure the plaintiff[357];

- a breach of the duty to care must have taken place, ie. the defendant must have failed to take `appropriate' and/or `adequate' precautions;

---

354 Ibid., at Article 18.

355 See further Beker, op.cit. supra n.346 and Reed, op.cit. supra n.18.

356 Register of the Supreme Court of Finland, Finlex, 9 October, 1989.

357 See *Caparo Industries plc v Dickman & Others*, 1990, 1 All ER 568 (and subsequently *Al-Nakib Investments Ltd v Longcroft* [1990] 3 All ER 321 and *James McNaughton Paper Group Ltd. v Hicks Anderson & Co.*, Times Law Report, October 2, 1990) where the UK courts seem to conclude that the duty of care for an information provider may be more restricted than that of manufacturers.

- the plaintiff must have suffered some damage as a result of the breach, ie. the type of damage suffered must have arisen directly from the breach, and it must have been reasonably foreseeable from the nature of the breach[358].

In terms of ensuring that a company's data communications activities operate within a `legally secure' environment, the second element is of critical importance: what are considered to be appropriate safeguards? This is viewed by the courts as essentially a question of fact that can be objectively arrived at; however, existing US case law does provide us with some idea of how the courts could decide a case involving data communications security.

In the US, the *T.J. Hooper Case*[359] was concerned with the use of radios in ships. The tug boat in question had lost its cargo-carrying barge in a bad storm, and the plaintiff (cargo owners) claimed that the loss could have been avoided if the defendant (ship owner) had used a radio to listen to the weather conditions and therefore take the necessary avoiding action.

The use of radios was not a mandatory requirement or an industry standard, indeed the vast majority of ship owners did not install such equipment. In spite of this, the court found in favour of the plaintiffs, stating that the fact that other ship owners did not use radios was irrelevant, since "a whole calling may have duly lagged in the adoption of new and available devices"[360]. One of the critical elements behind this decision was the fact that the relevant technology was cheap to install. In terms of network security, therefore, it would seem essential that security procedures and techniques are kept up-to-date, in terms of the currently available products, not necessarily based on use within the industry. The cost of implementation should also be considered, not simply on their own terms, but in relation to the nature of the data being protected, ie. the value of the information to all those concerned.

In other cases, under English jurisdiction, the courts have stated that it is not only necessary to have safety equipment, but that it is also used properly[361]. This places a responsibility upon the employers to ensure that their employees get adequate training in the use and application of any security procedures and techniques. There would also seem to be a legal

---

358 See generally, `The Liability of EDI Network Operators' report, op.cit. supra n.151, pp.52-57, for a review of tortious liability principles in France, Belgium, Germany and the Netherlands.

359 60 F.2d 737 (1932).

360 quoted in Baum, M., "Analysis of Legal Aspects", p.131, in Walden, op.cit. supra n.146.

361 *The Lady Gwendolen* [1965] P 294 C.A.

obligation[362] to keep the technology up to date, which is likely to be especially important in terms of upgrading computer hardware and using updated software.

One additional form of security regulation not given extensive coverage in this section, but of particular relevance to the issue of tortious liability, is that contained within sectoral or industry codes of practice[363]. These may be voluntary within a particular sector, or part of the conditions associated with membership of a particularly association. However, in either case, in the event of a dispute, a court may take account any codes of practice the defending organisation is ascribed to, when deciding their negligence in an action based on their failure to protect certain data from loss, alteration or manipulation etc. A failure to maintain the security standards stated in a particular code, to which the organisation had publicly associated itself with, would seem to be evidence that they had been acting negligently[364].

6.5.5 Comment

In the discussion on interchange agreements, it was noted that there is a tendency not to make substantial liability arrangements, since, in the vast majority of circumstances, any liability is likely to arise with respect to the underlying commercial contract, rather through the use of a particular mode of communication. This has historically been the same for the paper environment.

Recognition of this fact should similarly be borne in mind when considering the liability that the network providers should bear. Electronic communications can offer a much higher level of security than that provided by paper-based methods, such as the post, and therefore the network providers contract should be viewed in this light[365]. Wright argues that network providers should be responsible for a degree of consequential loss on two grounds:

> "First, the network is often in the best position to prevent errors because it controls and processes the data. Second, exposure to liability gives the network incentive to improve the quality of its service and controls"[366]

This argument was echoed at a conference on the vulnerability of financial information to computer crime, when it was noted that:

---

362 *Grand Champion Tankers v Norpipe A/S (The Marion)* [1984] A.C.563.

363 Eg. the UNCID Rules, op.cit. supra n.7; see also Chapter 5, at 5.4.2.

364 See Thomsen, op.cit. supra n.213, at p.173.

365 The Geisco EDI service has been operating for 5 years, with currently around 8000 worldwide customers, and yet it claims not to have received a single liability claim for loss of messages etc; quoted by Hunter, op.cit. supra n.275.

366 Wright 1989, op.cit. supra n.106, at p.50.

"As such bodies [ie. telecommunications service providers] offer a greater range of services and move away from being mere conduits for communications, the arguments for removing or reducing their immunity from civil liability increases in a system of law designed to spread and share the risk of the inescapable factor of loss involved in transnational offences..."[367]

With regard to the second point, in the absence of legislative provision supporting this proposition[368], the network providers are unlikely to adopt such a position, unless it was perceived as an effective element within a marketing strategy. However, companies might find an alternative course of action in the area of tortious liability.

Finally, over recent years, the appearance and dramatic use of various data corruption techniques, such as viruses and worms, has meant that users of communication networks have become increasingly concerned that such corruption techniques could be introduced into their corporate systems, via the external network. As a consequence of this fear, users could, as has occurred in the software industry, request the inclusion of an additional provision within the relevant communication contracts stating that, if it can be shown that a data corruption component was introduced through inadequate security procedures by a communicating partner, then that party shall be liable for an element of consequential loss[369].

---

367 "Forum on the international legal vulnerability of financial information", Summary Record & Statement, Toronto, Canada, 28 February 1990; at p.9.

368 The European Commission has recently put forward a "Draft proposal for a Council Directive on the liability of suppliers of services" of 7 August 1990 (SPC/149/90). In its current form, this directive would mean that the supplier of a service would have to prove that a `fault' was not committed by him: "Assessment of the fault is based on the security which may reasonably be expected." - see `The Liability of EDI Network Operators' report, op.cit. supra n.151, at p.104-105.

369 See Ford, D., "Virus Clauses", p.4-5, Applied Computer and Communications Law, Vol.7, No.6, June 1990.

Chapter 7 **CONCLUSION**

7.1 Introduction

This thesis has focused on one particular aspect of the information revolution, telematics: the integration of computer and telecommunication technologies. The potential benefits that telematics offer are obviously considerable in all aspects of society; however, we have been concerned with the increasing use of data communications between trading parties within the commercial sector.

The use of data communications would seem to be increasing rapidly among the business community[1]. However, obstacles, both real and perceived, can threaten to hold back the full and effective exploitation of telematics. This thesis has considered the extent to which the law can be both an obstacle and facilitator in the use of such technqiues.

The law is designed to provide rules within which our actions can be limited. The law should change as the society it serves develops. With regard to data communications, we have given detailed consideration to three specific legal aspects:

- legislation that restricts the use of data communications, to safeguard the rights of the third-party subject of the communication;

- legal rules that need to be amended, in order to recognise the developing role of data communications within commerce,

- and the form of contractual provisions that could be adopted, to enable companies to securely embrace the data communication revolution.

In Chapter 2, the nature of modern developments in data communications and the ability of trading partners to communicate electronically, nationally and internationally, was described. Data security is the critical requirement for the successful exploitation of such

---

[1] See generally Chapter 2.

communication networks: ensuring that messages arrive at their intended destination in an uncorrupted manner. The need for adequate technical security procedures is increasingly being acknowledged by companies, as they recognise their dependence on IT systems for a wide range of business-critical functions.

The current state of technology enables a business to implement an extremely secure communications environment. The degree to which such techniques are implemented obviously needs to be a function of the risks involved if something goes wrong; an assessment of costs[2] against potential benefits needs to be made.

The legitimate concerns of data users regarding the security of such systems need to be satisfied. However, distinguishing and identifying real security concerns is the first procedure towards establishing legal security: As Martino has stated:

> "...each time a new system or tool is produced, our more or less conscious attachment to tradition leads us to expect guarantees which were previously not only never fulfilled but were not even asked for"[3]

The use of electronic messaging techniques can be held back because management makes demands upon the technology, to satisfy an array of integrity criteria, that can often not be met because of weaknesses in their non-electronic corporate information flows[4].

7.2 Statutory Law

The range of law that can be seen to impact on data communications is considerable, and Chapter 3 reviewed that seen as most directly relevant.

The telecommunications regulatory framework should be primarily concerned with ensuring the effective provision of communication networks. Such legislation usually imposes minimum technical standards which have to be complied with in order to safeguard the integrity of the network as a whole. In addition, telecommunications legislation should implement policies designed to encourage the provision of an array of different types of communication service.

---

[2] Eg. effective security measures can consume 15% of processing power; stated in Greguras, Fred M, and Richard Sizer., "Impact of transborder data flow restrictions on cash-management services", p.20, Information Age, Vol.9, No.1, January 1 1987.

[3] Martino, A.A., "Paperless Trade: Legal and Techincal Standardization Problems", paper presented at COMPAT 88, Hague, Holland, 29 Feb.- 2 Mar. 1988.

[4] See generally, Waldron, M., "Applying a standard approach to document management", In-Form Systems Ltd, 1992.

The process of telecommunications liberalisation within Europe has removed many of the restrictions on the use of data communications noted by commentators in the late 1970s-early 1980s, such as discriminatory pricing. Such restrictions were primarily concerned with the transmission of data, rather than the content; and were designed to safeguard the income of the national telecommunication authorities from competition. Liberalisation, although progressing at different rates within Europe, has seen the emergence of a number of new communication services, such as mobile data networks, provided by companies from around the world. The continuing liberalisation process should mean that telecommunications legislation will be increasingly less relevant to a data communications user.

Over recent years, legislators have recognised the need to reform criminal law to take account of computer misuse. Such legislative initiatives would seem to be a necessary deterrent against those wishing to interfere with information technology. However, the disadvantage of using criminal law, as a means of legislative protection, is the need to depend on an action being pursued by the public authorities. In the current economic climate, the level of resources and expertise that the police and prosecuting authorities can devote to computer-specific issues can be expected to continue to be insufficient.

With regard to data security legislation, if companies continue to devote inadequate resources to the need for security procedures[5], despite telematic systems become more business-critical, then there will be increasing legislative pressure to pass regulations that imposes requirements upon data users to take adequate measures. The recent moves towards international harmonised security standards is likely to bolster such pressures.

Other legislative restrictions against international data communications have arisen for various political/economic reasons. The US dominance in the field of IT, and the complete dominance of the industrialised nations over the Less Developed Countries, has raised demands to prevent such imbalance through national legislative action. Such initiatives need to be seen against this economic background. Indeed, such demands would seem to rise and fall according to a matrix of social, political and economic factors. To that extent, such restrictions will continue to appear on national political agendas from time-to-time. The successful conclusion of the current GATT process, with its expansion to cover trade-in-services, could mitigate against such future actions.

Overall, with respect to fears over the control of international data flows, it should also be borne in mind the statement that:

---

[5] A recent data security survey found that 39% of respondents believed that their current procedures were insufficient; see Warman, Dr A., "Organisational Computer Security Policies", L.S.E, London, 1991.

"the right to the free flow of information or freedom of information tends to be guaranteed by technology, and not by law."[6]

The inherent difficulties in controlling data communications technology could also be expected to be act as a significant deterent to legislators.

Data protection legislation arose from fears that telematics technology posed new threats to a data subject's privacy. It is considered in Chapter 4 on three grounds:

- As an example of `sui generis' legislation, aimed at controlling and limiting the use of data communications;

- as legislation which directly addresses the need for adequate data security measures to be adopted, to the benefit of both user and subject;

- as an example of the need for international harmonisation of legislation when attempting to regulate an international technology.

With regard to restrictions on transborder data flows, both the respondents to Survey A, and the literature, indicate that the fears expressed by users have not significantly materialised.

In terms of data security, respondents had not generally found the legislative provisions restrictive. Indeed in certain cases, the legislative provisions had had the opposite impact, being used by data security managers as a lever to obtain additional resources to devote to data security.

In the first part of Chapter 5, consideration was given to the extensive range of potential restrictions over the use of data communications technology that exist in commercial law. The restrictions arise because of the lag between developing technology and the ability of the law to change to reflect such developments. Certain provisions within commercial law, often established many years ago, do not allow for the replacement of paper with electronic data.

In the long term, the successful and effective spread of electronic messaging will depend on governments reviewing the commercial legal framework to remove such unintended obstacles.

---

6 Ennison Jr., Thomas, "Sovereignty Considerations in TDF - developing country perspective", p.181, Transnational Data and Communications Report, Vol.VII, No.3, 1984.

One concern for organisations, becoming increasingly reliant on the use of information technology for business communication, is the lack of a permanent record of events. Electronic records are 'fleeting' compared to paper, and are therefore seen as unreliable source of information. In the event of a dispute, however, the ability of the data user to present a reliable record of events will be of critical commercial importance.

Record-keeping requirements are usually contained within regulations and, therefore, governments are able to amend such regulations comparatively easily. An additional issue concerns whether the various statutory bodies, that demand the records, are able to accept and adequately administer the electronic alternatives. Some authorities, such as Customs and Excise, already recognise the part that electronic records can play in simplifying their administrative tasks, thereby releasing personnel to carry out the investigative and control aspects of their duties[7].

In order for statutory authorities to agree to accept the submission of electronic records, the data user usually has to satisfy the authority that their communication system functions reliably; an objective that should match the needs of the business itself. As dependence on electronic messaging emerges within governmental authorities, it is likely that there will be pressure upon government to issue standards for record-keeping. This has already been seen in other countries, such as Canada[8]. Such standards are likely to penetrate into the private sector as the de facto minimum standard.

Finally, as discussed in Chapter 5, with respect to certain legal documents such as bills of lading, the use of data communications can enable the restoration of traditional securities and functions that certain legal instruments originally had, but had lost over the years as practical difficulties created by the use of paper meant that companies found practical means around the formalities.

7.3 Contract Law

Discussion has already considered the role of legislation in controlling data communications. However, one main theme of this thesis, is how contractual agreements can also play a critical part in establishing a self-regulatory, secure framework. Indeed, as illustrated by the transborder data flow provisions within data protection legislation, legislation can give rise to

[7] Morrin, J.P., "Customs requirements and international trade", Computer Law and Practice, Vol.6, No.2, pp.42-45, Nov.-Dec., 1989.

[8] See Chapter 5, at 5.3.1.

the need for contractual provision to supplement and enhance the intentions contained within the statute

The use of contractual means to maintain information security has a number of advantages over legislative protection. Through the use of a contract, the obligations owed by each party to the contract are specified; how the parties intend to apportion risk, and therefore any potential liabilities. As part of this process, the parties can determine the level of security they expect of each other and the system as a whole. A contract can therefore provide certainty for the parties and will reduce the chance of a dispute arising at some later stage.

The use of contracts within an international data protection context has only recently received significant interest within international organisations, such as the Council of Europe, and indeed within the business community. Although, a number of the survey respondents had incorporated data protection-related provisions within particular types of contracts, such as the employment and supplier agreements; none of the multinational had used contractual provisions for international data transfers to countries that lack appropriate legislation.

Since the first data act was passed in 1973, the European data protection authorities have made use of contractual terms as a means of extending protection outside of their national jurisdiction. However, it is only recently that concerted consideration has been given to the use of some standardised contractual form. Interest in this aspect would seem to have been generated by the European Commission's draft Directive. The re-newed move towards harmonised protection between the Member States has focused attention on the need to find a means by which companies can continue to communicate with other trading nations, such as the US, who continue to lack general legislation.

The degree to which such contractual provisions will be widely adopted, will depend on the degree to which they can be shown to offer real and effective protection; and the attitudes of the data protection authorities.

Interchange agreements are a completely novel form of contract, between trading partners, dealing with issues arising solely from the mode of communication. Although currently most data users operate without such agreements, at both a national and international level, there seems to significant support for the need to have some communication-specific contractual provisions.

There is, however, another aspect of interchange agreements that would appear unusual. Traditional contracts are usually either `freely' negotiated between the parties or based upon

`battle of forms' arrangements, not laid down by statute[9] Therefore, the final agreement is usually a reflection of the relative bargaining strengths of the parties. Existing interchange agreements, however, tend to reflect `legal security' concerns that are shared between the parties[10]. This fact would seem to suggest that in the medium-long term, as electronic trading becomes the norm, the need and popularity of such agreements will experience a decline. Eventually, as with paper, such communication agreements will cease to be necessary.

In the short term, however, companies can make legal provision for the use of data communications via one of three major methods:

- A separate interchange agreement;
- attach additional provisions or make amendments to their standard trading terms and conditions; or
- agree to abide by some form of code of conduct, either international or sectoral.

One of the major current trends in electronic trading is the use of a third-party network service provider. While a computer bureau offers external data processing; and a facilities management company manages and operates a computer installation; a network service provider provides an external communication capability[11].

The critical aspect when signing-up to any of these IT service providers, is the need to ensure that the contractual arrangements adequately reflect the security concerns of the user. Currently, however, users tend to establish contractual relations based upon a standard contractual form based firmly from the perspective, and in the interest, of the service provider.

Finally, however, it should also be borne in mind, that contracts can not provide for complete legal security, in the absence of legislation. The potential uncertainty of court judgements, and the problem of third party actions, mitigates against complete contractual reliance.

---

[9] Although certain statutory terms are implied into contracts, eg. The Sale of Goods Act 1974, ss.12-14.

[10] See Chapter 6, at 6.3.5.

[11] Obviously, the same company might offer the complete range of services.

7.4 Legal Security

> "It is interesting to note that many of the people responsible for developing and maintaining...security programs are using the rationale: `It's the law'. The rationale has been not that it is good management practice, not that security and integrity should be an integral part of our information systems - but that `It's the law'."[12]

The above quote was stated in connection with the US Computer Security Act 1987, however, it also has significant relevance to this thesis.

This thesis has considered two forms of law: that passed by national and supranational governmental bodies, which has either directly or indirectly impacted on a company's information security policy; the second form of law exists in a form which is primarily created according to the parties involved, although founded within a legal framework established over hundreds of years of commercial activity: contract law. Both have advantages and disadvantages over each other, but together can serve to provide companies with a high degree of legal security. The quote is obviously referring to statute law, but companies need to constantly be aware of what can be achieved through the use of contracts.

One purpose of this thesis has been to place the need for adequate information security in its proper context: a critical business requirement. Companies should not see information security law as a bare minimum, or an annoying requirement. Statute law should be used by information security managers as one of a set of issues to encourage action at board level in the area of security.

However, in response to the quote, it can be seen throughout the first part of the chapter, that statute law only provides vague guidelines for companies upon which to base a security policy. Therefore, implementing information security because `it's the law' will give little practical help in safeguarding the interests of the company!

Data communications managers have to ensure that data security issues are given an adequate profile in the negotiation of contracts. However, to incorporate information security clauses within company contracts requires a clear understanding of the practical implications. If this is not achieved, companies could agree to contractual clauses which are either ineffective as legal protection, or impose requirements that the company is incapable of matching.

---

[12] Tompkins.

The evidence for suggesting that security issues, both technical and legal, deter companies from exploiting data communication techniques would seem insufficiently clear. Certainly, within the European Community, a number of `legal security'-related initiatives are being pursued, on the presumption that such issues do act as potential barriers to the development of the information services market.

Overall, the purpose of this thesis has been to analyse the legal restrictions and insecurities that exist in the current commercial-legal framework, as well as the sources of legal protection, to ensure that the law does not prove an obstacle, rather than a facilitator, in the use of data communications.

Ian Newark Walden
June 1992

BIBLIOGRAPHY

CASE LAW

English:

Routledge v Grant (1828) 4 Bing 653
Taylor v Caldwell (1863) 3 B&S. 286 Queen's Bench; S&T. 406.
Raffles v Wichelhaus 1864 2 H&C 906.
Household Fire Insurance v Grant (1870) 4 Ex.D. 216.
Re Flavell (1883) 25 Ch D 89, CA.
Re London and Globe Finance Corpn Ltd [1903] 1 Ch 728.
R v Daye (1908) 77 LJKB 659
Lloyd v Grace Smith & Co. 1912 AC 716.
Dunlop Pneumatic Tyre Co. Ltdv Selfridge & Co. Ltd [1915] A.C. 847.
L'Estrange v F. Graucob 1934 2KB 394.
Hartog v Colin & Shields 1939 3 All ER 566.
Waterson's Trustees v. St. Giles Boys Club [1943] S.C. 369.
Shanklin Pier Ltd v Detel Products Ltd [1951] 2 KB 854, [1951]2 All ER 471
Goodman v J.Eban [1954] 1 Q.B. 550.
Entores Ltd v Miles Far East Corporation 2QB 327 (1955).
Davis Contractors Ltd v Fareham UDC (1956) AC 696; 2 All ER 633, CA.
Ladbroke (Football) Ltd v William Hill (Football) Ltd [1964] 1 All E.R. 465, H.L.
Hedley Byrne & Co. Ltd. v Heller & Partners Ltd. [1964] A.C. 465, H.L.
The Lady Gwendolen [1965] P 294 C.A.
The Statute of Liberty [1968] 2 All ER 195.
Beswick v Beswick [1968] A.C. 58.
R v Senat (1968) 52 Cr. App. Rep. 282.
R v Thompson 1978 E.Comm.Ct.J.Rep. 2247.
Oxford v Moss, [1979] 68 Cr App. R 183.
R v Pettigrew [1980] 71 Cr.App.R.39.
Barker v Wilson [1980] 1 WLR 884
Gates v Swift [1981] F.S.R. 57 & [1982] R.P.C. 339
R v Wood [1982] 76 Cr. App.Rep. 23.
Brinkibon Ltd v Stahag Stahl und Stahlwarenhanelsgesellschaft (1982) 2 WLR 264.
Kajala v Noble [1982] 75 Cr.App.R.149.
R v Absolom, Times, 14 Sept.1983.
Grand Champion Tankers v Norpipe A/S (The Marion) [1984] A.C.563
Castle v Cross [1984] Crim.L.R. 682
R v Thompson [1984] 3 All ER 565.
Express Newspapers Plc v Liverpool Daily Post and Echo [1985] F.S.R. 306 at 309, Ch.
Cox v Riley, 83 Cr. App. R. 54, Q.B.D. (1986).
R v Gold, [1987] 3 WLR 803 & [1988] AC 1063.
Clipper Maritime v Shirlstar Container Transport [1987] I Lloyds Rep.546, 554.
Faccenda Chicken Ltd v Fowler (1987) Ch.117.
Huddleston and another v Control Risks Information Services Ltd. [1987] 2 All ER 1035.
The Attorney-General v Guardian Newspapers Limited & Others [1987] 1 W.L.R. pp.1248.
R v McMahon, Isleworth Crown Court 1987.
Sophocleous v Ringer [1988] R.T.R. 52
MS Associates Limited v Power [1988] FSR 242.
R v Harper; R v Minors [1989] 2 All ER 208
Kleinwort Benson Ltd v Malaysia Mining Co. [1989] 1 WLR 379, CA.
Caparo Industries plc v Dickman & Others, 1990, 1 All ER 568.
Computer Aided Systems (UK) Ltd v Bolwell, IPD, 15, April 1990.
The Delfini, [1990] 1 Lloyd's Rep 252.
R v Spiby, [1990] The Times, 16 March
R v Governor of Pentonville Prison, ex parte Osman [1990] 1 WLR 277.
Derby & Co Ltd and others v Weldon and others (No.9) [1991] 2 All ER 901.
Lansing Linde Ltd v Kerr (1991) IRLR 80.
Camden LBC v Hobson, Times 28 January 1992.
Alliance & Leicester Building Society v Ghahremani & Others (ChD NLJ 6 March p.313; The Independent 9 March).

United States:

The T.J. Hooper 60 F.2d 737 (1932).
Coco v Clark [1969] R.P.C. 41.
Sterling Computer Systems of Texas., Inc. v Texas Pipe Bending Co., 507 SW 2d 282 (Tex.Civ.App. 1974).

Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976)
Perma Research and Development v Singer Co., 452, F.2d 111 [1976]
Amoco Production Co. v Lindley, 609 P.2d 733 at 745 (S.Ct.Okla.,1980).
NTA National Inc. v DNC Services Corp., 511 F.Supp.210 [DCC 1981].
Evra Corp. v Swiss Bank Corp., 522 F.Supp.820 (N.D.Ill.1981) aff'd in part, rev'd in part and vacated in part, 673 F.2d 951 (7th Cir.) cert. denied, 459 U.S. 1017 (1982).
Business Intelligence Services Inc v Hudson (580 F Supp 1068 (SDNY 1984)).
Dun & Bradstreet v Greenmoss Builder Inc., 472 U.S. 749 (1985).
Whelan Associates v Jaslow Dental Laboratory, 797 F.2d 1222 (3rd Cir., 1986).
Hawley Fuel Coalmart Inc. v Steag Handel Gmbh, 796 F.2d 29,33 (2d Cir. 1986).
Secure Servs. Technology, Inc. v Time & Space Processing, Inc., 722 F.Supp.1354, 1364 (E.D. Va. 1989).
Corinthian Pharmaceutical v Lederle Laboratories, 724 F.Supp.605 (SD Ind.1989).
In re Groseth Int'l, Inc. 442 NW2d (SD 1989).
J I Case Co. v Early's Inc., 721 F.Supp.1082 (ED Mo.1989).
Cubby v CompuServe, 776 F.Supp. 135 (SDNY 1991).
Shell Pipeline Corp. v Coastal States Trading Inc., 1990 WL 12249 (Tex.Ct.Appl.1990).

European Court:

Case 24/67 *Parke Davis v Centrafarm* (1968) ECR 55, at 71.
Internationale Handelsgesellschaft v. EVSt, Case 11/70 [1970] E.C.R. 1125.
Case 155/73 (1974) E.C.R.409 (*Sacchi*).
Case 8/74 *Procureur du Roi v Dassonville* (1974) ECR 837.
Regina v Thompson 1978 E.Comm.Ct.J.Rep. 2247.
ECJ, 13.12.1979, Case 44/79.
X and Church of Scientology v Sweden, 16D and R68, 73 (1979).
Case 120/78 *Rewe v Bundesmonopolverwaltung fur Branntwein* (`Cassis de Dijon') 1979 ECR 649.
Case 52/79 *Debauve* (1980) E.C.R.857.
Codital v Cine Vog Films 1980 E.Comm.Ct.J.Rep 881.
Case 144/81 *Keurkoop v Nancy Kean Gifts* (1982) ECR 2853.
Case 311/84 *Tele-Marketing v Compagnie Luxembourgeoise de Telediffusion*, 2 CMLR, at p.558, 1984.
Case 41/83 *Italy v Commission* (1985) CMLR.
Magill TV Guide v ITP, BBC and RTE, July 10, 1991, IP/91/668.

STATUTES:

Austria:

Bundesgesetz vom 18.Oktober 1978 uber den Schutz personenbezogener Daten; Bundesgesetzblatt 1978, pp.3619 ff (amended July 1986).

Denmark:

Lov om private registre m.v., Lov nr.293 af 8.juni 1978 (private sector)
Payment Cards Act 1984.

France

Loi No.78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertiés, J.O. du 7 Janvier 1978 et rectificatif au J.O du 25 Janvier 1978.
Computer Crime Act of 5 Jan. 1988.
Loi de finances rectificative pour 1990 (No.90-1169 du 29 décembre 1990), Journal Officiel du 30 décembre 1990 on 31st December 1991.

Germany

General Terms and Conditions Act ["AGB-Gesetz"] of December 9, 1976 .
Gesetz zum Schutz vor Missbruach personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) vom 27 January 1977, BGB1. I 1977 S.201.
Second Act on Economic Criminality (1986).
Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesgesetzblatt 1990 I, p.2954, 1991.

Iceland:

Act No.39/1985 with regard to the Systematic Recording of Personal Data (English Translation: Council of Europe Info.Doc. CJ-PD (86) 15.)

Luxembourg:

Loi dun 31 mars 1979 reglementant l'utilisation des donnees nominative dans les traitements informatiques, Journal Officiel du Grand-Duche du Luxembourg A No.29 11 avril 1979 (English Translation: Personal Data (Automatic Processing) Act, Council of Europe Info.Doc. CJ-PD (79) 3.
Grand-Ducal Regulation of 22 December 1986.

Norway:

Lov om personregistre m.m av 9.juni 1978 no.48 (English Translation: Act of 9th June 1978 Relating to Personal Data Registers, Council of Europe Info.Doc. CJ-PD (86) 26.)

United States:

Uniform Commercial Code
US Restatement of Torts, 1939.
17A C.J.S. Contracts § 329 (1963)
Fair Credit Reporting Act 1970.
Privacy Act of 1974, 5 USC 552a, Public Law 93-579 93rd Congress, S.3418 / December 31, 1974.
Federal Rules of Evidence 1976.
Electronic Funds Transfer Act 1978.
17 U.S.C. (Patent Legislation)
Electronic Communications Privacy Act 1986, 18 U.S.C. 2510-21.
35 U.S.C. (Copyright Legislation)
Computer Security Act 1987, Public law 100-235, 40 U.S.C.

United Kingdom:

Bill of Lading Act 1855.
Bills of Exchange Act 1882.
Marine Insurance Act 1906.
Law of Property Act 1925.
Import, Export and Customs Powers (Defence) Act 1939.
The Law Reform (Frustrated Contracts) Act 1943.
Theft Act 1968.
Civil Evidence Act 1968.
Criminal Damage Act 1971.
Unfair Contract Terms Act 1977
Interpretation Act 1978.
Limitation Act 1980.
Protection of Trading Interests Act 1980.
Forgery and Counterfeiting Act 1981.
Supply of Goods and Services Act 1982
The Value Added Tax Act 1983.
The Police and Criminal Evidence Act 1984.
Telecommunications Act 1984.
Data Protection Act 1984.
Finance Act 1985.
Interception of Communications Act 1985.
Copyright Designs and Patent Act 1988.
Criminal Justice Act 1988.
Law of Property (Miscellaneous Provisions) Act 1989.
Computer Misuse Act 1990.
Contracts Applicable Law Act 1990.
Local Government Finance Act 1992.

<u>BOOKS</u>:

Arkin, S.S., (ed.), *Prevention and Prosecution of Computer and High Technology Crime*, Matthew Bender, 1990.

Arora, A., *Electronic Banking and the Law*, IBC Financial Books, 1988.

Bainbridge, D.I.:

Computers and the Law, Longman, 1990.

Intellectual Property, Pitman Publishing, 1992.

Baum, Michael S., Henry H. Perritt, JR., *Electronic Contracting, Publishing and EDI Law*, Wiley Law Publications, New York, 1991.

Bender, D., *Computer Law*, Volume 1-3, Matthew Bender, New York, 1991.

Bigelow, R.P., *Computer Contracts: Negotiating and Drafting*, Volume 1-2, Matthew Bender, New York, 1990.

Black, U.D., *Data Communications and Distributed Networks* (2nd Ed.), Prentice Hall International Editions, 1987.

Blume, P. (ed.), *Nordic Studies in Information Technology and Law*, No.7 Computer/Law Series, Kluwer/The Netherlands 1991.

Bradgate, R., and N. Savage, *Commercial Law*, Butterworths, 1991.

Caelli, W., D. Longley, and M. Shain,:

Information Security for Managers, Macmillan Stockton Press, 1989.

Information Security Handbook, Macmillan Stockton Press, 1991.

Campbell, Duncan and Steve Connor, *On the Record: Surveillance, Computers and Privacy*, Michael Joseph/London 1986.

Castell, Dr S., *The APPEAL Report*, Eclipse Publications, 1991.

Collier, Harry, *Information flow across frontiers: The question of transborder data*, Learned Information, Oxford, 1988.

Corby, Michael (General Editor), *Telecomms Users Guide to Regulations*, CommEd Books, 1989.

Court, J M, *Personal Data Protection: The 1984 Act and its Implications*, Manchester, NCC Publications, 1984.

Cross, R., and C. Tapper, *Cross on Evidence* (6th ed.), London, 1985.

Czarnota, B., and R. Hart, *Legal Protection of Computer Programs in Europe*, Butterworths, 1991.

Davies, D.W., and W.L. Price, *Security for Computer Networks*, John Wiley & Sons, 1984.

Dicey & Morris, *The Conflict of Laws* (11th ed.), Stevens, London, 1987.

van Dijk, J.C., and Paul Williams, *Expert Systems in Auditing*, Macmillan 1990

Dommering, E.J., and P. Bernt Hugenholtz (eds.), *Protecting Works of Fact*, Kluwer, 1991.

Edwards, C., N. Savage & I. Walden (eds.), *Information Technology and the Law* (2nd edition), Macmillan 1990.

Flaherty, D.H., *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press 1989.

Galtung, Andreas, *Paperless Systems and EDI: A survey of Norwegian law*, Complex 4/91, Tano, Oslo, 1991.

Gifkins, M. & David Hitchcock, *The EDI Handbook*, Blenheim Online/London 1988.

Gifkins, M., *EDI Technology*, Blenheim Online/London 1989.

Goode, R.M., *Electronic Banking: The Legal Implications*, The Institute of Bankers 1985 and Centre for Commercial Law Studies, Queen Mary College, University of London.

Hill, Richard, *EDI and X.400: using Pedi*, Technology Appraisals, 1990.

Hondius, F.W., *Emerging data protection in Europe*, North Holland, Amsterdam, 1975.

International Chamber of Commerce, *International contracts for sale of information services*, ICC/Paris 1988.

Keustermans, J.A. & Ingrid Arckens, *International Computer Law*, Matthew Bender/New York 1988.

Kutten, L.J., Bernard D. Reams & Allen E. Strehler, *Electronic Contracting Law: EDI and Business Transactions*, Clark Boardman, 1991

Kuwahara, S., *The Changing World Information Industry*, Atlantic Institute, 1985.

Linant de Bellefonds, Xavier, *Le Nouveau Droit Des EDI*, Editions des Parques, 1991.

Lindberg, Agne, *Electronic Documents and Electronic Signatures*, IRI Papers: The Institute of Legal Informatics, University of Stockholm, Sweden.

Long, Colin D., *Telecommunications Law and Practice*, Sweet & Maxwell/London 1988.

Longley, Dennis, and Michael Shain, *Dictionary of Information Technology*, 3rd Ed., Macmillan, 1989.

Mathijsen, Professor P.S.R.F., *A Guide to European Community Law* (4th edit.), Sweet & Maxwell/London 1985.

Meijboom, A.P., and C. Prins (eds.), *The Law of Information Technology in Europe 1992*, No.9 Computer/Law Series, Kluwer, The Netherlands 1991.

Miles, M.B. and A.M. Huberman, *Qualitative Data Analysis*, 1984, Sage, London.

Millard, Christopher J., *Legal Protection of Computer Programs and Data*, p171, Sweet & Maxwell/London 1985.

Nimmer, Raymond, T., *The Law of Computer Technology*, Warren Gorham & Lamont, 1985, and Cumulative Supplement No.2, 1991.

NCC, *EDI in Action* (3 vols.), National Computer Centre, 1989

Nordenstreng, F. and H.I. Schiller, *National Sovereignty and International Communications*, Ablex Publishing,1980.

NORDIPRO, *Legal Acceptance of International Trade Data Transmitted by Electronic Means*, Special Paper No.3, CompLex no. 10/83, Universitetsforlaget 1983.

Creating Legal Security in Electronic Data Interchange, Special Paper No.4, Tano/Oslo 1988.

Nugter, A.C.M., *Transborder Flow of Personal Data within the EEC*, No.6 Computer/Law Series, Kluwer/The Netherlands 1990.

Pearson, H., and Clifford Miller, *Commercial Exploitation of Intellectual Property*, Blackstone Press, 1990.

Pichler, M.H., *Copyright Problems of Satellite and Cable Television in Europe*, Martinus Nijhoff, 1987.

Piette-Coudol, Thierry, *L' Echange de Donnees Informatise et le Droit*, Editions Hermes, 1991.

Pipe, R.G. and Brown, C. (ed.), *The International Information Economy Handbook*, TDR, Springfield, 1985.

Poullet, Y. & G.P.V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law*, No.1 Computer/Law Series, Kluwer/The Netherlands 1988.

Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

Reed, C.:

(ed.), *Computer Law*, Blackstone/London, 1990.

Electronic Finance Law, Woodhead Faulkner, 1991.

Robertson, R., *Legal Protection of Computer Software*, Longman, 1990.

Rudden, B. and Derrick Wyatt, *Basic Community Laws*, Clarendon Press/Oxford 1980.

Saxby, S.:

The Age of Information, Macmillan Press, 1990.

(General Editor)*The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990.

Sauvant, K P, *International Transactions in Services: The Politics of Transborder Data Flows*, The Atwater Series on the World Information Economy No 1, Westview Press/London.

Savage, R.N., and C. Edwards, *A Guide to the Data Protection Act*[2nd ed.], Financial Training, 1985.

Schaff, S., (Editor) *Legal & Economic Aspectsof Telecommunications*, North-Holland, Amsterdam, 1990.

Seipel, Prof. P.:

Computing Law, LiberFörlag, Stockholm, 1977.

(ed.) *From Data Protection to Knowledge Machines*, No.5 Computer/Law Series, Kluwer/The Netherlands 1990.

Sieber, U., *The International Handbook on Computer Crime*, John Wiley & Sons, 1986.

Sizer, R. and P. Newman, *The Data Protection Act 1984*, Gower, 1984

Slater, Ken, *Information Security in Financial Services*, Touche Ross/Macmillan, 1991.

Style C., and C. Hollander, *Documentary Evidence*, Longman, 1991.

Smith, J.C., *The Law of Contract*, Sweet & Maxwell, 1989.

Tapper, C., *Computer Law* (4th edition), Longman 1989.

Tapper, G., and K. Tombs, *Document Imaging and the Law*, Meckler, forthcoming 1992/3.

Thomsen, H.B., & B.S. Wheble, *Trading with EDI: The Legal Issues*, IBC Financial Books 1989.

Vandenberghe, Prof. G.P.V., (ed.), *Advanced Topics of Law and Information Technology*, No.3 Computer/Law Series, Kluwer/The Netherlands 1989.

Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989.

Wade, E.C.S., and A.W. Bradley, *Constitutional and Administrative Law*, p.10, (10th Ed.) Longman 1986.

Wasik, M., *Crime and the Computer*, Clarendon/Oxford 1991.

Westin A., *Privacy and Freedom*, Atheneum/New York 1967.

Williams, D.W, (ed.) *Tax on the International Transfer of Information*, Longman, 1991.

Wright, B.:

EDI and American Law, TDCC: The Electronic Data Interchange Association, 1989.

The Law of Electronic Commerce - EDI, Fax and E-mail: Technology, Proof and Liability; Little, Brown and Company, Boston, 1991.

Wyatt, D. and A. Dashwood, *The Substantive Law of the EEC*, Sweet & Maxwell, 1987.

ARTICLES:

Aldhouse, F., "UK Data Protection - Where are we in 1991?", pp.180-187, 5 Yearbook of Law Computers and Technology, Butterworths, 1991.

Allen, Thomas, "Electronic Data Interchange, computer ordering and the formation of contracts", pp.2-13, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

Amory, B.E. and Yves Poullet, "Computers in the law of evidence - a comparative approach in civil and common law systems", pp.114-124, Computer Law & Practice, March/April 1987.

Andersen, Dr M.B., "The Danish Teletrust Proposal for a Centre-Certifying Authority", p.88, The Computer Law and Security Report, Vol.8, No.2, 1992.

Anthony, C.G., p8-9, "Paperless Trading - The Legal Problems of Industry", Proceedings of CELIM Conference, `Paperless trading & the law in the EEC', Brussels, 17-18 March 1986.

Amory, B., and M. Schauss, "EDI as a way to perform and conclude contracts", Computer Aided Trade, Compat 88, The Hague, 29 Feb.-2 Mar., 1988.

Armstrong, N., "The Disclosure of Computerised Evidence in Civil Proceedings", p.3-5, Applied Computer and Communications Law, Vol.8, No.10, 1991.

Bach, Gabriel, "Law and Politics in Transborder Data Flow", p1-24, Law/Technology, 2nd Quarter 1981.

Barber, B., "Data Protection, Computer Security, Standards and Safety", NHS Information Management Centre, July 1990.

Barrett, D., "Telecommunications and the EEC: Piecing together a fragmented market", pp.94-114, in Proceedings of `Legal, Contractual, Responsibility & Evidential Issues in EDI, EFT, EM, Fax & Telex Communications', London, 20 February 1992.

Barrett, B. and Coulter, C., "Proposed Council Directive on the legal protection of databases", pp.34-37, Computer Law and Practice, Vol.8, No.2, 1992.

Baum, Michael,:

"EDI and the Law", p78-83, EDI Forum, Vol.2, 1989.

"Analysis of Legal Aspects", p.129, in Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989.

"Commercially Reasonable Security: A key to EDI enforceability", Computer Law and Practice, Vol.6, No.2, pp.52-54, Nov.-Dec., 1989.

"The linkage between security and electronic commerce law", pp.83-98, Proceedings of the EDI and the Law Conference, 7 May 1992.

Bellégo, A. and B. Beer, "Legal Aspects of Trade Data Interchange", p690-701, Journal of World Trade Law, Vol. 20, No.6, 1986.

Bensoussan, A., p.20, `La gazette de la télématique et de la communication inter-enterprises', No.11, spring 1991.

Bentley, D.F., "Computer auditing - an aid to fraud investigation", pp.250-256, Computer Law & Practice, Vol.7, No.6, 1991.

Benyekhlef, K., "Échange Électronique de Données - Contrat Commenté", Université de Montréal, Faculté de Droit, September, 1990.

Bequai, August, "Legal questions surrounding EDI", p.181, Computer Law and Security Report, Vol.7, No.4, 1991.

Berge, J., "EDIFACT - a technical introduction", pp.63-78, in Gifkins, M., *EDI Technology*, Blenheim Online/London 1989.

Bergsten, Eric,:

"Trade Data Transmission: A Uniform Code (UNCID) - The Challenge for the drafters", p.6, The Computer Law and Security Report, vol.3, no.3, 1987.

"Paperless Systems: The Legal Issues", p.23-26, The Computer Law and Security Report, Vol.3, No.6, 1988.

Berkvens, Professor J.M.A.,

"Contractual Protection against software diseases", pp.105-116, *Amongst Friends in Computers and Law*, Computer/Law Series, No.8, 1990.

"Payment systems meet the EC data protection initiative", p.33-35, International Financial Law Review, August 1991.

Bertrand, A.R., "Le Contrat d' Interchange dans une perspective historique: Vers des Incoterms E.D.I.", CIREDIT - Bulletin du Droit des E.D.I., No.1, January 1991, and pp.107-114, in Linant de Bellefonds, Xavier, *Le Nouveau Droit Des EDI*, Editions des Parques, 1991.

Binder, M., "Negotiating Agreements for UCC 4A Funds Transfer Services", pp.58-65, EDI Forum Special Edition, 1992.

Bing, Jon:

"Transnational Data Flows and the Scandinavian Data Protection Legislation", p65-96, Scandinavian Studies in Law, 24(1980).

"Data Protection and Social Policy", p82-98, in Proceedings of the Fourteenth Council of Europe Colloquy on European Law: Beyond 1984: The Law and Information Technology in Tommorrows's Society, Lisbon, 26-28 September 1984.

"Information Law?", p219-239, Media Law & Practice,Vol.2, No.3 (1981).

"Reflections on a Data Protection Policy for 1992", pp.164-179, *Yearbook of Law Computers & Technology*, Vol.5, Butterworths, 1991 (Paper presented at the Conference, `Access to public sector information, data protection and computer crime', held by the Commission of the European Communities and the Council of Europe, Luxembourg, 27-28 March, 1990).

Bing, J., P. Forsberg, and E. Nygaard, *Legal Issues related to transborder data flows*, DSTI/ICCP/81.9.

Blume, Dr P., "Data Protection and the EEC", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Boss, Amelia H., "The Proliferation of Model Interchange Agreements", pp539-553, Proceedings of the 3rd International Congress of EDI Users, 4-6 September, 1991.

Bourn, C & Benyon, J. "Data Protection: Perspectives on Information Privacy", contribution made to a Conference on 11 May 1983 at the University of Leicester, Continuing Education Unit.

Bortnik, Jane, "International information flow: The developing world perspective", p333-353, 14 Cornell International Law Journal, 1981.

Bradgate, R.:

"Evidential Problems of New Technology in Civil Litigation", p12-14, Law Society Gazette, 10 February 1988, Vol.85, No.6.

`Evidential Issues in EDI', p9-42, in Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989.

"The evidential status of computer output and communications", p142-148, Computer Law & Practice, Vol.6, No.5, May-June 1990.

"The computer, the court and the curate's egg: is it hearsay or not?, p174-177, Computer Law & Practice, Vol.7, No.4, March-April 1991.

"Privacy and Telecommunications", p.5-7, Applied Computer and Communications, Vol.8, No.7, 1991.

Briat, Martine, `Personal Data and the Free Flow of Information', in *Freedom of Data Flows and EEC Law*, proceedings of 2nd CELIM Conference,Kluwer, 1988.

Brizida, "Transborder Data Flows in Brazil" (1982) 13 CTC Reporter (UN Centre on Transnational Corporations).

Brock, William E., "Global Competition: What Impact on US Industry?", 52 Antitrust Law Journal, 147 (1983).

Brown, R.A., "EDI and proving your transaction", paper included in the proceedings for SOST'89, Australian Computer Society Inc., Sydney, May 1989.

Brown, Ronald Wellington:

"A Model Code for Transnational Commerce?", p117-124, Transnational Data and Communications Report, Vol.VII, No.2, 1984.

"Economic and Trade Related Aspects of Transborder Data Flow: Elements of a Code for Transnational Commerce", p1-86, Northwestern Journal of International Law and Business, Spring 1984, Vol.6, No.1.

Brousse, Pascal, "Towards a more suitable interchange contract", ICC Document No.460-10/Int.32.

Brunet, Christophe, "Artificial Intelligence in EDI", pp.93-101, Proceedings of '91 International Conference on EDI, 7-8 November, 1991.

Buffelan-Lanore, Professor Jean-Paul, "The legal definition of computer document", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Burkert, Herbert:

"Institutions of Data Protection - An attempt at a functional explanation of European data protection laws", pp167-188, Computer/Law Journal, vol.III, 1981

"Information Law Problems for the Eighties", p.331-336, Transnational Data Report, Vol.VII, No.5&6, 1984.

"International Data Protection", p155-160, Computer Law and Practice, May/June 1986.

Bushkin, Arthur A., "The threat to International Data Flows" Business Week (3 August 1981).

Buss, Martin, D.J., "Managing International Information Systems", Harvard Business Review 60 (September/October 1982).

Bytheway, A., "EDI: Technical opportunity or business necessity", working paper from `EDI: The longer term effects on international trade' research programme, July 1989.

Carlsen, R.C., "Network and User Responsibilities: A contract perspective", paper presented at EDI: Letters of the Law, Dallas, Texas, 15-16 February 1990.

Castell, Dr Stephen,:

"The Legal Admissibility of Computer Generated Evidence: Towards `legally reliable' information and communications technology", paper presented at COMPACS 89, London, 14-17 March 1989.

"Evidence, Authorization and Security: Is the technology `legally reliable'", Computer Law and Practice, Vol.6, No.2, pp.46-51, Nov.-Dec., 1989.

"Broadcasting and Cable - The New Framework", pp.20-24, The Computer Law and Security Report, Vol.6, No.1, 1990.

Chalton, S.:

"The Authentication of the Origin and Content of Paperless Transactions, and Questions of Liability in Common Law", p103, Proceedings of CELIM Conference: `Paperless Trading & the Law in the EEC', Brussels, March 17-18, 1986.

"Dematerialisation of financial instruments", p30-34, Computer Law & Practice, Vol.7, No.1, 1990.

Chalbainou, Dr E., "Some of the legal problems of electronic money", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Chamoux, Jean Pierre. "Data Protection in Europe: The Problem of the Physical Person and the Legal Person", p70-83, 2 Journal of Media Law and Practice 70 (1981).

Chamoux, F., "The Electronic Notary", pp.149-150, Tedis Legal Workshop, Brussels, June 19-20, 1989.

Chandler III, George F., "The Electronic Transmission of Bills of Lading", p571-579, Journal of Maritime Law and Commerce, Vol.20, No.4, October 1989.

Chaum, D., "Undeniable Signatures", pp.204-209, Proceedings of Compsec 89, London, 11-13 October 1989.

Cluff, E., "UK Privacy Law - A DP Management View" Transnational Data Report V (2), March 1982, pp103-104

Cocca, A.A., "Human Condition and Communications - the Right to Communicate", p15, Transnational Data and Communications Report, May 1988.

Cole, Patrick E., "New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data Protection Laws.", p893-947, New York University Journal of International Law and Politics, vol.17, No.4, Summer 1985.

Cook, Trevor, "Facilities Management and Other Computer Services Contracts", pp.130-141, in Edwards, C., N. Savage & I. Walden (eds.), *Information Technology and the Law* (2nd edition), Macmillan 1990.

Cook, W.:

"Paying the bill for hostile technology: PBX Fraud in 1991", pp.174-177, Computer Law and Security Report, Vol.7, No.4, 1991.

"Trends in Network Liability: 1992", pp.213-216, The Computer Law and Security Report, Vol.8, No.5, Sept./Oct. 1992.

Coombe, G.W. & Susan L. Kirk, "Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations", pp33-66, The Business Lawyer Vol.39, No.1, November 1983.

Cooper, David M.,[3] "Transborder Data Flow and the Protection of Privacy: The Harmonisation of Data Protection Law", p335-352, The Fletcher Forum, Vol.8, Prt 2, 1984.

Cornwall, Hugo, "Hacking away at computer law reform", p702-703, New Law Journal, Sept.30, 1988.

Cover, M., and M. Scoggins, "Anton Piller Orders - lessons for the software industry through a decade of development", pp. 62-67, Computer Law & Practice, Vol.8, No.3, 1992.

Cowen, T.:

"Judgement in France v Commission", p.3-5, Applied Computer and Communications Law, Vol.8, No.5, 1991.

"The deregulation of telecommunications in the European Community", p.202-206, Computer Law and Practice, Vol.7, No.5, 1991.

Crawford, B., "Strategic Legal Planning for EDI", p66-77, Canadian Business Law Journal, Vol.16, 1989.

Davies, David, "EDI Insurance - The `Red Herring' Theory Examined", in Proceedings of the 6th Annual Canadian Law Conference, London, 1 November 1991.

Deloitte Haskins & Sells, & National Computing Centre, "The External Auditor as Privacy Inspector" Information Age 5(3) July 1983, pp131-142.

de Cockborne, J-E., "The EC Commission Directive on Competition in the Market for Telecommunications Services", pp.96-115, *Yearbook of Law Computers & Technology*, Vol.5, Butterworths, 1991.

de la Presle, Madame Anne, "Towards a legal framework for EDI transactions", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

de Soete, M., "Smart Cards and their applications", pp.147-154, Proceedings of Compsec 91, London, 30 Oct.- 1 Nov., 1991.

de Vries, Dr H., "How to secure Legal Effect for Commercial Deals made by Electronic Messages Transmission".

Dixon, H., "Data registration rules criticised", Financial Times, 3rd October, 1986.

Draper, J., "Open networks and security", pp.330-337, in Proceedings from COMPAT'89, 3-5 April 1989.

Dresner, S., "New Style Data Protection Laws: Convergence or Radical Change?", Proceedings of `Data Protection in Ireland, The Netherlands and Switzerland' Conference, 19 October, London, 1988.

Dumbill, E.A.:

"Computer Crime", p.5, Applied Computer and Communications Law, Vol.7, No.4, 1990.

"Other criminal offences", p.36-48, Proceedings of `Data Security and the Law' Conference, London, 5 July, 1991.

"EC Directive on computer software protection", p.210-213, Computer Law and Practice, Vol.5, No.5, 1991.

Dumortier, Professor Jos, "Data Protection in the Schengen Convention", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Durie, R., "Problems with data protection legislation", p.164, in Proceedings of `Legal, Contractual, Responsibility & Evidential Issues in EDI, EFT, EM, Fax & Telex Communications', London, 20 February 1992.

Dziewit, H. S., Graziano, J. M., Daley, C.J., "The Quest for the Paperless Office - Electronic Contracting: State of the art possibility but legal impossibility?", Santa Clara Computer & High Technology Law Journal, Vol.5, No.1, pp.75-97, Feb. 1989.

Early, L., "Securing equivalent protection among nations in the context of transborder data flows: a possible role for contract law", pp.10-14, Droit de l'informatique et des telecoms, 1990/4.

Eger:

"Transborder Data Flow", p.50, 24 Datamation, Nov.15, 1978.

"The Global Phenomenon of Teleinformatics: An Introduction", pp.203-234, 14 Cornell International Law Journal, 1981.

Elias, Lieve:

"Data security and formation of contracts", paper presented at `Data Security in Computer Networks and the Legal Problems' Conference, Hannover, 23-24 September, 1991.

"Les questions juridiques soulevées par l'EDI", pp.32-35, Journal de réflexion sur l'informatique n°22, March 1992.

Ennison Jr., Thomas, "Sovereignty Considerations in TDF - developing country perspective", p175-181, Transnational Data and Communications Report, Vol.VII, No.3, 1984.

Epperson, Michael G., "Contracts for transnational information services: Securing equivalency of data protection", p157-175, Harvard International Law Journal, 22, Winter 1981.

European Communities Parliament, Sub-committee on Data Processing and the Rights of the Individual Protecting the Individual. Information Privacy 1(8) Nov 1979, pp335-364.

van Esch, R.E., "Electronic data interchange contracten", p.263, in *Hoofdstukken Informaticarecht*, F.de Graaf and J.M.A. Berkvens (ed.), , Alphen a/d Rijn, 3rd edition 1991.

Evans, A.C.:

"Emerging Restrictions on Transnational Data Flow: Privacy Protection or Non-Tariff Barriers?", p1055-1103, 10 Law & Policy in International Business.

"European Data Protection Law", p571-582, The American Journal of Comparative Law, vol.29, 1981.

Evans, Dr S., "CALS", at p.224-232, Proceedings of EDI'90, 30 Oct.-1 Nov, 1990.

Faber, Diana, "Shipping Documents and EDI", in Proceedings of the 6th Annual Canadian Law Conference, London, 1 November 1991.

Feldman, Mark, "Commercial Speech, Transborder Data Flows and the Right to Communicate under International Law", The International Lawyer, vol.17 no.1 (winter 1983), pp87-95.

Fergus, D., "European EDI in the financial sector", p.105-121, Proceedings of '91 International Conference on EDI, 7-8 Nov., Korea.

Fischer, A.M., "Electronic Document Authorization", 1990.

Fishman, "Introduction to Transborder Data Flows", 16 Stamford Journal of International Law 1, 1980.

Flaherty, D.H.:

"Cumulative data are not always anonymous", p.6, Privacy Journal, 9/1985.

"Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies", pp.7-18, Science, Technology & Human Values, Vol.11, Issue 1, Winter 1986.

"Towards the year 2000: The Emergence of Surveillance Societies in the Western World".

"Computers and Privacy: How to regulate the private sector", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Ford, D., "Virus Clauses", p.4-5, Applied Computer and Communications Law, Vol.7, No.6, June 1990.

Foremski, T., "Lax case of security standards", p.10, Computing, 16 August, 1991.

Franken, Hans, "Computing and Security", pp.131-140, *Amongst Friends in Computers and Law*, Computer/Law Series, No.8, 1990.

Freeman, R.C., "Legal aspects of computerised procedures for Customs administrations", p.28-42, Proceedings of Paperless Trading and the Law in the EEC Conference, 17-18 March, Brussels, 1986.

Fresse, Jan, "EDI and National Legislation" - Teresa (86) Draft Report, ICC Doc. No. 460-10/Int.43.

Frosini, Vittorio (Professor of Jurisprudence, University of Rome), "The European Convention on data protection", Computer Law and Practice, January/February 1987, pp84-90.

Gaskill, S.J., "Data Protection: Recent Court and Tribunal Cases", Proceedings of Privacy Laws & Business, 4th Annual Conference, Cambridge, 2-4 July, 1991.

Goebel, J.W., "The `Trustworthy Third Party' within the Security System", at 3., in *Concepts, Applications and Activities*, a TeleTrust Publication.

Goetzman, J., "Audit and Security Responsibilities: An EDI Service Provider's Perspective", paper presented at EDI: Letters of

the Law, Dallas, Texas, 15-16 February 1990.

Golden, K. "Transborder Data Flows and the possibility of guidance in personal data protection by the ITU", Houston Journal of International Law, Vol.6, No.2, pp215-41, 1984.

Goode R. & Bergsten E., "Legal questions and problems to be overcome", pp131-133, in Thomsen, H.B., & B.S. Wheble, *Trading with EDI: The Legal Issues*, IBC Financial Books 1989

Gotlieb, A., C. Dalfen and K. Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", pp227-257, The American Journal of International Law, Vol.68, 1974.

"Governments and Companies seek TDF Cooperation" Transnational Data Report VII(1) Jan/Feb 1984, pp26-31.

Greguras, Fred M, and Richard Sizer., "Impact of transborder data flow restrictions on cash-management services", pp17-22, Information Age, Vol.9, No.1, January 1 1987.

van Grevenstein, P.V.U., "Restrictions on transborder transmissions of commercial data under EEC law", pp.65-74, in Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

Gronfers, "The Paperless Transfer of Transport Information and Legal Functions", in Schmitthoff & Goode (ed.), *International Carriage of Goods: Some Legal Problems and Possible Solutions*, 1988.

Groshan, R.M., "Transnational Data Flows: Is the idea of an international legal regime relevant in establishing multilateral controls and legal norms?", Part I: pp1-30, Law/Technology (4th Quarter 1981); Part II: pp1-37, Law/Technology (1st Quarter 1982).

Grossman, Gary "Transborder Data Flow: Separating the privacy interests of individuals and corporations" Northwestern Journal of International Law and Business 4 (1981): 1-36.? 1982 1,21.

Groustra, F., "Transborder data flow and European Community Law", pp.75-84, in Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

Hanotiau, Bernard, "The transborder flow of data - applicable law and settlement of disputes", p.175-197, in ICC, *International contracts for sale of information services*, ICC/Paris 1988.

Harvey, S. and J. Newman, "Contracts by electronic mail: some issues explored", The Computer Law and Security Report, vol.3, no.6, March-April 1988.

Henriksen, R., "Signature and Evidence in the international trade and transport society without documents", p.44-101, in NORDIPRO, *Legal Acceptance of International Trade Data Transmitted by Electronic Means*, Special Paper No.3, CompLex no. 10/83, Universitetsforlaget 1983.

Herman and Halvey, *International Flow of Data is threatened*, American Banker, Sept. 25, 1990.

Hermann, A.H., "New Trade Pacts and Incoterms 1990", paper presented at the International Company Lawyers' Conference, Lisbon, 20-22 February, 1991.

Herson, D., "Security Evaluation and Certification", p.17-24, Proceedings of the `Data Security and the Law' Conference, London, 5 July, 1991.

Hickmott, G.T., "Data Restrictions: Users' Concerns", p25-27, Transnational Data and Communications Report, Vol. IX, No.12, 1986.

Himmelstrand, Ulf. "The Data Fetish", p21-22, New Society, 16th January, 1987.

Hoeren, T., "EDI and Transborder Flow of Personal Data: The perspectives of private international law and data protection", pp.81-88, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

Hogrebe, M E (1981) "Legal Persons in European Data Protection Legislation: Past Experiences, Present Trends and Future Issues"; DSTI/ICCP/81.25, OECD, Paris.

Hondius, F.W., "Data Law in Europe", p.109, 16 Stanford Journal of International Law, 1980.

Hoyle, C., "Transborder Data Flows", paper presented at `Legal, Contractual, Responsibility and Evidential Issues in EDI, EFT Email and communications by fax or telex', London, 20 February 1992.

Huet, Jérôme, "Aspects juridiques de l'EDI, Échange de Données Informatisées", Chronique, No.27, 1991.

Humphreys, E.J., "Open Systems Security, Paperless Trading and the Single European Market", British Telecommunications plc, Feb. 1987.

Hunter, B.E., "Legal Responsibilities of EDI Service Providers: A Service Provider's Perspective", paper presented at EDI & the Law, Washington, Feb. 1991.

Hurford, C., "The 1991 Computer Fraud Survey", p.67-71, Proceedings of Compsec 91, 30 Oct.-1 Nov., 1991.

Hustinx, P., "The role of the Council of Europe", Privacy, Laws and Business Conference on Data Protection in Ireland, The Netherlands and Switzerland, 19th Oct. 1988.

Hutchinson, W., "Data to declare", Communications, August 1987.

International Chamber of Commerce (ICC), "Policy Statement on Privacy Legislation, Data Protection and Legal Persons", adopted by the Council of the ICC in July 1984; in Transnational Data Report, vol.11, No.7, Oct/Nov 1984.

Jenkins, Lyn, "Legal admissibility of documents on microfilm or optical disk", p.17, Records Management Bulletin, No.48, February 1992.

Jones, M., The Computer Misuse Act 1990, in Proceedings of the *Data Security and the Law Conference*, 8 May 1992.

Kane, M.J. and D.A. Ricks, "The Impact of Transborder Data Flow Regulation on Large United States-Based Corporations", p23-29, The Columbia Journal of World Business, Vol.XXIV, No.2, 1989.

Kaspersen, H.W.K., "Standards for Computer Crime Legislation: A Comparative Analysis" in Vandenberghe, Prof. G.P.V., (ed.), *Advanced Topics of Law and Information Technology*, No.3 Computer/Law Series, Kluwer/The Netherlands 1989.

Katus, Sergej, "Three Types of EDI Contracts", pp.89-94, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

Kelley, P.L., "The impact of customs and taxation on data flows in the EEC", pp.115-126, in Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

Kelly, Michael, "Surveys Show Strategic Importance of TDF", p20, Transnational Data Report, vol.VII, no.1 [Jan/Feb 84].

Kelman, Alister, "Legal implications of emerging technology and applications", Proceedings of Managing Network Security in the 90's, Conference, London, 13 Sept., 1991.

Kemp, Richard, "Public Sector IT Acquisition", The Journal - Local Government, Spring 1991.

Kerkau, H.J., "Data Protection and Telecommunications", pp.75-77, Proceedings of *EDI - 1992 and beyond*, Brussels, September 1989.

Kerr, Susan, "Legal Laissez-Faire", p54-56, Datamation, 5 April, 1989.

Kesler, V.L., "Legal blueprint for transborder data flow cooperation" paper presented at IBI Second World Conference on Transborder Data Flow Policies, Rome, 26-29 June, 1984.

Ketelaar, Mr R.J.C., "Controlling the Data Controller", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Kindred, H. M., "Trading internationally by electronic bills of lading", pp.265-289, Banking and Finance Law Review, Vol.7, February 1992.

Kirby, M.:

"The Morning Star of Informatics Law and the need for a greater sense of urgency", paper presented at the Intergovernmental Bureau for Informatics, Rome, Italy, 26-29 June, 1984.

"Legal Aspects of Transborder Data Flow", pp.233-243, 11 Computer/Law Journal, 1991.

Kirsch, William J., "The Protection of Privacy and Transborder Flows of Personal Data: The work of the Council of Europe, the Organisation for Economic Co-operation and Development and the European Economic Community", Legal Issues of European Integration 2 (1982), p21-50.

Knoppers, J., "Transforming Cross Industry Practices into EDI: The business case for scenario modelling", p.578, in Proceedings of the 3rd International Congress of EDI Users, 4-6 Sept., 1991.

Krommenacker, R.J., "The Impact of Information Technology on Trade Interdependence", p381-400, The Journal of World Trade Law, Vo.20, No.4, 1986.

Kuitenbrouwer "The World Data War" (1981) 91 New Scientist, p604.

Kunzlik, P.F., "Completing the jigsaw - EC public procurement rules and the IT sector", pp.73-77, Computer Law & Practice, Vol.8, No.3, 1992.

Lambert, Jean, "Les aspects juridiques du télécopieur: un cauchemar juridique?", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Lane, David, "EDI: Can Equity cope?", pp.95-98, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

Lass, J., "Business Records and Paperless Trading", paper presented at `The Changing Pattern of Business' Conference, London, 25-26 September 1989.

Lee Johnson, G., "Electronic contracts: Are they enforceable under Article 2 of the UCC?", pp.247-269, Software Law Journal, Vol.4, April 1991.

Llewelyn, D., "The sale and transmission of non-personal data into England: the legal issues", pp119-124, Computer Law & Practice, March/April 1986.

Lindsay, D., "Encryption and Regulatory Controls in Europe", p.28-30, The Computer Law and Security Report, Vol.7, No.1, 1991.

Lindop, Sir Norman, "Legislating for Data Privacy" In Campbell, C (ed.), *Data Processing and the Law*, Sweet & Maxwell/London 1984, pp 155-170.

Lindup, K.R., "Computer Audit - a threshold", pp.17-21, Computer Audit Update, October 1991.

List, W.:

"Audit", p72, Proceedings of the EDI and the Law Conference, London, 4 July, 1990.

"Electronic trading - the implications", paper presented at EDP Auditors Association Conference on Electronic Trading, 11 June 1991.

"International EDI - the implications for record keeping", p.474-480, Proceedings of the 3rd International Congress of EDI Users, Brussels, 4-6 September, 1991.

Long, C., and David Kerr, "Chapter 2: The Licences", at s.2.3.1., in Corby, Michael (General Editor), *Telecomms Users Guide to Regulations*, CommEd Books, 1989.

Love, K., "Seadocs: The lessons learned", in proceedings of `The Future of Bills of Lading', 7-8 April, London, 1992.

Lowry, Houston Putnam.:

"Does computer stored data constitute a writing for the purposes of the statute of frauds and the statute of wills", Rutgers Computer & Technology Law Journal, Vol.9, No.1, pp.93-107, 1982.

"Transborder Data Flow: Public and Private International Law Aspects", Houston Journal of International Law, vol.6 part 2 (1984), pp159-174.

Madec, A. "Les flux transfrontières de données", Informatisation et Société, No. 12, 1982.

Malveaux, J., "Flyspecks on the scales of injustice", USA Today, 17th October, 1987.

Mandela, Audrey, "EDI trends and directions", Yankee Group Europe Seminar, Level:8, Vol.12, No.4, April 1992.

Mankabady, S., "The Electronic Transmission of Commercial Contracts", pp.125-130, in Conference Proceedings Bileta, 5th Annual Conference, 1990.

Markoski, Joseph P., "Telecommunications Regulations as barriers to the transborder flow of information", p287-331, Cornell International Law Journal, vol.14, no.2, Summer 1981.

Marsh, David:

"EDI Legal Developments in International Trade", paper presented at EDI'89, London, 31 Oct. - 2 Nov., 1989.

"Legal aspects of EDI', pp.427-430, Proceedings of EDI 92, Paris, 2-4 June 1992.

Marsh, S., "Application of IT Security Evaluation and Certification", pp.107-115, in Proceedings of the `Data Security and the Law' Conference, London, 8 May, 1992.

Martino, A.A., "Paperless Trade: Legal and Techincal Standardization Problems", paper presented at COMPAT 88, Hague, Holland, 29 Feb.- 2 Mar. 1988.

Martino, A.A., and Paola Palmerini, "International and national legislation on EDI", paper presented at FIRLITE Conference: `Data Security in Computer Networks and Legal Problems', 23-24 September,1991, Hanover.

Martyn, J., "Data Protection Legislation outside the UK", Aslib Proceedings, Vol.37, No.8 (August 1985), pp329-337.

McCarthy Tétrault, `Electronic Data Interchange: A survey of the legal issues', prepared for the EDI Institute, January 1991.

McKeaver, E.D., "Is it best not to regulate Transborder Data Flow?", pp.159-163, International Business Lawyer, April 1984.

McMurchie, S.E., "Will the Jolly Rodger fly again? Can pirate databanks be prevented?", pp299-301, European Intellectual Property Review 11, 1984.

McTaggart, B., "Developments in the use of EDI for CAD/CAM interchange", p.581-587, Proceedings of EDI'90, 30 Oct.-1 Nov, 1990.

Mellors, C & Pollitt, D., "Legislating for Privacy: Data Protection in Western Europe", Parliamentary Affairs 37(2) Spring 1984, pp199-215.

Menou, M.J., "Cultural Barriers to the International Transfer of Information", p 121-129, Information Processing and Management, Vol.19, No.3, 1983.

Messmer, A., "Is EDI legal", Information Week, July 1989.

Meyer, J., "The Challenge of Electronic Commerce", p.85, ABA Journal, March 1992.

Miller, A.P., "Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age", pp89-144, Columbia Journal of Law and Social Problems, 20:89, 1986.

Miller, C., "Proving the transaction took place", pp. 55-83, in Proceedings of `Legal, Contractual, Responsibility & Evidential Issues in EDI, EFT, EM, Fax & Telex Communications', London, 20 February 1992.

Millard, C.J.:

"Transborder Data Flows: The European Perspective", paper presented at the Computer Law Association's Conference on `Distribution, Access & Communications', Amsterdam, 1-3 June 1988.

"Contractual Issues of EDI", pp.43-48, in Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989.

Millard, C., and Sa'id Mosteshar, "International Telecommunications", p.10003-10043, in Saxby, S., (General Editor) *The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990.

Moakes, J., "Data Protection in Europe - Part 1", pp77-86, Journal of International Business Law, no.2, 1986; "Part 2", pp143-151, 3 JIBL, 1986.

Moitinho de Almeida, J.C., "Data Flow and Community Law", p.7-22, in Proceedings of the 2nd CELIM Conference, *Freedom of Data Flows and EEC Law*, No.2 Computer/Law Series, Kluwer/The Netherlands 1988.

Monssen, W., "Transborder Data Flow Presentation" on behalf of the International Air Transport Association to Data Commissioners Conference, Quebec, September 1987.

Morrin, J.P., "Customs requirements and international trade", Computer Law and Practice, Vol.6, No.2, pp.42-45, Nov.-Dec., 1989.

Morris, B. and M. Hutchings, "Cross Frontier Broadcasting and the Law", Law Society's Gazette, No.22, 11/6/1986.

Morriss, P.W., "Electronic Data Interchange: Security, Control and Audit", p.81-96, COMPSEC 89, London, 11-13 Oct., 1989.

Mosteshar, S., "Liability Issues in EDI", pp.49-55, in Walden, I. (ed.), *EDI and the Law*, Blenheim Online/London 1989.

Moyse, Malcolm, "No room left for the middle-man", p.10, Financial Times, 8/8/90.

Nacamuli, A., "The SWIFT Project", p.77-85, Proceeding of the 3rd International Congress of EDI Users, Brussels, 4-6 Sept., 1991.

Napier, B.W.:

"Contractual solutions to the problem of equivalent data protection in transborder data flows", pp.8-19, International Computer Law Adviser, September 1990.

"Information Security: Contractual Issues", pp.83-94, in Proceedings of `Data Security & the Law' Conference, London, July 1991.

"Ensuring international personnel databases comply with national laws", p.19-20, Privacy Laws & Business, No.14, August 1991.

"Computerization and employment rights", pp.1-14, Industrial Law Journal, Vol.21, No.1, March 1992.

Nellson, A., "Insuring against the inevitable", pp.195-200, *Data Security & the Law* Conference, 8 May 1992.

Nelson, Jim and David Reisman, "Transborder data barriers may restrict encryption", p41, Computerworld, 24 March 1980.

Nimmer, R.T., "Legal obligations of the EDI Service Provider", paper presented at EDI & the Law, Washington, Feb. 1991.

Novotny, Eric J.:

"Transborder Data Flow and International Law: A Framework for Policy-Orientated Inquiry", p141-180, 16 Stamford Journal of International Law, 1980.

"Transborder Data Flows Regulation: Technical Issues of Legal Concern,", pp105-124, Computer/Law Journal III, Spring 1982.

Nycum, S.H., "Electronic Data Interchange", in proceedings from University of Southern California Law Center Twelfth Annual Computer Law Institute, June 6-7, 1991.

O'Brien, Kevin O., "Global Value Added Network Providers: Contractual Analysis of Legal Liability Issues", paper presented at the 4th EDI Electronic Data Interchange Conference, USA??

O'Conner, W.F., "Information - the next trade problem?", Data Communications, March 1986, pp186-191.

Pearson, H., "A blow to computer data base protection", p6-7, Applied Computer and Communications Law, Vol.8, No.5, 1991.

Petre, Blanche, "Network Providers", p8-18, Computer Law and Practice, Vol.7, No.1, Sept-Oct. 1990.

Piette-Coudol, Thierry:

"Quel Regime Juridique pour l' E.D.I.?", Expertises, No.130, p.270, 1990.

"La Problématique Juridique Générale du Passage à l'E.D.I.: Entre le Formalisme et la Preuve", CIREDIT - Bulletin du Droit des E.D.I., No.1, January 1991.

"From Interchange Contracts...To Interchange Profiles", ICC Document No. 460-10/Int.34.

"Legal aspects of electronic billing", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Pinegar, Kevin R. "Privacy Protection Acts: Privacy Protection or Economic Protectionism?", p183-88, The International Business Lawyer, April 1984.

Pipe, G.R.:

"National Policies, International Debates", p118, Journal of Communication, vol.29, Summer 1979.

"Searching for Appropriate TDF regulation", p9, Tranational Data Report 7 (1984).

Ploman, E.W., "Transborder Data Flows: The International Legal Framework", pp551-562, Computer/Law Journal, Vol.III, 1982.

Pool, I & R.J. Solomon, "Intellectual Property and Transborder Data Flows", pp113-139, Stanford Journal of International Law, vol.16, 1980.

Poullet, Y.:

"The Information Contract - contractual aspects: confidentiality clauses", pp.119-156, in ICC, *International contracts for sale of information services*, ICC/Paris 1988.

"Privacy Protection and Transborder Data Flow: Recent Legal Issues", pp.29-42, in Vandenberghe, Prof. G.P.V., (ed.), *Advanced Topics of Law and Information Technology*, No.3 Computer/Law Series, Kluwer/The Netherlands 1989.

"Law of evidence and the new information and communication technologies: From laissez-faire to regulation", in Proceedings of International Conference on Computers and Law, Montreal, Canada, 30 Sept.-3 Oct., 1992.

Pounder, C., "EC sharpens the claws of data protection law", p.24-25, Computing, 18 October, 1990.

Power, L., "The legal implications of commercial electronic letters of credit", pp.115-137, in Proceedings of the *3rd National Conference on Law, Computers and Artificial Intelligence*, University College of Wales, Aberystwyth, 30 March-2 April 1992.

Prins, Corien, "Standardisation of EDI Technology - A Trojan Horse?", pp.138-145, Proceedings of the 3rd National Conference on Law, Computers and Artificial Intelligence, University College of Wales, Aberystwyth, 30 March-2 April 1992.

Pym, J. and Peter Hill, "Taurus", pp.13-22, Practical Law for Companies, Vo. II, No.7, August 1991.

Quest, P., "Computer Fraud - The auditor's approach", pp.19-22, The Computer Law and Security Report, Vol.6, No.3, 1990.

Radcliffe, M., "Coping with EDI under sales law", pp.38-40, EDI Forum Special Edition, 1992.

Ramsey, "Europe Responds to the Challenge of the New Information Technologies: A Teleinformatics Strategy for the 1980's", Cornell International Law Journal, Vol.14, No.2, Summer 1981, p279.

Rankin, T. Murray., "Business secrets across international borders: one aspect of the transborder data flows debate", Canadian Business Law Journal, 10 (1985).

Raymont, P., "New Technology and Data Protection", 119-121, Yearbook of Law Computers and Technology, Vol.2, 1986.

Raysman, R. and P. Brown, "An electronic data interchange agreement", p.3, New York Law Journal, Vol.203, April 10, 1990.

Reed, C.:

"The Legal Aspects", p.86-94, in Potts, R.J., (ed.) *An Introduction to the Security of Computer Systems*, PLC Consultancy Services, 1988.

"Authenticating Electronic Mail Messages - Some evidential problems", p649-660, Modern Law Review, Vol.52, September 1989.

"EDI - contractual and liability issues", p.36-41, Computer Law & Practice, Vol.6, No.2, 1989.

"Electronic Trade Documentation: Legal Obstacles and Solutions", pp.35-55, *EDI & the Law*, 7 May 1992.

Rees, F., "Australia's laws and electronic data interchange", p.23, Business Law Review, Vol.12, January 1991.

Reidenberg, Professor J.R.:

"United States Data Protection in the Private Sector: Between a Fortress for Individual Rights and the Wild West", Proceedings of Privacy Laws & Business, 4th Annual Conference, Cambridge, 2-4 July, 1991.

"An American solution to TBDF personal data contractual problems", pp.12-14, Privacy Laws and Business, No.19, December 1991.

"Personal Information and Global Interconnection: The Challenge of Regulatory Convergence", pp.27-36, The Economic Integration Frontier, Project Promethee Perspectives n.18-19, December 1991.

"The privacy obstacle course: hurdling barriers to transnational financial services", pp.137-177, Fordham Law Review, Vol. LX, No.6, May 1992.

Reinskou, Kurt Hegle, "Bills of Lading and ADP: Description of a Computerized System for Carriage of Goods by Sea", Journal of Media Law & Practice, Vol.2, No.2, September 1981.

Rettig, Dr. and Dr. Otto, "Insurance Coverage and EDI", paper presented at `Data Security in Computer Networks and the Legal Problems' Conference, Hannover, 23-24 September, 1991.

Richardson, J.B., "International Trade Aspects of Telecommunications Services", p385-399, Common Market Law Review, Vol.23, 1986.

Ritter, J.B.:

"Who's responsible when technology fails?", p6, EDI Executive, February 1990.

"Scope of the Uniform Commercial Code: Computer contracting cases and electronic commercial practices", pp.2533-2557, Business Lawyer, Vol.45, August 1990.

"Electronic commerce and international law: a tapestry in the making", pp.117-126, Proceedings of the 3rd International Congress of EDI users, 3-6 September, 1991, Brussels.

Robertson, Ranald, "Playing with a new set of rules", p.51, Banking Technology, February 1990.

Robinson, Peter:

"Sovereignty and Data: Some Perspectives", p419-421, Transnational Data and Communications Report, Vol. VII, No.7, 1984.

"Extraterritoriality and Data Flows", p27-28, Transnational Data and Communications Report, Vol.IX, No.6, 1986.

"Legal Issues Raised by Transborder Data Flow", 295, 11 Can.-U.S. Law Journal, 1986.

Ros, N., "La Communanté Européene Planche Sur l' EDI, Expertises, No.130, p.287, 1990.

Rowbotham, G.:

"EDI: the practitioner's view", p32-33, International Financial Law Review, August 1988.

"What are the legal issues arising from the integration of EDI into the corporate treasury?", paper presented at `EDI and the Corporate Treasury' Conference, 26-27 February, 1990.

Rowe, H., "The UK `Computers (Compensation for Damage) Bill'", p.6-7, ACCL, Vol.7, No.8, September 1990.

Rumbelow, Clive., "Privacy and Transborder Data Flow in the UK and Europe", p153-157, International Business Lawyer April 1984.

Sanger, "Wire Static: Multinationals Worry as Countries Regulate Data Crossing Borders", Wall St.J., Aug 26, 1981.

Sarson, Richard., "EDI in the Dock", p118-127, Network, May 1989.

Sauvant, K.P., "Transborder data flows: importance, impact, policies", Information Services & Use, 4 (1984), pp3-30.

Savage and Edwards, "The Legislative Control of Data Processing -The British Approach", Computer/Law Journal, p143-56, Vol.VI, No.1, Summer 1985.

Savage, R., "How to resolve legal issues in EDI agreements: Acknowledgements and the Battle of Forms", pp.66-71, EDI Forum, No.1, 1991.

Scott, A., "Paperless trade: doing busines by computer", pp.6-12, Practical Law for Companies, Vo. II, No.7, August 1991.

Shalgren, K., "Role of UNCTC in TDF", Transnational Data Report V(7) Oct/Nov 1982, pp 325-327.

Schauss, M., "Issues of Contract Law", at p.69-96, in Poullet, Y. & G.P.V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law*, No.1 Computer/Law Series, Kluwer/The Netherlands 1988.

Scherer, Professor J., "European Telecommunications Law", pp.225-242, in Meijboom, A.P., and C. Prins (eds.), *The Law of Information Technology in Europe 1992*, No.9 Computer/Law Series, Kluwer, The Netherlands 1991.

Schlundt, Virginia., "Transborder data flow and its importance in the international arena", Information Age, vol.7 no.2 (April 1985): 67.

Schnurr, Lewis, "Conduit-Content Convergence: its causes and effects", in E.J. Mestmäcker (ed.), *The Law and Economics of Transborder Telecommunications*, Baden-Baden 1987, p.157-173.

Schulte-Braucks, Reinhard., "European Telecommunications Law in the light of the British Telecom Judgement", p39-59, Common Market Law Review, vol.23, No.1.

Schutte, H., "Investigating into the Legal Situation for introducing the Single Administrative Document and electronic data interchange", paper presented at Conference, The Hague, Holland, 3-4 May 1988.

Schwank, F. and W. Mitchell, "Data and the documentary credit", p33-35, International Financial Law Review, August 1988.

Seipel, P., "Paper laws in transition", pp.99-134, in Seipel, Prof. P. (ed.), *From Data Protection to Knowledge Machines*, No.5 Computer/Law Series, Kluwer/The Netherlands 1990.

Shain, M., "How secure is EDI", p.77-90, Proceedings of EDI and the Law Conference, November, 1990.

Sharpe, D.M.:

"EDI - The Legal Issues", paper presented at the `Gain the competitive edge with EDI' Conference, Sydney/Melborne, May, 1990.

"Are legal issues really a problem in EDI?", pp.481-490, Proceedings of the 3rd International Congress of EDI Users, Brussels, 4-6 September 1991.

Shaw, S.N.D., "Drafting an interchange agreement", pp.24-26, Proceedings of the EDI and the Law Conference, London, 4 July, 1991.

Sieber, U., "The Comprehension of Computer Crime by Substantive Law", pp.7-49, in *The Legal Aspects of Computer Crime and Security*, document prepared for the European Commission's Legal Advisory Board, December 1987.

Sieber, V., "The development of the law in the United States", p.139-151, Proceedings of `Copyright Protection of Computer Software' Conference, Hungary, 14-18 Oct., 1991.

Simitis, Spiros, "Reviewing Privacy in an Information Society", pp707-746, University of Pennsylvania Law Review, Vol.135.

Singleton, S.:

"Facilities Management - Part 1", pp.6-8, Applied Computer and Communications Law, Vol.9, No.4, April 1992.

"The EC Database Directive", pp.2-4, Applied Computer and Communications Law, Vol.9, No.5, May 1992.

Sizer, R., S. Chalton, and S.J. Gaskill, "Data Protection", p.16020/2, in Saxby, S., (General Editor)*The Encyclopedia of Information Technology Law*, Sweet & Maxwell, 1990.

Snyder, D.M., "Service level agreement in network services", p.93-101, in Proceedings of `Networks 91: Current Issues', Birmingham, June 1991.

Spero, Joan Edelman:

"Information: The Policy Void" p139-156 Foreign Policy 48 (Fall 1982).

"Barriers to International Information Flows: more than a war of words", p67-69, Telecommunications, November 1983, Vol.17, No.11.

Staubitz, Arthur F., "Antitrust considerations/implications and EDI: The broader perspective", paper in proceedings of EDI and the Law '91, Conference, Washington, February, 1991.

Stuurman, C., "Legal aspects of standardization and certification of information technology and telecommunications: an overview", paper presented at FIRLITE Conference: `Data Security in Computer Networks and Legal Problems', 23-24 September,1991, Hanover.

Stuurman, K., "Codes of Conduct", pp.102-113, in *The Legal Aspects of Computer Crime and Security*, document prepared for the European Commission's Legal Advisory Board, December 1987.

Takach, George, "EDI Trading Partner Agreements: A Canadian Perspective", pp.28-31, EDI Forum Special Edition, 1992.

Tallyen, J., "IRS record retention rules and the computer age", p.441, The Tax Adviser, July 1992.

Tapper, C., "Liability Issues", pp.95-102, in Proceedings of `Data Security & the Law' Conference, London, July 1991.

Tate, Lee, "EDI - a vision of the future", p.165, Proceedings of the 3rd International Congress of EDI Users, 4-6 Sept., 1991.

Tener, Ralph M., "Copyright Issues relating to the development and maintenance of EDI standards", paper in proceedings of EDI and the Law '91, Conference, Washington, February, 1991.

Thomas, D., "Employment Law", ACCL, Vol.7, No.3-5, 1991.

Thomsen Hans B., "Creation of Legal Security - UNCID explained", paper presented at COMPAT 88, Hague, Holland, 29 Feb.- 2 Mar. 1988.

Todd, P., "The effect on letters of credit of new documentation, and the introduction of electronic and paperless transactions", paper presented at IBC's International Letters of Credit Conference, London, 3rd July 1990.

Tombs, K., "Beyond reasonable doubt", p43-44, Image Processing, July/August 1990.

Torvund, Olav, "Paperless systems in international trade", p48-58, IRI's Spectrum, Dag Wiese Schartum (ed.), Tano, Oslo, 1989.

Toye, P., "Review of OSI standards", pp.88-107, in Gifkins, M., *EDI Technology*, Blenheim Online/London 1989.

Troye, A.:

"The European Dimension: Particular legal requirements to consider when trading throughout Europe", paper presented at EDI'90, London, Oct. 30-Nov. 1, 1990.

"European Issues", paper presented at EDI'90, London, Oct. 30-Nov. 1, 1990.

"From legal `formalism' to legal `functionalism'", paper presented at EDI'92, Birmingham, 6-8 October, 1992.

Tucker, G., "Trends in the protection of personal information", Proceedings of Privacy Laws & Business, 4th Annual Conference, Cambridge, 2-4 July, 1991.

Turn, "Privacy Protection and Security in Transnational Data Processing Systems", pp.67-74, 16 Stamford Journal of International Law, 1980.

Urbach, A., "The Electronic Presentation and Transfer of Shipping Documents", in Goode, R.M., *Electronic Banking: The Legal Implications*, The Institute of Bankers 1985 and Centre for Commercial Law Studies, Queen Mary College, University of London.

Wahlstrom, S., "International Data Transfers Experience", p55, Proceedings of the International Data Protection Commissioners Conference, Paris 1990.

Walden, I. and R.N. Savage, "The Legal Problems of Paperless Transactions", p102-112, The Journal of Business Law, March 1989.

Walden, I.:

"Why are companies shy of EDI?", p9-11, Management Europe, 29 August, 1988.

"How data protection complements and complicates EDI", pp.20-22, Privacy Law & Business, No.10, May 1989.

"Information Security and the Law", p. 179-238, in Caelli, W., D. Longley, and M. Shain, *Information Security Handbook*, Macmillan Stockton Press, 1991.

Waldron, M., "Applying a standard approach to document management", In-Form Systems Ltd, 1992.

Warman, Dr Adrian, `Organisational Computer Security Policies', Department of Information Systems, the London School of Economics and Political Science, 1991.

Wasik, M., "The role of the criminal law in the control of misuse of information technology", p.8, Working Paper No.8, University of Manchester, July, 1991.

Weiss, Peter N., "Electronic Data Interchange and the law of public contract formation: Will the Federal `Statute of Frauds' thwart the paperless contract', pp.17-25, Computer Law Reporter, Vol.12, No.1, Sept.1990.

Wheble, B.S.:

"International Trade Procedures", p20, The Computer Law and Security Report, vol.3, no.2, 1987.

"Think data, not documents", p.37, International Law Review, June 1988.

"Creating Legal Relationships with Trading Partners", p.126-138, The EDI Handbook (ed. M.Gifkin and D.Hitchcock), Online Publications, Middlesex, 1988.

"Should there be an electronic as well as a documentary credit", ICC's 12th Banking Conference, Paris, 23-26 October, 1989.

"UNCID Rules and interchange agreements", pp.62-64, Computer Law and Practice, Vol.6, No.2, Nov-Dec. 1989.

"EDI in International Trade", paper presented at `*EDI and the Law 90: Making Paperless Trade Legally Secure*', London, 14-15 November 1990.

"ECE WP.4 - EDI Legal Group Work Programme", paper presented at *EDIFORUM*, Pisa, Italy, 5 November 1991.

"Documentary credit requirements - towards a revised UCP", in Proceedings of the Conference *The Future of Bills of Lading*, 7-8 April 1992.

Whybrow, M., "The storm before the calm", pp.18-22, Banking Technology, October 1992.

Wiebe, Andreas, "EEC Law and Policy in Telecommunications", paper presented at `Data Security in Computer Networks and the Legal Problems' Conference, Hannover, 23-24 September, 1991.

Wigand, Rolf T., "Transborder data flow: its impact on business and government", p55-65, Information Management Review 1(2), Fall 1985.

Wigand, Rolf T., Carrie Shipley and Dwayne Shipley, "Transborder Data Flow, Informatics, and National Policies", Journal of Communications, Winter 1984, p153-175.

Wilkin, R.P., "The EC Directive on the Legal Protection of Computer Programs", p.2-4, Applied Computer and Communications Law, Vol.8, No.3, 1991.

Williams, D., "Taxing the international transfer of information", paper delivered to seminar at Brooklyn Law School, 5 December 1990.

Williams, M., "Something old, something new: the bill of lading in the days of EDI", pp.555-587, Transnational Law and Contemporary Problems, Vol.1, Fall 1991.

Wissels, C.M., "European Community Law", pp.10-11, in Meijboom, A.P., and C. Prins (eds.), *The Law of Information Technology in Europe 1992*, No.9 Computer/Law Series, Kluwer, The Netherlands 1991.

Whitaker, R.D., "EDI and Letters of Credit", pp.66-70, EDI Forum Special Edition, 1992.

Woods, A., "The Telecommunication Legal and Regulatory Environment", in the proceedings of the `Telecommunications Contracts' Conference, London, 3 December, 1991.

Wotherspoon, K., "Computer Misuse Act 1990", p.391, Lloyd's Maritime and Commercial Law Quarterly, 1991.

Wright, Benjamin,:

with R.A. Payne, "Rules for electronic conduct", The Journal of Commerce, 5 August, 1988.

"Electronic transactions require changes in laws", p31, Network World, August 7, 1989.

"Authenticating electronic contracts: the case for international recordkeeping", paper in proceedings of EDI and the Law '91, Conference, Washington, February, 1991.

"Auditing the electronic invoice", pp.51-52, Journal of State Taxation, Vol.9, Spring 1991.

"Contracts without paper", p.61, Technology Review, July 1992.

NEWSPAPER ARTICLES:

"When Privacy Laws Hurt Trade", p.104, Business Week, 14 April 1980.

"Waging a trade war over data", New York Times, March 13, 1983.

"Privacy proves expensive", p2, Computer Weekly, Nov.6, 1986.

"EDI in the international legal arena: a cacophony of voices", p.7, Data Channels, Vol.17, October 26, 1990.

"Defuse legal time bombs through trading agreements", p.7, Data Channels, Vol.17, Dec.10, 1990.

"Big split on data laws", C. Chace, The Guardian, January 8, 1991.

"Telecomms: when will Europe be connected?", p.24-26, Electronic Trader, Vol.1, No.3, January 1991.

"Users brand government security draft irrelevant", Computing, 10 October 1991.

DOCUMENTS:

American Bar Association:

`The Commercial Use of Electronic Data Interchange', prepared by the Electronic Messaging Services Task Force, p.1645; `Model Trading Partner Agreement and Commentary', p.1719, 45 Business Lawyer, No.5, June 1990.

`Security Techniques in Electronic Transactions' (Draft), proposed ABA policy.

Australian Law Reform Commission, Privacy, Report No.22, Vol.1: Background, Australian Government Publishing Service, Canberra 1983...also Vol.2, p198.

Business International Report, *Transborder Data Flow: Issues, Barriers and Corporate Responses*(New York: BI, 1983)

Congress of the United States, Office of Technology Assessment, *Computer Software & Intellectual Property: Background Paper*, Macmillan Stockton Press, 1990.

Council of Europe:

Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, Council of Europe, 1981. (European Treaty Series No 108).

Recommendation No.R(81) 20 to Member States "on the harmonisation of laws relating to the requirement of proof and to the admissibility of reproduction of documents and recordings on computers" ISBN 92-871-0044-6.

`Computer-related crime', Report by the European Committee on Crime Problems, Strasbourg 1990.

Data Protection Act: Advertising and Tracking Study (RS 2060), Oct.1986, Office of the Data Protection Registrar.

Department of Trade and Industry:

`Vanguard EDI and X.400 study', HMSO, 1988.

`Dealing with computer misuse', 1992.

European Convention on Human Rights 1950 Cmd.8969.

European Economic Community:

EEC Treaty 1957, Cmnd 5179-11, 1972.

The General Programme, 5 J.O.Comm.Eur.32, 1962.

Commission Communication, Working Plan for Creating a Community Information Market, COM(85) 658 final, of Nov. 29, 1985

Commission White Paper: `Completing the Internal Market', COM (85) 310.

"The Legal Aspects of Computer Crime and Security: A comparative analysis with suggestions for future international action", document prepared for the European Commission's Legal Advisory Board, December 1987.

Green Paper on the development of the common market for telecommunications services and equipment, COM(87) 290 final.

Commission, `On the Way to a Competitive Community-Wide Telecommunications Market in the Year 1992', COM (88) 48 final of Feb.9, 1988.

Commission Directive of May 16, 1988 on Competition in the Market of Telecommunications Terminal Equipment (88/301/EEC), OJ L 131/73 of May 27, 1988.

Commission Directive of June 28, 1990 on Competition in the Market of Telecommunications Services (90/388/EEC), OJ L 192/10 of July 24, 1990.

EDI in perspective, EUR 11883 en (1989).

"The Legal Position of the Member States with respect to Electronic Data Interchange", TEDIS final report, September 1989.

"Analysis of the market for Value Added Services in Europe", Scicon Networks, TEDIS final report, December 1989.

"Survey of EDI in all the Member States 1989", Tedis report, XIII/D/5/6-90.

Council Directive of June 28, 1990, on the Establishment of the Internal Market for Telecommunication Services through the Implementation of Open Network Provision (ONP) (90/387/EEC), OJ L 192/1 of July 24, 1990.

Proposal for a Council Resolution in the Field of Information Security, OJ C 277/18 of Nov.5, 1990.

Commission Communication, `On the Way to European-wide Systems and Services - Green Paper on a Common Approach in the Field of Satellite Communications in the European Community', COM(90) 490 final of Nov.28, 1990.

`A proposal concerning the use of Digital Signatures in EDIFACT': A report prepared by Cryptomathica/s, 29 November, 1990.

Commission Directive on the Introduction of an Open Network Provision for Leased Lines, COM(91) 30 final of Feb.14, 1991, OJ 58/10 of Mar.7, 1991.

Council Directive of May 14, 1991, on the legal protection of computer programs, O.J. 1991 L 91/250.

`Information Technology Security Evaluation Criteria: Provisional Harmonised Criteria', June 1991.

"The Liability of Electronic Data Interchange Network Operators", Tedis final report, July 1991.

"La formation des contrats par echange de donnees informatisees", Tedis final report, July 1991.

"The Legal Position of the EFTA Member States with respect to Electronic Data Interchange", July 1991.

"Trusted Third Parties and similar services", TEDIS final report, November 1991.

"A Service Infrastructure for EDI Security", TEDIS final report, December 1991.

"Secure EDI - a management overview", EUR 13794 en.

Institute of Chartered Secretaries & Administrators, "A Short Guide to the Retention of Documents", 1991.

Intergovernmental Bureau for Informatics:

Declaration of Mexico on Informatics, Development and Peace, June 23, 1981.

"IBI World Survey of National Policies and Company Practices Concerning Transborder Data Flows", TDF 110, Rome, IBI, 1983.

"Proceedings of the Second World Conference on Transborder Data Flow Policies", Rome, 26-29 June 1984, TDF 260.

International Consultative Commission for TDF Development, "Inaugural Meeting Proceedings", 18-20 September, Rome, 1985, TDF 270.

International Chamber of Commerce:

"Information Flows - Analysis of Issues for Business", Doc.No. 373/23 Rev.3, Paris 1983.

"Computer Related Crime and Criminal Law: An International Business View", Position Paper No.11, Doc. No. 373/76 Rev., Paris, 1988.

"Communications Network Security: an International Business View", Position Paper No.13, Doc.No. 373/103 Rev., July 1990.

INCOTERMS 1990, No.460.

"Protection of Personal Data: An International Business View", Doc. No.373/124, 1 August, 1991.

"Toward greater competition in telecommunications: Basic services and network infrastructure", Position Paper No.17, December 1991.

International Covenant on Civil and Political Rights, G.A.Res.2200, 21 UN GAOR Supp. (No.16) 52, UN Doc. A/6316 (1966)

International Telecommunications Convention, Malaga-Torremolinos, October 25, 1973 [28 UST 2510, TIAS No.8572].

Law Commission:

Report No.110, `Breach of Confidence', Cmnd.8388, 1981.

Working Paper No.110, `Computer Misuse', HMSO, 1988.

`Computer Misuse' Report No. 186, Cm.819, London: HMSO, 1989.

`Rights of Suit in Respect of Carriage of Goods by Sea', No.196, Scot. Law Com. No.130, HMSO, London 1991.

Consultation Paper No.121, `Privity of Contract: Contracts for the Benefit of Third Parties'.

OECD:

Transborder Data Flows and the Protection of Privacy: Proceedings of a Symposium held in Vienna, Austria 20-23 September 1977. Paris OECD 1979 (Information, Computers and Communications Policy Series, No.1)

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, 1981 (Annex to the Recommendation of the Council of September 23, 1980).

`Transborder Data Flows in International Enterprises', Document DSTI/ICCP/83.23.

`Computer-related crime: Analysis of legal policy', OECD, Paris 1986.

UK Government:

Data Protection Committee Report, Cmd.No.7341 (1978).

`Banking Services: Law and Practice', Report by the Review Committee (Chair: Professor R.B. Jack), Cm 622, February 1989.

"Competition and Choice: Telecommunications Policy for the 1990's", November 1990.

White Paper, "Competition and Choice: Telecommunications Policy for the 1990s", Cmnd 1461, HMSO 1991.

Universal Declaration of Human Rights, G.A.Res.217, UN Doc. A/810 (1948)

UN Convention for the International Sale of Goods, 11 April 1980, Annex I, U.N. Doc.A/Conf. 97/18, [1980].

UNCITRAL:

`Legal Value of Computer Records', A/CN.9/265, 21 February 1985.

`The Legal Implications of Automatic Data Processing', A/CN.9/279, 11 July 1986.

`Electronic data interchange: Preliminary study of legal issues related to the formation of contracts by electronic means', A/CN.9/333, 18 May. 1990.

`Electronic Data Interchange', A/CN.9/350, 15 May 1991.

`Comments on the Draft Model Law on International Credit Transfers - Report of the Secretary-General', 15 May 1991, A/CN.9/346.

UNECE:

`An Overview of Legal Problems of Trade Facilitation', TRADE/WP.4/GE.2/R.102, 10 November 1977.

`Draft Recommendations on Signatures/Authentication in Trade Documents', TRADE/WP.4/GE.2/R.111/REV.1

`Legal Aspects of Automatic Trade Data Interchange', TRADE/WP.4/R.185/Rev.1, 21 October 1982.

`Transborder Data Flows', TRADE/WP.4/R.200.

`Transborder Data Flows', TRADE/WP.4/R.246.

`Proposal for Uniform Rules for Communication Agreements (UNCA)', TRADE/WP.4/R.300, 18 January 1985.

`Use of computer-readable data as evidence in Court proceedings', TRADE/WP.4/R.330, 25 February 1985.

`Proposal for the Inclusion in the Trade Data Elements Directory (UNTDED) of Data Elements Signifying "Legal Acceptance", TRADE/WP.4/R.399.

`Trade Data Interchange Protocols', TRADE/WP.4/R.609

Introduction to UN/EDIFACT, TRADE/WP.4/INF.105, 12 July 1988.

`National legal requirements concerning electronic transmission of trade data', TRADE/WP.4/R.629, 3 January, 1990.

`Electronic Data Interchange in Foreign Trade: German law requirements concerning written form and siganture', TRADE/WP.4/R.709, 14 August, 1990.

`Electronic Bill of Lading', Transmitted by NCITD, TRADE/WP.4/R.710, 15 August 1990.

UNESCO:

Commission on Transnational Corporations, "The role of transnational corporations in transborder data flows", E/C.10/1986/16, 12 February 1986.

Human Rights and Technological Developments, E/CN.4/1990/72, 20 February, 1990.

US, "International Information Flow: Forging a new framework", p13, 32nd Report by the Committee on Government Operations, No.96-1535.

US, "Report on the potential legal issues arising from the implementation of CALS by the DoD", Prepared by the US Legal Issues Committee of the Acquisition Task Group, CALS/CE Industry Steering Group, 10 November 1991.

US Comptroller General Decision: `Use of Electronic Data Interchange Technology to Create Valid Obligations'; B-245714, December 13, 1991.

US Legal Issues Committee of the Acquisition Task Group, CALS/CE Industry Steering Group, "Report on the potential legal issues arising from the implementation of CALS by the DoD", Prepared by the 10 November 1991.

Quarterly Survey of Small Business in Britain, p9, Small Business Research trust, 1985, Vol.1, No.3.

"Sweden and Transborder Data Flows", Ministry of Public Administration, Ds C 1985:19.

Appendix A:

TDF and Data Protection Regulation: Company Survey

1. United Kingdom

Bank of America
Barclays
EMI Music
CCN Systems
Grace
IBM
ICI
Linklaters & Paine
3.M.
NDL International Ltd
Reader's Digest
Shell
Standard Chartered Bank
Texaco
Visa International

2. Germany

Bundes-Schufa
Deutsche Lufthansa AG
Hoechst Aktiengesellschaft
Volkswagenwerk AG
Siemans AG

3. Sweden

EMI Svenska AB
Molnlycke AB
IBM Sweden
Federation of Swedish Industry
KPMG Peat Marwick
Sparn muden
Philips Norden
AGA AB
Astra AB

Western Europe Survey
on Data Protection, Transborder Data Flows and Data Subject Rights

This survey is addressed to manufacturing and service companies operating internationally. The results will contribute to a better understanding of company practices, needs and problems with regards to meeting the requirements of different national data protection regulation; transborder communication (both technical and personal data) and upholding data subject rights. Your cooperation in completing this questionnaire will be appreciated.

Due to the limited nature of such questionnaires in meeting the particular characteristics of any one company, I would like to use this questionnaire as a base level of information. I would, therefore, be grateful if when I collect the survey, I was able carry out an interview in order to gain a more complete picture of current attitudes and practices in your company, removed from the constraints of the questions. The interview will be free-format, to allow as much ground to be covered as possible.

All responses will be dealt with in the strictest of confidence.

COMPANY DESCRIPTION

Name:_____

Name and Title of Respondent: _____

_____

1. Is the company national or multinational in terms of:

		Yes	No	N/A
a)	having company-owned operations located only in one country			
b)	being a parent company controlling, or having a majority shareholding in foreign subsidiaries			
c)	being a subsidiary of a foreign company			

2. What are the company's principal activities (check as appropriate):

a) Consumer goods ___
b) Computers, Telecoms and Networks ___
c) Chemicals and Pharmaceuticals ___
d) Industrial ___
e) Retail and Wholesaling ___
f) Banking and Finance ___
g) Other Services ___

3. Where does your company operate computer communications:
(Check as appropriate)

a)	Western Europe	e)	Eastern Europe
b)	EEC only	f)	Latin America
c)	North America	g)	Africa
d)	Asia, Australasia and Japan	h)	Worldwide

I PRIVACY AND DATA PROTECTION: Subject Access.

4. Since several countries have passed data protection legislation, has your company reorganized any of the following activities:

		Yes	No	N\A
a)	data collection			
b)	data processing			
c)	data transmission			
d)	storage procedures			

If not, are there plans to reorganise?

_____

5. Did your company make organizational changes in order to deal with the new rights of `data subjects' created in national data protection legislation, if so how?

_____

_____

_____

6. With regard to data subject access, does your company do any of the following:

		Yes	No	N/A
a)	provide free of charge access to employees			
b)	charge for access, and if so is it fixed by the government, or by the company			
c)	have a centralized enquiry point			
d)	provide standard application forms			
e)	include all manual records, even if legislation does not cover such records			
f)	automatically provide records to all data subjects held, e.g. once a year			
g)	release records in response to a specific request			

h) inform subjects when data on them is passed on to a third party

i) seek their consent when data on them is passed on to a third party

If necessary, any further details_____

_____

_____

7. What level of subject access has your company already experienced across Europe in the last year?

Country	no. of records relating to individuals	no. of access requests

8. Does your company have its own privacy or data protection code, or is it planning to have one?

_____

_____

9. Who in the company is responsible for overseeing data protection compliance, in your country or Europe-wide? (Please write in name, job title, addresss and phone no.)

_____

_____

II INTERNATIONAL COMMUNICATIONS IN COMPANY OPERATIONS: Transborder data flows (TDF).

10. Is the company presently using international computer communication (in any medium) in your location?

a) yes ___, please go to question 11

b) no ___, if not, is this planned for the future?

1988-89 ___
1990-91 ___
1992-93 ___
never ___

1990-91
1992-93

11. From your location, how much data is transferred to another country? Please reply for the five countries to which you most frequently transfer computer data (in descending order):

Country	for processing vol.(Mb) per month	for storage vol.(Mb) per month

12. For which activities does your company use international data flows?

		Direction of TDF	
		outgoing	incoming
a)	marketing and sales	___	___
b)	customer orders and billing	___	___
c)	product distribution	___	___
d)	production coordination and planning	___	___
e)	inventory management	___	___
f)	research and development	___	___
g)	financial management	___	___
h)	personnel management	___	___
i)	other (please specify)	___	___

_____

III ROLE OF TRANSBORDER DATA FLOWS IN THE COMPANY

13. How important are international data flows to your company operations:

a) essential ___
b) very important ___
c) useful, but not essential ___
d) not important ___

14. Has the use of international computer communications changed your company's management structure:

a) greater centralization of planning and decision-making ___
b) more decentralization of planning and decision-making ___
c) no effect ___

Please explain_____

_____

15. Has transborder computer communications opened new business opportunities for your company?

Please explain_____

_____

IV POLICIES RELATING TO TRANSBORDER DATA FLOWS

16. In the country, where you are located, have you experienced or do you expect government regulatory policies relating to TDF, in terms of:

a) reporting or disclosure to government authorities of certain types of information to be exported, such as concern (please explain):

i] individuals (e.g. personnel records)_____

_____

ii] company activities (e.g. investments)_____

_____

_____

iii] national economy (e.g. currency flows)_____

_____

_____

iv] national resources (e.g. energy resources)_____

_____

_____

v] national security (e.g. military projects)_____

_____

_____

In the country, where you are located, have you experienced or do you expect government regulatory policies relating to TDF, in terms of:

b) prohibiting the export of certain types of information concerning:

i] individuals_____

_____

ii] company activities_____

_____

iii] national economy_____

_____

iv] national resources_____

_____

v] national security_____

_____

In the country, where you are located, have you experienced or do you expect government regulatory policies relating to TDF, in terms of:

c) payment of custom duties, value-added taxes or other forms of taxation on information or data processing services or value added networks

_____

_____

17. Have you experienced, or do you expect, any such regulatory policies in any other country where your company operates? If so please explain:

_____

_____

_____

18. Does your company have policies on the export from this country, by telecommunications or storage media (e.g. discs/tapes), of information concerning:

		Yes	No
a)	personal data on individuals		
b)	legal persons, such as companies and trade unions		
c)	the national economy, industries and natural resources		

19. If so, do the policies mentioned in questions 16 and 17 above (as appropriate) involve maintenance in your country of copies of certain types of exported data

If so, please briefly explain the policy_____

_____

_____

20. Do the above company policies apply in other countries? If so please explain:

_____

_____

_____

V INTERNATIONAL COMMUNICATION RESTRICTIONS

21. Which of the following telecommunication services are used by your company for international transfers of data:

		Yes	No	N/A
a)	dial-up data network			
b)	leased circuits			
c)	cellular telephone			
d)	others (please write in)_____			

_____

22. Has your company been faced with any of the following policies on the transfer of data between countries? If so, could you please describe the problem in simple terms, and describe how your company has adapted?

a) Network controls, such as restrictions on the availability of private leased lines

_____

_____

b) Telecommunications rates favouring home country data processors

_____

_____

c) Volume sensitive charging_____

_____

_____

d) Taxes or tariffs charged on information content (e.g. value of software)

_____

_____

_____

e) Restrictions on the flow of non-personal data_____

_____

_____

f) Technical standards imposed on computer and data telecommunications hardware

_____

_____

_____

g) Restrictions on use of public networks_____

_____

_____

h) Monopoly on purchase of modems or other telecoms hardware

_____

_____

_____

VI DATA SECURITY

23. In general terms, what types of security procedures does your company have concerning the protection of the following types of data (both for data used at home and that transferred abroad):

a) personnel management_____

_____

b) customer orders and billing_____

_____

c) production coordination and planning_____

_____

d) inventory management_____

_____

e) product distribution_____

_____

f) financial management_____

_____

g) research and development_____

_____

h) marketing & sales_____

_____

i) suppliers_____

_____

24. Have the company's security procedures changed in response to national data protection legislation. If so how?

_____

_____

25. Have you yet extended these new procedures to countries which have not yet passed data protection laws?_____

_____

26. How would you like to see data protection <u>legislation</u> cover data security issues?

_____

_____

_____

27. How would you like to see data protection <u>authorities</u> cover data security issues (e.g. regulations/recommendations)?

_____

_____

_____

28. Have security measures been affected by policies and regulations of national telecommunication authorities (e.g. ban on encryption)

_____

_____

_____

29. How important a role do you see data security issues playing in your company's use of information technology, now, and over the next five years? Please explain_____

_____

_____

Thank you for your time.

Any questions concerning the questionnaire, please contact Ian Walden, Legal Studies Department, Trent Polytechnic, Nottingham, United Kingdom. Tel: (+44.602) 418248.

Company	Data storage & transmis. changed	Nature of TDFs to business	Impact of TDFs: centralise	Impact of TDFs: decentral.	New business opp.	Expect/experience regulation of TDFs	Extend DP policy to non-DP countries	Means of communication	Impact on data security policies
Reader's Digest	processing: accuracy / storage: retention	very important	no impact	no impact	mailing lists	no - dormant issue	parent company guidelines	dial-up leased lines	yes - for PCs and data disposal
CCN Systems	collection / processing	very important	no impact	no impact	no	Australia: tax on sale of data	no	-	physical access procedures
International Business Machines (IBM)	transmis. / storage	essential	-	planning & decision-making	on supply side: eg. customer service	no	worldwide guidelines	dial-up leased lines	greater education & awareness
Linklaters & Paine	no	useful, but not essential	planning & decision-making	-	-	no	no	dial-up	no
EMI Music	storage	essential	financial control	planning & decision-making	not yet	PTT equipment: eg. Spain, Portugal	corporate policy manual: principles	dial-up VAN Email	no
Standard Chartered	no	essential	-	federal structure	probably	no - dormant issue	global code to be developed	dial-up leased lines	global security code

NDL International Ltd.	all activities	essential	information & co-ordination	planning & decision-making	access to US	no	yes	dial-up leased lines	–
Barclays	no	very important	no impact	no impact	no - new bus. opps. needed TDFs	Singapore & South Korea ban encryption	no	dial-up leased lines	no, but useful lever
3M (UK)	no	essential	no impact	no impact	improved customer service	no - dormant issue	no	dial-up leased lines	no
W R Grace	no	essential	planning, decision-making & standards	–	integrated customer / supplier relations	* availability * expect in non-EEC: eg. Far East	code of practice	dial-up leased lines	yes - control software
Shell International Petroleum	no	essential	no impact	no impact	–	no	code of practice	dial-up leased lines Email mag. tape	–
Dun & Bradstreet	no	very important	no impact	no impact	yes - international sale of data	Germany - equipment & availability	yes	dial-up leased lines	yes - more money for more controls
Bank of America	no	essential	planning & decision-making	–	improved customer service	Ireland, Germany, Belgium	worldwide Privacy Compliance program	dial-up leased lines	no

Texaco Ltd.	no	essential	no impact	no impact	no	availability is slow - dormant issue	employee handbook	leased lines VAN	no
Visa International	no	essential	no impact	no impact	no	expect in EEC	normal confidential	IPSS dial-up leased lines	no

Appendix B:

EDI and the Law: Questionnaire Respondents

Aeroquip Ltd.
British Airways
British Steel
Cable & Wireless Plc
Coats Viyella Plc
Conoco (UK) Ltd
Courtaulds
Digital Equipment Corporation
Dixonx Stores Group
Du Pont de Nemours (International)
D.S.M.
Eagle Star Insurance Co. Ltd.
Elida Gibbs
Evergreen International (UK) Ltd
Glaverbel
Goodyear Ltd
Hazlewood Foods Plc
Hewlett Packard
Hoover Plc
Icelandic Air
ICL
Intesa s.p.a.
Kesko Oy
Lucas Industries Plc
Maersk Line
Mercedes-Benz AG.
Michelin Tyres Plc
Motorola Gmbh
Neddata
Nokia Data
Philips Industries
P & O Containers
Rabobank Nederland
Rank Xerox Ltd
Rowntree Mackintosh Confectionery Ltd
Scott Ltd.
Sealink British Ferries Ltd.
Shell Nederland Chemie B.V.
STC Telecoms
Swift Service Partners
Tallent Engineering Ltd
Texas Instruments Ltd

Electronic Data Interchange

- The Legal Issues -

Survey Questionnaire

This survey is addressed to organisations making use of electronic data interchange (EDI) in their day-to-day business operations. This 'short' questionnaire is designed to reveal the range and types of legal issues that such organisations may have had to confront when adopting EDI.

It is intended to use the results as a base of knowledge and experience to contribute to a book: EDI and the Law. The book, to be published by October/November 1989, is to be the second in a series of works in the field of EDI and paperless trade, following on from the introductory EDI Handbook, published by Blenheim Online Publications.

The aim of the book is to provide a practical legal guide for organisations embarking on, or engaged in, the use of electronic data interchange, including their legal counsel. Therefore, the information gained from the survey will be used to focus the attention of the book on practical issues experienced by organisations.

Your co-operation in completing this questionnaire will be greatly appreciated. If you are not able to complete the questionnaire, would you be so kind as to pass it on to the relevant individual or department.

All responses will be dealt with in the strictest of confidence.

COMPANY DESCRIPTION

Name of Company:

Name and Title of Respondent:
(please include address and telephone number)

1. What are the company's principal activities (check as appropriate):

(a)	Consumer goods	☐
(b)	Computers, Telecoms and Networks	☐
(c)	Chemicals and Pharmaceuticals	☐
(d)	Motor industry	☐
(e)	Retail and Wholesaling	☐
(f)	Banking and Financial services	☐
(g)	Distribution and Transportation	☐
(h)	Construction	☐
(i)	Engineering	☐
(j)	Other Manufacturing/Service	☐

Please explain

---

2. Is your company using electronic data interchange (EDI) systems to communicate business documents:

		Yes	No	N/A
(a)	for intra-company communication	☐	☐	☐
(b)	to suppliers	☐	☐	☐
(c)	to customers	☐	☐	☐
(d)	to government authorities (eg Customs authorities)	☐	☐	☐

3. Please list the EDI communities you are involved with (eg Odette, Cefic, Ana, Dish, Edicon)

_____

4. As a member of an EDI community (as indicated above), were you involved in discussions concerning legal issues?

_____

_____

_____

Did the discussions result in a set of industry guidelines?
(Would it be possible to obtain a copy?)

_____

5. What has prevented your organisation from implementing EDI, or 'slowed down' implementation (please rank in order, 1-10 where 10 is most important)?

(a)	practical barriers (eg lack of software)	☐
(b)	administrative barriers	☐
(c)	running costs	☐
(d)	set-up costs (Internal/External)	☐
(e)	lack of standardisation (eg messages)	☐
(f)	need for paper backup	☐
(g)	legal barriers	☐
(h)	staff problems (eg skill/training)	☐
(i)	lack of user group (eg within sector)	☐
(j)	lack of user-oriented services	☐
(k)	security and confidentiality (of electronic transfers)	☐

Please list any other reasons

_____

_____

THE LEGAL ISSUES

6. **Do you have contractual arrangements that exist for the use of EDI in your organisation?**

Yes ☐ **No** ☐

If 'Yes', what type of clauses feature in the contract: (eg communication standards/ procedures)

Would it be possible to obtain a blank copy?

If 'Yes', would you answer Q.6(a), if 'No', please go on to Q.7.

(a) What reference is made to standard terms and conditions under which the company normally operates, in the EDI contracts?

7. **What security arrangements are adhered to, in order to protect EDI communications from negligence, fraud and/or unauthorized access (eg paper back-up, encryption)?**

(a) externally

(b) in-house (physical and electronic),

What arrangements have been made to safeguard against system failure (ie contingency planning for disasters)?

8. Under what arrangements would liability be allocated in the event of:

(a) communication failure;

(b) mistake;

(c) fraud;

(d) unauthorised access?

9. What arrangements are made to ensure that any action taken through an EDI system can be made legally enforceable, and would stand up in court (eg 'electronic signatures', record-keeping and audit requirements)?

10. What in-house administrative arrangements/governmental regulatory requirements, related to an EDI transaction, have to be conducted by your company by methods other than by EDI (eg informing the accounts dept., Customs certificates, bills of lading, letters of credit, escrow agreements)?

11. What arrangements have been agreed upon for the resolution of disputes that may arise through the use of EDI (eg arbitration)?

12. **Please make any additional points that you think may be applicable to the issues dealt with in this survey, or in connection with the book: EDI and the Law.**

Thank you for your time.

To obtain further information concerning the EDI questionnaire, please contact Ian Walden, Editor: EDI and the Law, Legal Studies Department, Trent Polytechnic, Nottingham. Telephone: (+44 602) 418248, Telex 377534 Polnot G, Fax (0602) 484266.

Appendix B3: EDI and the Law Respondents

Company	Barriers	Security	Liability	Evidential	Dispute Resolution	Contracts
Courtaulds	-	(1) paper back-up (2) VAN security	VAN liable for hacking	audit records	-	yes
Michelin Tyres Plc	legal standards admin.	paper back-up	-	audit records	arbitration	network only
Tallent Engineering Ltd.	admin.	(1) exception reports generated (2) call-back	-	audit	-	network only
Conoco (UK) Ltd	standards user group paper	-	-	audit	-	network only
SWIFT Service Partners	admin. costs standards	encryption	after reaches regional processor	contract	court	yes
Dupont de Nemours	standards cost	(1) one-way access (2) paper back-up	contract	contract	-	yes
Goodyear	-	-	-	-	-	yes - not finalised
Elida Gibbs	standards	VAN security	-	-	-	network only
Shell Nederland Chemie	costs standards legal	(1) paper back-up (law) (2) VAN security	VAN liable for failure, hacking & fraud	-	-	no
Rabobank Nederland	costs legal	encryption	contract	contract	court	yes
Neddata	costs staff	authenticate - encryption	controller of failed link	records kept by VAN	arbitration	no
Kesko Oy	admin. practical	specified contact person	-	(1) log of all incoming mesages (2) microfilm	-	no
DSM	staff user group	paper back-up	good business practice!	-	-	no
Mercedes-Benz AG	-	paper back-up	-	written summary bills	-	only if requested
Cable & Wireless	admin. standards	encryption	contract	contract audit	-	yes
Coats Viyella Plc	-	paper/mag. tape back-up	-	-	-	network only
P&O Containers	legal	paper back-up	message sender	-	-	-
STC Telecoms	costs standards paper back-up	VAN security	-	-	gentlemans agreement	in the commercial agreement

Appendix B3: EDI and the Law Respondents

ICL	legal admin. paper back-up	-	-	paper audit trail	arbitration	yes
DEC	security confidentiality	encryption	transaction owner	(1) contract (2) audit/log (3) defined person	mediation	yes
British Airways	all, but legal!	VAN back-up	under negotiation	microfilm copy	-	no
Hoover Plc	admin. practical	-	-	-	-	no
Evergreen International (UK) Ltd	standards user group legal	VAN special clause	(1) network provider (2) sender	-	arbritation	no
Lucas Industries	-	paper back-up	commercial agreement	contract	courts	yes - EDIA
Rowntree Mackintosh	admin. security	-	-	paper confirmation	-	network only
Hazlewood foods	costs admin.	VAN security audit	message sender	-	-	no
Rank Xerox	standards user group	paper back-up	-	-	-	in development
Texas Instruments	availability of resources	VAN security	message sender	audit records	arbitration	no
Eagle Star Insurance Co.	practical costs	VAN security	-	-	-	in development
Scott Ltd.	standards practical	(1) VAN (2) paper back-up until received	not assigned	audit trails	-	no
Sealink British Ferries	standards practical	-	accept message - bound to pay			in development
Dixons Stores Group	costs practical	paper/mag. tape back-up	-	-	arbitration	no
Aeroquip Ltd.	standards legal	paper back-up	-	audit	-	yes
Philips Industries	admin. practical	-	message sender	VAN archive	-	no
British Steel	-	-	-	-	-	network only
Nokia Data	practical staff	(1) VAN (2) paper back-up	-	-	-	yes
J Whitaker & Sons Ltd.	-	-	as normal, what is special about EDI?	-	-	yes
Motorola Gmbh	staff standards	-	failure & fraud - neither party	audit	-	yes
Maersk Line	costs paper back-up	external audit	-	-	-	in development

Appendix C:

Interchange Agreements

Cabinet Alain Bensoussan: Contrat D'Interchange
American Bar Association Model Trading Partner Agreement
American Bar Association Model Electronic Payments Agreement (draft)
Barclays: EDI Trading Master Interchange Agreement
British Aerospace
CAD/CAM Data Exchange Technical Centre: The Exchange Agreement
CMI Rules for Electronic Bills of Lading
Conference of European Post and Telecommunications administrations (CEPT): Eaxmple d'unde `Convention' (France)
Le Centre International de Recherches et d'Etudes du Droit de l'Informatique et des Télécommunications (CIREDIT): Contrat-type d'interchange EDI (France)
Customs Co-operation Council: Guidelines concerning Customs-Trader Data Interchange Agreements
DIN: EDI Agreement (German)
DISH Pilot Project Interchange Agreement
Eastman Kodak Company Agreement: Electronic Data Interchange (US)
The EDI Association Standard Interchange Agreement (2nd Edition)
EDI Council of Australia: Model EDI Trading Agreement
EDI Council of Canada: Electronic Data Interchange Agreement
European Commission, Tedis Programme: European Model EDI Agreement - final draft
FINPRO: Model Agreement on Transfer of Data in International Trade (agreed upon by the Republic of Finland and CMEA Member States 1991)
The First National Bank of Chicago: Agreement for settlement of interbank electronic payment instructions
Hewlett Packard: Electronic Data Interchange (EDI) Exhibit
ICL: Electronic Data Interchange Agreement
IBM: Electronic Data Interchange Agreement
National Health Service Interchange Agreement - draft
National Westminister Bank Terms and Conditions for Bankline Interchange
New Zealand Customs Department (CEDI): Interchange Agreement
New Zealand EDI Association Standard EDI Agreement
Nixdorf Computer AG (German)
Odette: The Guidelines for Interchange Agreements, prepared by the Organisation for Data Exchange Through Teletransmission in Europe, 1990.
Quebec: The Standard Interchange Agreement prepared by the Ministry of Communications of the Province of Quebec, 1990.
RINET General Terms and Conditions
SITPROSA (South African) Interchange Agreement
Southern Pacific Transportation Company (US)
Texas Instruments: Electronic Purchase Agreement (US)
UN/ECE Proposal for Uniform Rules for Communication Agreements (UNCA)

EDI ASSOCIATION STANDARD ELECTRONIC DATA INTERCHANGE AGREEMENT

THE EDI EDIA ASSOCIATION

The Terms of this Agreement shall govern the conduct and methods of operation between the Parties in relation to the interchange of data by teletransmission for the purposes of or associated with the supply of goods and/or services. They take account of the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission as adopted by the International Chamber of Commerce.

PARTIES:

1. Signature .....
   Name .....
   Position .....
   On behalf of .....
   .....
   Address .....
   .....
   .....
   Date .....

2. Signature .....
   Name .....
   Position .....
   On behalf of .....
   .....
   Address .....
   .....
   .....
   Date .....

3. Signature .....
   Name .....
   Position .....
   On behalf of .....
   .....
   Address .....
   .....
   .....
   Date .....

4. Signature .....
   Name .....
   Position .....
   On behalf of .....
   .....
   Address .....
   .....
   .....
   Date .....

2nd Edition August 1990

EDI ASSOCIATION
TERMS OF THE STANDARD ELECTRONIC DATA INTERCHANGE AGREEMENT

2nd Edition August 1990

1. Definitions

"Adopted Protocol" :
the accepted method for the interchange of Messages based on the EDIFACT standard for the presentation and structuring of the transmission of Messages, or such other protocol as may be agreed in writing by the parties.

"Message" :
data structured in accordance with the Adopted Protocol and transmitted electronically between the parties, including where the context admits any part of such data.

"Data Log" :
the complete record of data interchanged representing the Messages between the parties.

"User Manual" :
the handbook of commercial and technical procedures and rules and legal requirements applicable to the transmission of Messages using the Adopted Protocol.

2. Scope

2.1 This agreement shall apply to all Messages between the parties using the Adopted Protocol and the parties agree that all such Messages shall be transmitted in accordance with the provisions of the User Manual.

2.2 Notwithstanding the existence of a User Manual the parties may agree terms to reflect additional or different requirements which they may have for the interchange of Messages, which terms shall be included in an Appendix which shall form part of this Agreement.

3. Security of Data

3.1 Each of the parties shall:

3.1.1 take all such appropriate steps and establish and maintain such procedures so as to ensure that as far as reasonably practicable Messages are properly stored, are not accessible to unauthorised persons, are not altered, lost or destroyed, and are capable of being retrieved only by properly authorised persons.

3.1.2 ensure that any Message containing confidential information as designated by the sender of the Message is maintained by the recipient in confidence and is not disclosed to any unauthorised person or used by the recipient other than for the purposes of the business transaction to which it relates. Messages shall not be regarded as containing confidential information to the extent that such information is in the public domain, or the recipient is already in receipt of it or receives the information from a thirty party entitled to disclose it. Any authorised disclosure to another person shall be on the same terms as to confidentiality as contained in this clause.

3.2 Where permitted by law, the parties may apply special protection to Messages by encryption or by other agreed means including those set out in the User Manual. Unless the parties otherwise agree, the recipient of a Message so protected shall use at least the same level of protection for any further transmission of the Message.

4. Authenticity of Messages

4.1 All Messages must identify the sender and recipient(s) and must include a means of verifying the authenticity of the Message either through a technique used in the Message itself or by some other means provided for in the Adopted Protocol.

4.2 Parties may by agreement also use higher levels of authentication to verify the Message.

5. Integrity of Messages

5.1 Each party being a sender shall ensure that all Messages are complete, accurate and secure against being altered in the course of transmission by him and, subject to clauses 5.2 and 5.4, shall be liable to any other person for the direct consequences of any failure to perform his obligations under this clause.

5.2 Each party accepts the integrity of all Messages and agrees to accord these the same status as would be applicable to a document or to information sent other than by electronic means, unless such Messages can be shown to have been corrupted as a result of technical failure on the part of machine, system or transmission line.

5.3 Where there is evidence that a Message has been corrupted or if any Message is identified or capable of being identified as incorrect it shall be re-transmitted by the sender as soon as practicable with a clear indication that it is a corrected Message.

5.4 Notwithstanding clause 5.1, the sender will not be liable for the consequences of an incomplete or incorrect transmission if the error is or should in all the circumstances be reasonably obvious to the recipient. In such event the recipient must immediately notify the sender thereof.

5.5 If the recipient has reason to believe that a Message is not intended for him he should notify the sender and should delete from his system the information contained in such Message but not the record of its receipt.

6. Confirmation of Receipt of Messages

6.1 Except where receipt of a Message is automatically confirmed the sender of a Message may request the recipient to confirm receipt of that Message.

6.2 When the recipient has received such a request for or where the User Manual requires a confirmation he must send it without unreasonable delay.

6.3 Each party shall process or deal with Messages received by him in accordance with any response times specified in the User Manual, or as the parties may agree or, in the absence of specification or agreement, as soon as possible.

7. Storage of Data

7.1 The Data Log including any Message as sent and received and comprised in each party's Data Log shall be maintained without any modification.

7.2 Subject to any requirements of the national law in the country of the party maintaining a Data Log or any requirements contained in the User Manual, the parties may agree a period during which the Data Log must be stored unchanged but in the absence of such agreement, a party shall have the right to maintain its Data Log for such period as it thinks fit.

7.3 The Data Log may be maintained on computer media or other suitable means provided that the data can be readily retrieved and presented in readable form.

7.4 Each party shall be responsible for making such arrangements as may be necessary for the data contained in the Data Log to be prepared as a correct record of the Messages as sent and received by that party.

7.5 Each party shall ensure that the person responsible for the data processing system of the party concerned, or such other person as may be agreed by the parties or required by law, shall certify that the Data Log and any reproduction made from it is correct.

8. Intermediaries

8.1 If a party to this Agreement uses the services of an intermediary in order to transmit, log or process Messages, that party shall be responsible towards another party or other parties to this Agreement for any acts, failures or omissions by that intermediary in its provision of the said services as though they were his own acts, failures or omissions, and for the purposes of this Agreement the intermediary shall be deemed to be an agent of that party.

8.2 If a party instructs any other party to use the services of such intermediary for transmitting a Message, then that party shall be responsible towards the other party for such intermediary's acts and omissions.

8.3 Any party giving such instructions shall ensure that it is a contractual responsibility of the intermediary that no change in the substantive data content of the Messages to be re-transmitted is made and that such Messages are not disclosed to any unauthorised person.

9. Term and Termination

9.1 This Agreement shall take effect from the date of this Agreement. A party may terminate its participation in this Agreement at any time by giving to the other party or parties not less than four weeks notice.

9.2 Notwithstanding termination for any reason, Clauses 3, 7, 8 and 15 shall survive termination of this Agreement.

9.3 Termination of this Agreement shall not affect any action required to complete or implement Messages which are sent prior to such termination.

10. Interpretation of The User Manual

10.1 Any question relating to the interpretation of the User Manual may be referred by the parties to the body responsible for the publication of the User Manual or the Council of the EDI Association as may be applicable acting as experts and not arbitrators, whose decision shall be final and binding on the parties making the reference.

11. Force Majeure

11.1 A party shall not be deemed to be in breach of this Agreement or otherwise be liable to any other party, by reason of any delay in performance, or non-performance, of any of its obligations hereunder to the extent that such delay or non-performance is due to any Force Majeure of which he has notified such other party; and the time for performance of that obligation shall be extended accordingly.

11.2 For the purposes of this clause "Force Majeure" means, in relation to any party, any circumstances beyond the reasonable control of that party (including, without limitation, any strike, lock-out or other form of industrial action).

12. Invalidity and Severability

12.1 In the event of a conflict between any provision of this Agreement and any law regulation or decree affecting this Agreement, the provision of this Agreement so affected shall be regarded as null and void or shall, where practicable, be curtailed and limited to the extent necessary to bring it within the requirements of such law regulation or decree but otherwise it shall not render null and void other provisions of this Agreement.

13. Notices

13.1 All notices or other forms of notification, request or instruction required to be given by a party to any other party under this Agreement shall be delivered by hand or sent by first class post to the address of the addressee as set out in this Agreement or to such other address as the addressee may from time to time have notified for the purpose of this clause or sent by electronic means of message transmission producing hard copy read-out including telex and facsimile, and shall be deemed to have been received:

13.1.1 if sent by first-class post: 3 business days after posting exclusive of the day of posting;

13.1.2 if delivered by hand: on the day of delivery;

13.1.3 if sent by electronic means: at the time of transmission if transmitted during business hours of the receiving instrument and if not during business hours, one hour after the commencement of the next working day following the day of transmission.

14. Amendments in Writing

14.1 Any terms agreed between the parties as additions or amendments to this Agreement shall only be valid if they are set out in the Appendix referred to in clause 2.2 or are otherwise in writing and signed by the parties.

15. Disputes and Law

15.1 Unless the parties agree to submit the matter to arbitration or other procedure for the resolution of disputes, or to select a different jurisdiction, any matter or dispute arising from, out of or in connection with this Agreement, as to its validity, interpretation, construction or performance shall be subject to the sole and exclusive jurisdiction of the English Courts.

15.2 Unless the parties otherwise agree this Agreement shall be construed and have effect according to English Law.

Published by the EDI Association, Venture House, 29 Glasshouse Street, London W1R 5RG

THE EDI
EDIA
ASSOCIATION

STANDARD ELECTRONIC DATA INTERCHANGE AGREEMENT

Explanatory Commentary

PART I

The purpose of an Interchange Agreement

Any method of communication requires discipline in order to be effective. The discipline is achieved by applying rules of conduct which by their use have become customary or by law have been imposed. Electronic Data Interchange (EDI) has not yet been in existence long enough to have acquired in these ways a collection of standard rules of conduct. An Interchange Agreement provides them.

The Standard Electronic Data Interchange Agreement (SIA) can be used in bilateral or multilateral EDI relationships. Its terms govern the conduct of the parties and set out those rules which are applicable to the general use of EDI. If they use the SIA, the parties are confirming their intention, when communicating by EDI, to be committed to each other and they cannot claim ignorance of the rules of behaviour or that they do not accept them and are not bound by them.

The distinction between an Interchange Agreement and other contracts or agreements

A fundamental principle is that the SIA relates to the interchange of data, not to the various underlying commercial or contractual obligations of the parties. The SIA is not itself a substitute for any individual contracts, express or implied, between trading partners, such as those for the supply and purchase of goods or services. Such underlying contracts and contractual relationships are assumed to exist, or to be brought into existence, just as they would if the exchange of information between the parties had been by means other than electronic. The SIA should not disturb or interfere with these normal commercial and contractual relationships. In this respect, as in others, the SIA follows the precepts of UNCID, delevoped in 1987 by the International Chamber of Commerce.

General Rules

The SIA addresses in a conveniently uniform manner those issues which are present in all EDI relationships and some which are present in most. Its rules can, therefore, be used by any EDI pair or group. A detailed commentary on the SIA clauses is in Part II.

Special Rules, User Manuals and Appendices

In individual trade sectors there will be additional rules concerning communication between the parties; rules which are specific to the requirements of that trade and not to all others. Such rules need to be set down somewhere and to be embraced by the same commitment evidenced by the SIA.

In most EDI operations there are User Manuals. These contain the procedures and rules for the technical aspects of transmission and the commercial meanings of the messages used in that trade. A User Manual can be a suitable place to set down the legal requirements associated with the specialist, trade-specific messages.

Not all trade sectors, however, will have developed and published formal User Manuals or it may be that these are for some reason not the most suitable place for some trade-specific additions or modifications. The SIA therefore provides, as an alternative, for the additional or different trade-specific requirements to be included in an Appendix forming part of the Agreement.

Liability

If a party to an agreement fails to ensure that his obligations under it are met it is possible that damage will be caused. The liability for that damage then falls upon the party whose breach caused it to occur. Unless this principle needs special emphasis or must be modified for some special reason, there is no need for an agreement to elaborate on the attribution of liability. The SIA makes little reference to attribution of liability; and then only for emphasis.

Agreements might also contain references to liability in order to place limits on it. In the SIA there is no general limitation of one party's potential liability to another because that would be to the detriment of the latter.

The SIA deals only with the conduct of the parties' communications, not with their obligations to act in accordance with the terms of their underlying commercial contract. A breach of the terms of the SIA is not of itself likely to be the direct cause of damage. If damage is caused it is more likely to have arisen out of the negligence of one party or from a breach of the underlying commercial contract which will have, if necessary, its own terms for attributing or limiting liability.

It is for these reasons that the SIA contains no special clauses about attribution or limitation of liability. If any liability were to occur it would lie where it falls.

Insurance

For reasons similar to those used in considering liability, one party or another does not acquire a significant additional burden of risk just because of the use of EDI. There is, therefore, no obligation on the parties to make special insurance arrangements. It is nevertheless recommended that individual users should check their existing insurance arrangements, advising their brokers or underwriters that they are intending to use EDI.

PART II

The implications of many of the Clauses are self-evident but the following is an explanation of the reasoning behind some of them, where this might be helpful.

Clause 1.
The importance of the EDIFACT standards is reflected in the definition of the 'Adopted Protocol'.

Clause 2.2
The use of a User Manual or an Appendix has been referred to in Part I of this commentary.

Clause 3.1.1
An important clause dealing with the security of messages.

Clause 3.1.2
"Confidentiality" is an obvious requirement in certain cases but it needs some qualification in order to avoid one party unreasonably using it to describe information which is not really confidential.

Clause 3.2
It is inappropriate for the SIA to compel encryption or any other particular methods of message protection; they must be selected by those engaged in the trades concerned. It is, however, a sound principle that the same level of protection should be required for further transmissions. It should be noted that encryption, or some methods of it, are not permitted in some jurisdictions.

Clauses 4 & 5
There could be some confusion as to the terminology frequently used; "integrity", "verification", "authenticity", "identity", "completeness" etc.

Clause 4 requires a sender of a message to state his "identity" (and, obviously, that of his addressee). There must be a means of checking that his statement is true ("verification") so that the other parties know that his message and his identity are genuine.

Clause 5 deals with the "integrity" of messages; meaning that messages must be complete and have no inaccuracies and that they stay that way. With this integrity, together with the authentication resulting from Clause 4, there is no reason for parties to the SIA to regard an EDI message as inferior in reliability to other more conventional means of communication. They can therefore agree that they will regard an EDI message as having as good a status as is possessed by a document or other form of communication. Moreover, provided the level of authentication and the technique used are good enough, they can even be confident that the message has the same essential and characteristic attributes which are present in a written communication which has been signed.

Clause 5 also deals with the procedural discipline necessary if there is obvious message corruption or misdirection.

Clause 6

There has been much debate about whether every message should be acknowledged by the recipient. It is felt that to insist on this would result in an unnecessarily and unacceptably large and costly volume of transmissions. With some messages it is not important for the sender to know that his message has been received. With some messages the sender will be made aware of the receipt because of some subsequent action by the recipient which he would not take if the message had not been received. Many EDI systems in any case automatically provide an acknowledgement signal.

Nevertheless, it is important that some messages have their receipt acknowledged. The particular trade-specific rules, which may be contained in the User Manual, will specify what is to be done; alternatively the sender will request the acknowledgement. The recipient must then comply.

Clause 7

This clause deals with the maintaining of a Data Log. Its text is such that it should result in the parties retaining essential records to satisfy commercial, administrative and fiscal requirements. Such records should also satisfy most evidential requirements, both as to admissibility and as to probative value.

Clause 8

It is not a purpose of the SIA to lay down the terms and conditions of network service providers' contracts with their clients. That must be dealt with by the clients negotiating with their network operators. However, the use of a network should not be an excuse for a sender to escape his responsibilities under the SIA. This clause therefore makes the sender's obligations clear. He is responsible for the network's acts, failures or omissions. The exception is when his use of the network is on the instructions of another party, in which case the latter party is responsible.

Clause 10

This clause refers to questions of interpretation of the contents of the User Manual. This is not to be confused with the actual settlement of disputes arising from the Agreement, which is referred to in clause 15.

Clause 12

It is possible, though not probable, that under some jurisdictions some provisions of the SIA might not be permissible. This clause enables the SIA to be widely adopted but without partial exclusions invalidating the whole agreement.

Clause 14

Additions or amendments should only be considered if they are absolutely necessary. This clause sets out the disciplined manner in which they should be made.

Clause 15

Some trades prefer Arbitration for dispute settlement. Furthermore, some parties may require that their dispute settlements are made in particular jurisdictions or that particular laws should apply. This clause provides for these alternatives to be arranged by the parties if they wish. In the event, however, of the parties making no such special arrangements, rather than having no applicable law or jurisdiction, this clause provides for English law and the English courts to be used.

Appendix D:

Network Provider Contracts

ADAPSO: Remote Processing Services Agreement
AT & T: Messaging Service and Software Agreement (US)
British Petroleum Co. Plc.: EDI Network Services Contract
British Telecom: Dialcom Service
British Telecom: EDI*Net Global Network Services
British Telecom: Prestel Information Provider Contracts
British Telecom: Conditions for Prestel Service
BT Tymnet EDI Agreement (US)
CCN Systems Ltd: Terms and Conditions
Compuserve: Computer Services Agreement (US)
Control Data Corporation: Agreement for Control Data products and services (US)
GE Information Services: Agreement for Computer Services (US)
GE Information Services: Multinational Access Agreement (Europe)
Harbinger (US)
IBM: General terms and conditions for information network service
INS: Tradanet User Contract
Istel: Computer Services Agreement
McDonnell Douglas Co.: EDI*Net Communications Services Agreement (US)
Mercury: MercuryLink Standard Conditions of Sale
Mercury: Standard Network Services Agreement
Ordernet Services Inc. (US)
One-To-One Incorporated: Terms and Conditions
PMS Communications: DIALnet User Contract
Sears Commnications Network (US)
Telenet [Sprint]: Master Agreement for Data Communications Services (US)
TranSettlements Inc.: EDI Network Services Agreement (US)

DIALnet Service Contract

This is an Agreement between:

1 PMS · Communications Limited, whose registered office is at Norfolk House, Smallbrook, Queensway, Birmingham B5 4LJ (herein referred to as "PMS"); and

2 ..... (Organisation/Subscriber)

..... (Address)

.....

.....

.....

This Agreement governs the provision of the services by PMS to the User in accordance with the specifications in each of the schedule's and on the terms and conditions attached. This covers:

* DIALnet User Contract.
* Schedule : Description of the DIALnet Service.
* Schedule : Price Tariff.

Signed	Signed .....
Print Name	Print Name .....
Position	Position .....
Date	Date .....
On behalf of	On behalf of PMS Communications Limited

DIALnet User Contract : Terms and Conditions

Whereas

a PMS carries on the business, inter alia, of providing an electronic communications and information service, the DIALnet Service, as hereinafter defined

b The User wishes to subscribe to and use the said service

c PMS has agreed to permit use of the DIALnet Service on the terms and conditions hereinafter defined

Now it is hereby agreed as follows: -

1. Definitions

"The DIALnet Service" means the service(s) provided by PMS.

"Transmission" means a transmission of data between the User and his Network Partner's and/or the User and the DIALnet Service.

"Network Partner" means other users of the DIALnet Service to whom a User will communicate via the DIALnet Service.

"CIUG Provider" means the organisation which establishes the Common Interest User Group.

"Common Interest User Group" means those DIALnet Users permitted by the CIUG Provider to have access to information provided by a private Service(s).

"DIALnet User" means an individual user that has been granted access to the DIALnet Service and has a DIALnet Mailbox.

2. Service

2.1 This Agreement governs the provision of the parts of the DIALnet Service which shall be provided by PMS, in accordance with the specifications in the 'Description of the DIALnet Service' Schedule as such specifications may be varied by PMS from time to time.
Such services are provided according to the descriptions of them herein and/or in PMS's applicable price schedule(s) current at the date of signature of this contract; as such may be amended from time to time in accordance with the provisions of this contract.

2.2 PMS grants the DIALnet User a non-exclusive and non-transferable right to obtain access to, process and use for its own internal purposes information provided by the DIALnet Service, which may be made available to it by PMS from time to time.

2.3 PMS reserves the right to withdraw or modify any particular service in the interest of maximising the effectiveness of its services.

3. Payment

3.1 The User shall pay, on receipt of PMS's invoices, all applicable fees and charges of the types and amounts stated in PMS's applicable price schedule, as amended from time to time. Any such invoices shall be payable by the User within 30 days of the date of such an invoice.

3.2 In the event that any charges are unpaid as at the end of the 30 days specified in sub-clause 3.1 above, then PMS reserves the right to:

3.2.1 suspend the DIALnet Service for the User, having given to the User 14 days notice of its intention so to do; and/or

3.2.2 charge interest on a daily basis which shall be calculated from the original due date at 4 per cent above the Bank of England base rate in force from time to time.

3.3 In the event that the DIALnet Service is suspended, the User shall pay a charge of 25% of the then current annual mailbox fee, currently as specified in the 'Price Tariff' Schedule, in order to be reconnected.

4. User Obligations

4.1 The User shall have available at its expense and on its premises all such equipment, communications lines, magnetic media, programs, personnel and any other materials as are necessary for the submission of Transmissions to the DIALnet Service and for their retrieval and deletion therefrom. The User shall interface to the DIALnet Service only hardware and software validated for the purpose by PMS.

4.2 The User shall be responsible for the accuracy of the data and addressing and for the proper use of passwords within Transmissions submitted to the DIALnet Service and for the correct formatting thereof in accordance with the standards specified by PMS from time to time.

4.3 The User shall keep confidential all information, including passwords, identifying all other Network Partners and the contents of their Transmissions.

4.4 The User shall retain a copy of all Transmissions submitted by the User to the DIALnet Service, or shall otherwise retain the ability to reconstitute such Transmissions until their correctness shall have been established so that PMS is able to perform its obligations at sub-clause 8.5.

4.5 The User shall give reasonable notice of any significant change which it expects to make in the average monthly volume of transmissions.

4.6 The User shall nominate one representative and one deputy (which person may be substituted by the User from time to time) either of whose authority PMS may rely on in its relationship with the User.

4.7 If the User is a member of a Common Interest User Group, the User shall at all times abide by the terms and conditions operated by the Common Interest User Group, except where such terms and conditions conflict with the terms of this Agreement.

5. Security of data

5.1 PMS shall use all reasonable endeavours to ensure that the User's data is not lost or corrupted within the DIALnet Service.

5.2 PMS shall keep all the User's data submitted to the DIALnet Service strictly confidential and shall not disclose it to any third party other than as permitted under the Contract or to any body having statutory authority so to require.

5.3 PMS shall not alter any of the User's data save to the extent necessary for performing conversions of protocol or of data structure and by deletion of passwords so as to make such data available to its intended recipient in a standard and acceptable format.

5.4 Subject to the provisions of sub-clause 5.5 below, PMS shall ensure that data is exchanged only between the User and his Network Partners who have agreed to exchange types of data concerned and whose current passwords coincide with passwords submitted for Transmissions of the data concerned.

5.5 Whilst PMS has built into the computer programs, which will be used in the provision of the DIALnet Service, checks and controls designed to detect and prevent unauthorised access to the User's data which is being transmitted or stored in electronic form. PMS does not guarantee that a third party could not, using wilful and persistent efforts, gain unauthorised access, but PMS shall at all times endeavour to prevent any such unauthorised access.

5.6 PMS shall ensure at all times that all access to computer operations and to computers used in the provision of the DIALnet Service shall be strictly controlled.

5.7 PMS shall ensure at all times that effective restart and recovery procedures are available.

6. Intellectual Property Rights

6.1 All data submitted to the DIALnet Service by the User shall be and shall remain the property of the customer.

6.2 PMS hereby warrants that either it or its licensor is the proprietary owner of the right to use all specifications and computer programs written or provided by PMS for or in relation to the DIALnet Service and undertakes to indemnify the User at all times against all liability in respect of claims from third parties for infringement thereof.

6.3 The User accepts that all such copyright and said intellectual property rights shall remain vested in PMS or its licensor.

7. Publicity

PMS shall be entitled to refer to the User in its promotional material as a user of the DIALnet Service.

8. Exemptions and Liability

8.1 Neither party hereto shall be liable for any breach of its obligations hereunder resulting from causes beyond its reasonable control including, but not limited to, refusal of licence (including refusal or revocation by any duly authorised public telecommunications operator of consent in respect of communications equipment and/or transmissions, other than revocation due to any act or omission on the part of PMS); fires strikes (of its own or other employees) insurrection or riots embargoes container shortages wrecks or delays in transportation inability to obtain supplies and raw materials requirements or regulations of any civil or military authority.

8.2 PMS shall have no liability for consequential loss, including loss of business and loss of profits, arising from the provision of, or any failure to provide the DIALnet Service.

8.3 PMS shall have no liability for any loss or damage suffered by the User as a result of the non-availability or failure of any telecommunications line of any duly authorised public telecommunications operator, except where such non-availability or failure is caused by any act or omission on the part of PMS.

8.4 Since PMS has no knowledge or control over the types or volumes of Transmissions which the User or other users will submit to the DIALnet Service at any particular time, PMS does not guarantee any specific time for delivery of any Transmission. PMS shall however use all reasonable endeavours to deliver Transmissions within the shortest possible time.

8.5 If any transmission submitted by the User to the DIALnet Service is, through the fault of PMS, incorrectly transmitted, PMS will, at the request of the User, re-transmit at the request of the User such transmission at PMS's expense, provided that the User has fulfilled its obligation at sub-clause 4.4.

8.6 PMS shall have no liability for any injury loss or damage suffered by the User caused by

8.6.1 any neglect or default of the User, its servants or agents or any third party or

8.6.2 failure by the User, its servants or agents to follow any reasonable instructions or recommendations which PMS may give with respect to the DIALnet Service, or to follow good computing or telecommunications practice.

8.7 Total liability of PMS under this Contract shall be limited in respect of each event or series of connected events as follows:

8.7.1 £250,000 in respect of physical damage to or loss of tangible property;

8.7.2 no limit in respect of negligence causing death of or injury to persons; and

8.7.3 for any other loss or damage arising from use or failure of the DIALnet Service, whether in contract, tort or otherwise, shall not exceed three months' average billing to the User over the twelve months preceding the month in which the damage or injury is alleged to have occurred.

8.8 The User shall indemnify PMS against all third party claims of whatever kind arising directly or indirectly from or consequential upon the use of the DIALnet Service by the User, providing PMS has complied with the instructions of the User.

8.9 The User shall indemnify PMS against any and all losses, costs, damages and expenses which PMS may suffer as a result of or in any way in connection with any wilful or negligent breach by the User of any of the User's obligations duties and responsibilities under this Agreement.

8.10 PMS gives no warranty or representation as to the fitness or accuracy of the information contained within all or any databases, conferences, distributions, mail messages or provided by a on-line enquiry service, accessed via the DIALnet Service.

9. Data Protection

9.1 In the event that any of the electronic data held by PMS in the course of supplying the DIALnet Service consists of personal data as defined by section 1(3) of the Data Protection Act 1984, then PMS shall at all times comply with the provisions of the said Act insofar as they relate to such personal data.

9.2 The User shall indemnify PMS against all or any damages, losses, claims, costs and expenses sustained or incurred by PMS in connection with any prosecution of PMS under the Data Protection Act 1984 or any civil action brought by any person or persons under the said Act against PMS in so far as any such prosecution or civil action may be in respect of the User's data.

10. Termination

10.1 This Agreement may be terminated:

10.1.1 forthwith by PMS if the User fails to pay any sum due hereunder within 30 days of the due date therefor;

10.1.2 forthwith by either party if the other commits any material breach of any term of this Agreement and which (in the case of a breach capable of being remedied) shall not have been remedied within 30 days of a written request to remedy the same;

10.1.3 forthwith by either party if the other shall convene a meeting of its creditors or if a proposal shall be made for a voluntary arrangement within Part I of the Insolvency Act 1986 or a proposal for any other composition scheme or arrangement with (or assignment for the benefit of) its creditors or if the other shall be unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986 or if a trustee receiver administrative receiver or similar officer is appointed in respect of all or any part of the business or assets of the other or if a petition is presented or a meeting is convened for the purpose of considering a resolution or other steps are taken for the winding-up of the other or for the making of an administration order (otherwise than for the purpose of an amalgamation or reconstruction);

10.1.4 by either party giving not less than 90 days written notice to the other expiring on any anniversary of the Commencement Date.

10.2 Any termination of this Agreement pursuant to this clause shall be without prejudice to any other rights or remedies either party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities of either party nor the coming into or continuance in force of any provision hereof which is expressly or by implication intended to come into or continue in force on or after such termination.

11. Notices

Any notice request instruction or other document to be given hereunder shall be delivered or sent by first class post or telecopier to the address or telecopier number of the other party set out above (or such other address or telecopier number as may have been notified) and any such notice or other document shall be deemed to have been served at the time of delivery or transmission by telecopier or if sent by post upon the expiration of 48 hours after posting.

12. Waiver

The waiver by either party of a breach or default of any of the provisions of this Agreement by the other party shall not be construed as a waiver of any succeeding breach of the same or other provisions nor shall any delay or omission on the part of either party to exercise or avail itself of any right power or privilege that it has or may have hereunder operate as a waiver of any breach or default by the other party.

13. Invalidity and Severability

If any provision of this Agreement shall be found by any court or administrative body of competent jurisdiction to be invalid or unenforceable the invalidity or unenforceability of such provision shall not affect the other provisions of this Agreement and all provisions not affected by such invalidity or unenforceability shall remain in full force and effect. The parties hereby agree to attempt to substitute for any invalid or unenforceable provision a valid or enforceable provision which achieves to the greatest extent possible the economic legal and commercial objectives of the invalid or unenforceable provision.

14. Arbitration

Any dispute arising out of or in connection with this Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the Rules of the London Court of International Arbitration, which the Rules are deemed to be incorporated by reference into this Clause. The tribunal shall consist of three arbitrators. The place of arbitration shall be London.

15. Entire Agreement

This Agreement is the entire agreement between the parties and all other terms whether or not agreed or offered and all conditions and warranties whether express or implied statutory or otherwise and all representations whether made orally or in writing before or after the date hereof are hereby expressly excluded and cancelled save to the extent that the same appear herein or are specifically agreed in writing after the date hereof and signed on behalf of both parties by a director of each and the User acknowledges that save as contained herein there are no representations or warranties which have been made by PMS in respect of the Licensed Programs, the Equipment or the DIALnet Services upon which the User has relied in entering into this Agreement.

16. Assignment and Sub-Licensing

16.1 The User shall not be entitled to assign this Agreement nor any of its rights or obligations hereunder nor sub-licence the use (in whole or in part) of the Licensed Programs.

16.2 Nothing herein contained shall operate so as to prevent PMS from performing its obligations hereunder by the use of sub-contractors.

17. Law

This Agreement shall be governed by and construed in accordance with English law and the parties hereto agree to submit to the exclusive jurisdiction of the English courts

Schedule : Description of DIALnet Service

Access	DIALnet can be accessed asynchronously via direct dial, BT's Dialplus service or a DIALgate facility, or synchronously via dedicated lines. Special requirements for linking other networks are subject to separate discussion and negotiation. The usual access protocols employed are MNP Class 4 for error correction and the DIALnet protocol for general session control and file transfer. For synchronous connections a variety of protocols are supported including but not limited to FTAM, X25, X400, DECnet and SNA. The key access product specifications for access (and file transfer) are : a V22bis modem with MNP Levels 4 & 5, and access software with VT52 emulation, KERMIT ft protocol & DIALnet protocol.
Accounts	Facilities subscribed to on a fixed cost basis will be charged annually, 12 months in advance.
Applications	PMS work closely with a number of authorised suppliers of third party applications software to automate data exchanges. A current list of authorised suppliers is available from PMS. PMS provide support for problems relating to direct access and to the DialUp access software. Queries relating to communications initiated from the application must be firstly directed to the applications supplier.
Approval	Suppliers of DIALnet communications hardware where possible have approval granted under BS5750. Only modems with BABT approval are authorised for use by PMS.
Auditing	An audit trail of all EDI message receipt and delivery within the retention period is available showing times of messages delivery, routing, delivery and collection. DIALnet also automatically generates periodic summary reports. Network usage is automatically monitored and traced. This provides event logging and notification to network operators.
Availability	PMS will endeavour to ensure the DIALnet network and DIALnet service is available for 361 days a year, 20 hours a day. Maintenance downtime relates only to upgrades. The only other scheduled downtime is for security backups. Availability is based on a probability analysis of the aggregate MTBF figures for the hardware involved in a link to DIALnet. This will differ depending on the hardware employed for a particular link. Based on this, availability of the network for sites taken individually is likely to differ from that for the network as a whole, although not significantly.
Backups	All data received is backed up on a daily basis.
Consultancy	Charges may be levied for pre or post technical consultancy, and customers will be notified of this in writing in advance. We are happy to respond to requests for site visits by PMS staff to install or assist in installations of the access software and communications hardware provided. Charges will be levied in accordance with the installation task, and as above, customers will be notified in writing in advance of the rate of any charges to be levied. Any requests from the customer for an input to areas which affects the operation of their system will need to be formally agreed beforehand and only be carried out in conjunction with intense consultation of customer staff.
Delivery	PMS will endeavour to keep to any agreed delivery dates unless prevented from doing so by circumstances outside its control. PMS will not be liable for any loss resulting from delay.
DIALgate	A 4-hour callout is included as part of the standard contract for hardware error conditions at remote sites. Alternative access will be offered during the failure period. Maintenance of hardware components is carried out by the original suppliers of that equipment. British Telecom's lines are maintained by themselves.
Documentation	Training manuals are provided free of charge on training courses, and quick reference cards are provided free of charge to LEAs or Exam Boards for general distribution. User manuals or additional manuals are also available, at minimal charges, from PMS.
EDI	DIALnet supports the following EDI standards : DIALNET; ExamData, EDIFACT & TRADACOMS. Validation of EDI messages is limited to the control segments, and does not cover the data content.
E-Mail	The E-Mail facility is X.400 compliant.
Failures	The system will report non-delivery of messages back to the originator.
New Facilities	New facilities developed for general use on the DIALnet service or within the access software will be offered to customers as they become available. PMS will however reserve the right to make charges for these facilities.
On-Line Enquiries	For the development of an on-line enquiry facility the customer must undertake bespoke development work to allow an appropriate request mechanism to be set up on their system which will make use of an appropriate protocol as agreed.
Options	A package of additional options to suit an LEA or Exam Board, such as extended support, itemised billing, is available for an additional fee. Please contact PMS for more details.
Orders	All orders must be accompanied by an Official Purchase Order. Goods and services will not be despatched until the order has been received.
Payment	All goods will be invoiced within the same week of delivery. Invoices are due for payment within 30 days of the date of invoice.
Price Changes	Any future prices changes to our educational customers will be kept in line with changes in the main cost of components of the service provided. This is in line with other supplier's of goods and services to the educational sector. PMS will give customers at least 30 days notice in writing of any amendments to prices before subscription renewal dates.
Recovery	In the event of the failure of the DIALnet system at the central site, all data can be moved to a second computer site nearby and the system will endeavour to be operational within 24 hours.
Reliability	No component of the hardware used in the provision of the DIALnet service and used for control of the network shows a MTBF of less than 10.4 years.
Response Time	PMS will endeavour to respond to requests from the customer for software maintenance within the following timescales: 24 hours for remedial maintenance; 48 hours for system management & 10 working days for training.
Responsibility	PMS's responsibility begins when a message is received by DIALnet.
Security	The operating system under which the DIALnet service runs achieves American Department of Defence C2 security clearance. DIALnet uses 2 further levels of access password protection. In addition, use of the recommended access software, DialUp, offers a unique security checking mechanism.
Software	A software licence agreement is provided independently for the use and maintenance of the DialUp communications access software.
Storage	The maximum space available for mail message and personal non-EDI file storage is 20Mb per LEA/Examining Board, 1MB per £150 mailbox account and 0.5Mb per £75 mailbox account. Extensions to this are negotiable. PMS maintain a standard retention period of 30 days for EDI transmissions, 60 days for READ mail messages and 90 days for UNREAD mail messages. After this period data is removed from the system (and will not be archived further). Separate agreements with extended (or reduced) archiving periods can however be made with PMS. PMS will however reserve the right to make charges for these facilities.
Support	Help desk facilities are available between 9.00am and 5.00pm during weekdays (excluding public holidays) for CIUG providers, LEAs or individual users with support contracts. A higher level of support can be provided if required, the cost of which is separately negotiable.
Training	PMS run a number of DIALnet training courses and the rates per person per day are listed in the 'Price Tariff' Schedule. These courses cover use of the recommended DialUp access software, and user and account manager facilities on the DIALnet service. Training on the use of a particular applications software is not generally provided, but can be accommodated on special request. There may be additional charges associated with the latter. Please note that a 3 day training programme for up to a maximum of 12 people is included for LEA or Exam Board staff in their EDI registration fee.
Upgrades	DIALnet (and the DIALgate equipment) is constructed using a modular approach. Upgrades to deal with the need for increased capacity of data traffic or processing are thus easily accommodated.
Warranty	PMS provide a 30 day warranty with the DialUp access software, a 3 year warranty with modems supplied in the communications starter package & a 3 month warranty with a DIALgate installation. During this period, and faults or failures which occur will be rectified free of charge.

Schedule : Price Tariff

Electronic Mail	Educational User	..... £150	per annum

NB : The tariff of other facilities and products, training and consultancy will be appended according to individual customer requirements.