UNIVERSITY OF STRATHCLYDE

DATA PROCESSING AND INDIVIDUAL FREEDOM

DATA PROTECTION AND BEYOND

THE LAW SCHOOL

SUBMITTED BY IAN J LLOYD FOR THE DEGREE OF Ph.D.

MAY 1988

Abstract

This thesis attempts to place data protection legislation in its historical and legal context. Initially, it is argued that, within the United Kingdom's legal traditions, this subject should not be seen primarily as a response to concerns for the individual's right of privacy but rather as a means of safeguarding more tangible liberties.

Within the confines of data protection legislation the merits of the Data Protection Act of 1984 are considered, both internally and as a response to the demands of the Council of Europe Convention for the Protection of Individuals with Regard to the Automated Processing of Personal Data.

Within Western Europe the establishment of a supervisory agency to monitor data users' compliance with its dictates has come to be regarded as an integral feature of legislation. Whilst recognising the value of such an agency, this thesis criticises the manner in which the performance of its functions has been linked to a system of near universal registration of data users. In the age of the personal computer, this provides no realistic check upon the activities of users serving, rather, to dilute the resources of the

supervisory agency.

In addition to establishing a supervisory agency, data protection legislation confers directly enforceable rights upon individuals. These are, however, subject to exceptions, the scope and extent of which it is argued serve to considerably and unnecessarily limit their utility.

In conclusion, it is argued that although data protection performs a valuable role, it must be only one part of an information policy designed for today's "information society". Data protection functions largely at the individual level, and can have little impact upon developments in informational practices involving, for example, policing strategy, which possess general societal implications. Data protection must, therefore be seen as an intitial rather than as a definitive legislative response.

Table of Contents

Chapter One

Information and Knowledge: Privacy and Liberty

Information and Knowledge: Privacy and Liberty

1. From Knowledge to Information

When the philosopher Francis Bacon wrote in the sixteenth century to the effect that:

> "Knowledge, of itself, is power."(1)

he did no more than restate an accepted sentiment. Today it has become trite comment to assert that we live in an information society where:

> "Information is power"(2)

At first glance these phrases might appear synonymous, a view which is to some extent confirmed by reference to the dictionary. Here the word 'knowledge' is defined, inter alia as:

> "The process of knowing, familiarity gained by actual experience."(3)

whilst information includes:

> "Intelligence communicated; notice, knowledge

acquired."

Although a degree of overlap undoubtedly exists between these two definitions the critical distinction rests, it is submitted, in the fact that knowledge is gained by an individual through the application of his own physical and/or mental capabilities. Although knowledge can be represented as information it remains a subjective quality. It can, to some extent, be transferred to another person but this requires the application of some degree of intellectual application on the part of both teacher and pupil and total transference may rarely be obtained. The illustration might be provided of a legal text book. The text or information contained therein will represent the legal knowledge of the author. Possession of the information will be obtained by a purchaser of the book; what is less easily acquired is the knowledge and understanding of the subject possessed by the author.

From this state of affairs the conclusion may be drawn that whilst all knowledge may be represented by information, information may not always be equated with knowledge. In many cases information will consist of items of data,(4) each piece of data representing an item of information, being either factual or judgmental. When divorced from the qualitative and subjective aspects of knowledge, information acquires an objective status and, as such, may be considered a

commodity. As with all commodities it may possess economic value and take its place in the market place to be bought and sold.(5)

The increasing role of information, a fact which pre dates the computer age, has considerable significance for the individual. Many situations may be envisaged in which the individual's quality of life will be affected by the actions of others. These actions may take a variety of forms with consequences for the individual's emotional, physical and financial well being. Whilst, in some circumstances, this may involve the application of knowledge, for example when a doctor uses his acquired expertise and observational facilities to diagnose a patient's affliction, increasingly it is the case that actions are based not on direct observations or knowledge but from recourse to acquired information. A credit company, for example, faced with an application for credit may base its decision not on its own knowledge of the applicant's character but may have recourse to information held by a credit reference agency.

Reliance upon information as opposed to personal knowledge may serve to render the decision making process more equitable from the subject's perspective. The fact that knowledge is a subjective quality allows decisions to be founded on personal prejudices. A decision based on objective informational criteria may

be considered preferable but this requires that the information used be accurate. Human personality can easily be subsumed in a cold, unemotional and inaccurate record system.

The effects of modern informational practices, both in terms of their impact upon the individual and on a wider, societal basis can be felt in a variety of areas. From the individual's perspective, the technical facility increasingly available to organisations acquire, store, process, store, use and disseminate information relating to that person may be considered invasive of privacy. Many aspects of our lives which may previously have passed unrecorded or which may have been subjected to partial or temporary scrutiny may now be permanently recorded and widely disseminated. The fear exists of a computerised 'Big Brother' who is aware of our every movement and action.

The legal response to the challenges resulting from the application of information technology has hitherto taken the form of the promulgation of data protection legislation. Such legislation is normally, expressly or impliedly, based upon considerations of the individual's "right to privacy". It will be argued in this thesis that, although the privacy implications of modern informational practices cannot be ignored, an excessive concentration on this aspect results - particularly within a United Kingdom context - in a

failure to fully address some of the most threatening aspects of the topic. Prior to considering the limitations of privacy, however, it is necessary to briefly consider the legal and philosophical basis and the historical development of this concept.

2. Privacy and the Law

Linguistically the word "privacy" can be simply defined as the state of being withdrawn or secluded. As a factual description of such a condition or state the notion of privacy is, indeed, susceptible of easy definition. Within the legal context, however, the task is less straightforward. Numerous definitions of the scope of the individual's demand for privacy have been essayed but only the broadest can be regarded as encapsulating all the nuances of this elusive commodity. Thus, in the legal context, the manifestation of the individual's demand for solitude has been described as constituting the:

> "right to be let alone"(6)

Although the wish to enjoy a measure of privacy is a near universal human characteristic, different individuals and indeed different cultures have varying expectations of privacy. It has, for example been reported that:

> ".. it is now official Swedish policy to establish a central register of personal information covering all Swedish residents .. This central register will be public and will show each resident's income, as well as his name, personal number, address and nationality. In the UK, by contrast, it is generally the case that the privacy of a person's financial circumstances is jealously guarded, and this is reflected in the strict statutory rules of secrecy which govern the work of the Inland Revenue. As one member of the new Swedish data protection commission is reported to have said, "I know that if you tell an Englishman that he can't keep his income secret from his wife, he thinks he has nothing less to lose but Swedes are quite happy to .. (have the information publicly available)"(7)

Confirmation of the accuracy of this statement as representing the prevailing British attitude may be found in the report of the Committee on Privacy which commissioned a survey of public opinion on privacy related matters. This identified a widespread view that personal financial matters should be accorded a high degree of confidentiality.(8)

Beyond the individual's instinctive perceptions of privacy considerable philosophical debate centres upon

the extent of such a right and, in particular, upon the extent to which the individual's wish to be let alone may conflict with his role as a member of society. In the final analysis, a decision may have to be made whether it is the task of society to serve its individual members or the duty of individuals to so order their affairs as to best serve society as a whole. In large part the debate in this area has centred upon the question whether the province of the legislature should be restricted so as to retain for the individual aspects of life over which he retains sovereignty. At one level this question is concerned with rights of property and, at a less tangible level, with individual privacy. Mill, for example, argues(9) in favour of the essential supremacy of the individual stating that society has the right to control his behaviour, normally through the imposition of legal sanctions, only to the extent that this is necessary to prevent him from causing positive harm to another. Mill considered that this freedom from legal control contained two components; firstly, the right to freedom of thought and, secondly, to freedom of action where this did not cause harm to others. Thus,

> ".. the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self protection. That the only purpose for which power can be rightfully

> exercised over any member of a civilised community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant ... Over himself, over his own body and mind, the individual is sovereign."(10)

The application of Mill's doctrines concerning the relative roles of the individual and of society can perhaps best be illustrated by reference to constitutional developments in the United States of America. Under the terms of the ninth and tenth amendments to the Constitution it is provided that:

> "The enumeration in the Constitution of certain rights shall not be construed to deny or to disparage others retained by the people."

> "The powers not delegated to the United States by the constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

In applying these provisions coupled with the more substantive elements of the Constitution, the Supreme Court has, albeit not unanimously, identified privacy interests as being among those protected under the Constitution. In the case of Griswold v. State of Connectitut(11) the Supreme Court ruled on the validity

of a state law rendering the use of contraceptives criminal. Striking down the statute the Court referred to its previous decision in the case of NAACP v. Alabama(12) in which it was held that a requirement compelling disclosure of membership lists of an association violated the first amendment establishing freedom of speech. The court here was willing to accept freedom of association as an element of free speech and held that the requirement of disclosure might inhibit the exercise of this right, making specific reference to the

> ".. freedom to associate and the right to privacy in one's associations."(13)

and concluding that:

> "Inviolability of privacy in group association may in many circumstances be indispensible to preservation of freedom of association, particularly where a group espouses dissident beliefs."(14)

In the present case the court relied variously upon the terms of the fourth, fifth and fourteenth amendments to the Constitution holding that:

> ".. specific guarantees in the Bill of Rights have penumbras, formed by emanations from those

> guarantees that help give them life and substance."(15)

Among these must be numbered a right to privacy and, in the present case the marital relationship was considered as:

> ".. lying within the zone of privacy created by several fundamental constitutional guarantees."(16)

The decision can thus be seen as providing recognition of the fact that the rights protected in the Constitution are illustrative rather than exhaustive and that other rights may be identified as fundamental and removed from the province of the legislature. The majority opinion was, however, subjected to a strenuous dissent from Mr Justice Black arguing that:

> "The Court talks about a constitutional "right to privacy" as though there is some constitutional provision or provisions forbidding any law to be passed which might abridge the "privacy" of individuals. But there is not. There are, of course, guarantees in certain specific constitutional provisions which are designed in part to protect privacy at certain times and places with respect to certain activities."(17)

Referring to the provisions of the fourth amendment guaranteeing protection against "unreasonable searches and seizures", he commented that the question whether any infringement occurred in private or in public was largely irrelevant. The majority, he argued, used:

> "the term "right of privacy" as a comprehensive guarantee for the Fourth Amendments guarantee against "unreasonable searches and seizures."(18)

The two approaches were not, he considered interchangeable and, he concluded, whilst:

> "I like my privacy as well as the next one .. I am nevertheless compelled to admit that government has a right to invade it unless prohibited by some specific constitutional provision."(19)

Despite these doubts subsequent decisions of the Supreme Court have served to expand the role of privacy as a constitutional guarantee. In the case of Roe v Wade(20) it was held that the provisions of the fourteenth amendment prohibiting the deprivation of liberty or property without "due process of law" rendered unconstitutional a state law prohibiting a woman's right to obtain an abortion. Whilst recognising that the woman's rights were not unqualified in this

situation the court held that a total prohibition infringed, inter alia, rights of privacy.

The decisions of the Supreme Court can be seen as creating a number of zones of privacy within which the individual must be permitted freedom of action without the risk of legal interference. In this respect the American approach may be regarded as conforming to Mill's dictates. It must be noted, however, that a distinction has been drawn between invocation of rights to privacy as a defence against legal sanctions and the grant of a more general right of privacy. The individual may be protected in the situation where his liberty or his property rights are put at risk but this is far from enshrining a "right to be let alone." In order to establish this it is necessary that an individual's privacy should be protected not for fear of the legal consequences which may follow any invasion but simply because he wishes to be let alone from the gaze of others, whether public officials or his fellow citizens. In Katz v. United States(21) the Court, albeit holding that the tapping of the appellant's telephone violated his rights of privacy, specifically held that no general right to privacy existed under the Constitution. The issue of a general right to privacy was further explored by the court in the case of Whalen v. Roe.(22) Here the Court considered a challenge to a New York statute requiring that medical practitioners supply public authorities with details of prescriptions

issued for certain categories of narcotics. These details were subsequently recorded on computer. Although unauthorised possession of these drugs would constitute a criminal offence the records in this case were concerned with legitimate prescriptions and no legal sanctions could be invoked against those identified on the computer record. Nonetheless the statute was struck down in the District court(23) on the basis that it infringed patients' rights of privacy. This conclusion was reversed by the Supreme Court. Although recognising that individuals' reputations might be adversely affected in the event that the information concerning their drug taking was further disseminated and although stating that it was:

> ".. not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.."(24)

the court declared that no general constitutional right to privacy existed. Privacy concerns might be linked to more tangible invasions of rights but could not be protected in isolation.

This decision serves to illustrate the difficulties encountered in attempting to apply an elusive and subjective concept, such as that of privacy, into any system of basic or fundamental rights. Two particular

problems may be identified. First, fundamental rights protect an individual against the abuse of legal power but can offer little protection where the threat is not one of legal sanction but, rather, of public opprobrium. Second, the notion of fundamental rights serves to protect the individual against the abuse of state power seeking to grant immunity against the imposition of legal sanctions for actions which may be considered to lie in the province of individual morality. Whilst this formulation may be effective against at least some of the actions of public authorities many of the activities which may be considered to amount to an invasion of privacy are carried out by one private individual against another or by a public agency in circumstances not directly concerned with the imposition of criminal sanctions.

The enshrining of rights in a constitutional document having an authority greater than that granted to other forms of law may be seen as a prerequisite to the imposition of limitations upon the powers of the legislature. No such limits apply in the United Kingdom where the doctrine of Parliamentary supremacy holds sway. Although moral and philosophical considerations may motivate Parliamentary actions the validity of any statute cannot be challenged on such a basis. Bentham has argued that:

"The greatest happiness of the greatest number

is the foundation of law and morals."(25)

but Devlin comments that:

> "It can be said in general terms, and often is, that law makers are bound to legislate for the common good. The common good is perhaps a useful and compendious, if vague, description of all the things law makers should have in mind when they legislate. But it does not constitute a clear limitation upon the right to legislate."(26)

In the field of privacy the question was posed and answered:

> "Can then, the judgement of society sanction every invasion of a man's privacy, however extreme? Theoretically that must be so; there is no theoretical limitation. Society must be the judge of what is necessary to its own integrity if only because there is no other tribunal to which the question can be submitted."(27)

Although Lord Devlin is willing to concede that, so far as is possible, individual privacy should be respected by the law maker this can constitute no more than one factor to be taken into account in determining the

shape of the law.

Of the competing schools of thought discussed above it seems clear that the views of Lord Devlin most accurately represent the current state of British constitutional theory. The absence of legal provisions expressly or impliedly enshrining rights of privacy does not, of course, mean that this value is not recognised in the law and in the following section the extent of legal recognition of rights of privacy in the UK will be discussed.

3. The Right to Privacy

Acceptance of the right to be let alone within one's property is an established feature of English and Scottish laws. In a series of seminal decisions during the 17th and 18th centuries(28) the English courts placed substantial restrictions upon the rights of the state to infringe the property rights of its citizens. The law's concern was, however, directed almost exclusively at property rights with non-physical invasions of privacy giving rise to little in the way of legal redress. In the field of criminal law the Scottish authority of Raffaelli v. Heatly(29) suggests that conduct amounting to an invasion of privacy might be prosecuted as breach of the peace. Here, the appellant had been observed to peer through the window

of a house. Although the occupant was unaware of his actions the High Court upheld his conviction on a charge of breach of the peace.

The traditional approach towards such activities can be demonstrated by reference to the case of Malone v. Commissioner of Police for the Metropolis ((Number 2).(30) The plaintiff in this action had been suspected by the police of having received stolen property. In an attempt to obtain evidence on this point his telephone was tapped. In the course of a subsequent criminal prosecution the fact of the telephone tapping emerged and, following his acquittal on the criminal charges, the plaintiff instituted civil proceedings seeking a declaration that the tapping of his telephone should be considered illegal. This action was dismissed by Vice-Chancellor Megarry who commented that:

> "England, it may be said, is not a country where everything is forbidden except what is expressly permitted; it is a country where everything is permitted except what is expressly forbidden."(31)

Whilst this passage may appear to provide a ringing endorsement of individual rights and freedoms, its effects were less happy from the plaintiff's standpoint. The freedom to act unless specifically stopped permitted the police authorities, or indeed

anyone else, to tap telephones in the absence of a clear legal prohibition. Whilst such an approach may be appropriate in the case of notions such as freedom of speech, association and movement which require positive action on the part of the claimant with the sole duty imposed on others being one of non-interference; the situation is radically different with the claim to privacy in as much as the attainment of the claimant's desires is totally dependent upon the conduct of others. In discussing this concept McCormick has distinguished between "claim rights" and "liberties" with privacy falling into the first category and other freedoms into the second and concluding that the traditional English approach ill serves the attainment of the former.(32)

Accepting that no general right to privacy existed in English law, the plaintiff further argued that a specific right should be recognised consisting of the entitlement to hold a private telephone conversation. Once again, this suggestion failed to obtain the Vice-Chancellor's support. Whilst he was:

> ".. not unduly troubled by the absence of English authority: there has to be a first time for everything.."(33)

he considered that:

> ".. it is no function of the court to legislate in a new field. The extension of existing laws and principles is one thing; the creation of an altogether new right is another."(34)

Support for the plaintiff's argument would, he considered, involve the creation of just such a new right; a task belonging to Parliament rather than to the courts.

The limited recognition of a right of privacy was further demonstrated in the case of Bernstein of Leigh (Baron) v. Skyways and General Ltd..(35) Here, the defendants arranged for the taking of aerial photographs of properties with a view to offering to sell copies of these to the owners. In the course of this business the plaintiff's country house was photographed. On discovering that this had taken place, and following a series of misunderstandings and disagreements with the defendants, the plaintiff instituted legal proceedings contending that the defendants' conduct amounted to an actionable invasion of his privacy. He consequently sought damages, the delivery up of the offending photograph and an injunction to prevent further invasions of privacy. This action was dismissed by Griffiths J. who held that, although the defendants' plane had entered into the airspace extending above the plaintiff's property, this was not to be considered as a trespass. Whilst

the rights of a property owner extended above ground level a balance had to be struck between the rights of an owner as against those of the general public. In this case the judge concluded that this would be best accomplished by:

> ".. restricting the rights of the owner in the air space above his land to such height as is necessary for the ordinary use and enjoyment of his land and the structures upon it, and declaring that above that height he has no greater rights in the air space than any other member of the public."(36)

It was recognised, however, that certain forms of surveillance might give rise to action, the judge commenting that:

> ".. no court would regard the taking of a single photograph as an actionable nuisance. But if the circumstances were such that a plaintiff was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity, I am far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance for which they would give relief."(37)

The fact that any such action would lie in the law of nuisance would appear to emphasise the fact that protection of privacy interests in English law are linked to property interests, an action in nuisance lying where property rights are adversely affected by another's actions. This linkage between privacy and property rights has prompted criticism that privacy is an elitist concept and that:

> ".. the right to be let alone can acquire a heavily negative meaning when this implies a disregard for the conditions of the less wealthy, abandoning the weakest to social violence."(38)

Whilst it may be unreasonable to equate a desire for solitude with the absence of social concern the above quote does indicate that, in common with other rights and liberties, even the most general right of privacy cannot be unqualified. One man's demand for privacy may effectively compel others to modify their behaviour and a balance will have to be struck between demands for privacy and other competing rights, perhaps most notably that of free speech. The clash between the desire to be 'let alone' and the exercise of free speech is most vividly demonstrated in the activities of the media. The seminal article of Warren and Brandeis(39) arguing for the recognition of a tortious remedy in the event of invasion of privacy would appear

to have been prompted by the publication of press reports concerning the social activities of one of the author's families. The need for such a development may be considered more necessary in the United States than has been the case in the United Kingdom. In the former jurisdiction the development of the defence of privilege in defamation suits has accorded pre-eminence to the desirability of free speech and has limited the liability of the media to situations where it can be demonstrated that their actions were motivated by malice.(40) Although the financial costs involved in pursuing an action for defamation may make such a course of action difficult for all but the wealthiest individual, proof of the inaccuracy of a report will normally suffice to establish liability. In Scotland, the existence of the action of convicium may extend liability still further although the lack of recent authority makes analysis of this area of the law uncertain. The basis for this action rests in the publication of material which is calculated to expose the subject to public ridicule or opprobrium. Although in the most recent cases upon this point argument has proceeded on the basis that statements made were false, and although the point cannot be regarded as settled, it was suggested by Lord Deas in the case of Cunningham v. Phillips(41) that

> "I am not disposed to doubt that there are some kinds of injurious publications , for which,

according to our law, there may be a relevant claim of damages, although there is no slander. Examples of such a claim are afforded by cases in which some physical deformity or secret defect, such, for instance, as that particular defect in respect of which marriage may be annulled, is wantonly and offensively paraded before the public. Other examples might also be given, and, in such cases, the truth may often be an aggravation of the offence or injury."(42)

A comment which would certainly appear to indicate that the truth of any comments will not serve as a defence. A similar conclusion was reached by Lord Kilbrandon who in discussing this point and contrasting the Scottish doctrine of convicium with the English action for defamation argued that:

".. our law recognises the right of every man to maintain his personal private dignity, apart from his private patrimony or his public reputation, against the assault of lies. It is a question whether this protection is adequate. Since it is always a defence to an action of damages for defamation that the statement complained of is true, a victim has no remedy in this narrow branch of the law when his adversary rakes up and publishes some remote

> incident from the past, perhaps a conviction before a juvenile court, and parades it in circumstances in which it has no relevance. The law of Scotland, however, it is submitted, may give an action in such a case when none would lie in England."(43)

Although the doctrine of convicium may be seen as affording a degree of protection to the individuals privacy the requirement that statements be published coupled with the need for the pursuer to demonstrate that the defender was activated by malice would appear to restrict its application to a narrow range of circumstances. It has also been suggested(44) that an action for invasion of privacy might lie in Scots law under the actio injuriarum. In contrast to the remedy based approach of the English common law the Scottish legal system strongly influenced by the provisions of Roman law has accepted the notion of general rights whilst its recognition of solatium as a basis for the award of compensation marks a divergence from the physical or property based system applied in England. Applying these principles it has been argued that any culpable act which causes another personal distress should give rise to an action, a conclusion which would appear to offer a remedy in respect of conduct amounting to an invasion of privacy. This argument is not, however, supported by any authority and, indeed, the decision of the Court of Session in the case of

Murray v. Beaverbrook Newspapers(45) declined to grant a remedy to a Sheriff whose comments regarding the punishment of motoring offenders, he himself having been recently convicted of such an offence, had been adversely commented upon by a newspaper. Here, the fact that details of the Sheriff's own convictions were published was held to give rise to no actionable claim for invasion of privacy although the court left open the question whether a similar action might succeed in the face of a systematic or deliberate persecution of an individual by a newspaper.

Analysis of the principles of both English and Scottish law would appear to indicate that in neither jurisdiction does a general right to privacy exist at common law. An Englishman's home may be his castle but his legal protection is sharply diminished once he steps over his doorstep. This rejection of a specific right to privacy may be contrasted with the approach adopted in other common law jurisdictions, most notably that of the United States, and in several European legal systems. Reference has previously been made to constitutional developments within the United States. In the field of civil law, following the publication of the famous Warren and Brandeis article, 'The Right to Privacy',(46) the existence of such a right has been explicitly recognised firstly by the courts but also through legislative interventions. Although the basis of the right remains the subject of some debate it is

clear that an action will lie on this basis where the conduct complained of amounts to "unreasonable intrusion upon the seclusion of another". On the European mainland the French courts have long provided a remedy in the event of conduct being characterised as invasive of privacy(47) whilst in West Germany, although the provisions of the civil code make no explicit mention of a right to privacy the courts have in recent years implied into this the constitutional provision demanding that individuals be afforded the opportunity of freely developing their personality.(48) Placing individuals under surveillance or otherwise intruding upon their seclusion may be regarded as infringing this right.

The practices of totalitarian regimes during the Second World War and the infringements of basic human rights resulting therefrom prompted international action in this field. In 1948 the fledgling United Nations organisation adopted the Universal Declaration on Human Rights stating, inter alia, that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.. Everyone has the right to the protection of the law against such interference or attacks."(49)

Similar sentiments were expressed in the European

Convention on Human Rights, opened for signature in 1950 and providing that:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights or freedoms of others."(50)

In contrast to the provisions of the Universal Declaration which have only moral force, the European Convention is legally 'binding' in international law. As a signatory state, therefore, the United Kingdom accepts the obligation to give effect to its provisions within domestic law. The Convention, however, leaves the manner in which compliance is achieved to the discretion of national authorities and, as has been stated above, the traditional approach of the common law has been to endeavour to provide individual rights through a multiplicity of separate legal provisions. In

addition to establishing general criteria the Convention provides, through the creation of a Commission and a Court of Human Rights,(51) a mechanism for the ventilation of individual complaints regarding signatories' compliance with its requirements.(52) The Convention leaves it open to signatories to accept as binding the decisions of the Court of Human Rights in such proceedings, an option which has been exercised by the United Kingdom government(53) but which has led to increasing doubt as to the compatibility of the traditional British approach with the evolving jurisprudence of the European authorities.

Within the United Kingdom concern at the adequacy of the legal protection of privacy reached a peak during the 1960's. In part this may be traced to the influence of the international developments described above, in part as a response to media activities in several controversial episodes and, finally, in response to a somewhat vague fear concerning the extent to which developing computer capabilities might be used to the detriment of individuals. During the period from 1960 - 1970 no fewer than six private member's bills(54) were introduced into Parliament. Several of these proposals were targetted at traditional notions of privacy with particular concern being expressed at the intrusive nature of much media activity. Typically, the proposal introduced by Alex Lyon MP(55) would have ensured that:

> "Any person who has been subject to any serious and unreasonable infringement of his right of privacy shall have a cause of action against the offender."(56)

The "right of privacy" was to be defined as:

> "The right of any person to preserve the seclusion of himself, his family or his property from any other person."(57)

Although none of these proposals became law the support offered to the final measure, introduced by Brian Walden MP(58) prompted the Government of the day to appoint a Committee, chaired by Sir Kenneth Younger,(59) with the remit:

> "To consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies and to make recommendations."(60)

Significantly, the Committee's remit was restricted to an investigation of the private sector, a limitation which two appeals from its chairman to the Home Secretary of the day could not remove.(61) After a comprehensive study of the forms which an invasion of

privacy might assume the majority of the Committee recommended against the creation of a general right. This was largely on the basis that such a sweeping declaration of rights would be alien to the British legal tradition, would result in a period of uncertainty pending the judicial resolution of particular disputes whilst the subsequent application of the doctrine of stare decisis might freeze the interpretation of the right in attitudes which might be rendered obsolete or inappropriate with changing social mores.(62)

Whilst rejecting the notion of a general right to privacy the Committee identified a number of areas where reform might usefully be considered. At the widest level they considered that many of the manifestations of invasion of privacy occurred in situations where the information had been received in circumstances consistent with the existence of an obligation of confidence. Development of this aspect of the ~~the~~ law would, in the opinion of the Committee offer a powerful antidote to many invasions of privacy.(63) Subsequent to the report of the Committee the Law Commissions have investigated this area and have produced proposals for legislation(64) which would serve to expand the range of circumstances under which the obligation of confidence would arise. To date these have not been acted upon and there appears little likelihood of early legislation.

The Younger Committee's deliberations prompted direct legislative action in only two areas. Its concern at the implications of the use of credit reference agencies as the basis for decisions concerning an individual's entitlement to credit facilities(65) resulted in the regulation of such bodies and the introduction of an individual right of access to and correction of his record under the Consumer Credit Act of 1974.(66) In many respects this legislation can be seen as a precursor to the Data Protection Act and its provisions will be considered in more detail at a later stage. Finally, and most significantly, the Committee considered the extent to which the storage of personal data on computer might be considered to amount to an invasion of the individual's privacy.(67) The work of the Committee in this area demonstrates a significant dichotomy between perceptions and reality and one which may remain valid today. In terms of evidence of abuse the Committee concluded that:

> "Of all the forms of invasion of privacy which have been cited in evidence to us that involving the use or misuse of computers has been the least supported in concrete terms."(68)

a view supported by Professor Westin who in evidence before a Committee of the European Parliament commented that

> "Most cases of actual harm involving individuals are still arising from manual records: these remain the places where most sensitive medical records and health data are stored."(69)

A survey of public attitudes to privacy carried out on behalf of the Committee revealed, however, that when faced with the proposition:

> "In a few years from now, it may be technically possible for details of your life, such as family circumstances, financial situation, political views and so on to be recorded on a big central computer, with any of the information being available to anyone who asks for it."(70)

87% of respondents considered that this would be invasive of their privacy with 85% believing that such conduct should be prohibited by law. These figures were greater than those achieved in relation to any other issues suggested to respondents.(71)

Although the wording of the question appears somewhat "loaded" and a high response rate might be expected it would appear to indicate a widespread perception of the

dangers of computer abuse, a perception which may be in advance of reality. An analogy may be drawn, however, between the public attitude towards the implications of automated data processing and towards the use of nuclear power. In the latter case there is clearly a widespread fear of the consequences of any accident. Whilst the justification for these fears may form a subject for expert debate their mere existence constitutes a significant factor to be taken into account in policy formulation. In the same way concern as to the privacy implications of data use undoubtedly provided an impetus towards legislation. It may be considered, however, that to consider data protection as a species of privacy may have unfortunate consequences within the British legal systems. Whilst in other jurisdictions, data protection can build upon existing privacy legislation, the absence of any general rights must have the consequence that British legislation in a particular field lacks any historical or philosophical basis. Lacking established foundations, data protection may come to be seen as an irrelevance whose strictures may be observed in the letter but whose influence will not be felt on any wider basis.

3. Data Surveillance and Individual Rights

In essence the claim to be let alone involves the

ability to lead our lives free from the surveillance of others. Surveillance may take a variety of forms. Professor Westin has identified three categories, viz physical, psychological and data surveillance.(72) All of these have long been a part of human society. Under Westin's criteria, the first two forms of scrutiny involve a degree of direct contact between the watcher and the watched. Physical surveillance may be regarded as the act of spying in order to acquire information whilst pyschological surveillance involves the assessment of information, normally supplied by the individual concerned, with a view to reaching conclusions as to his opinions or beliefs; examples might include the use of questionnaires or personality tests. Finally, data surveillance may be considered to involve the maintenance of records concerning the individual. These records may constitute the proceeds of either physical or psychological surveillance but, more often, will consist of factual or quasi-factual statements supplied either directly or indirectly by the individual concerned.

Although the application of technology serves to considerably extend the powers of those engaging in physical or pyschological surveillance, examples might include advances in the field of telephone tapping and the interception of communications and the development of 'lie detectors', the labour intensive nature of these forms of scrutiny currently restrict their

application to a minority of society. The practice of data surveillance, however, affects everyone with the development of the computer facilitating massive advances in the scale and sophistication of this form of surveillance. Very few actions do not involve the individual in giving out a measure of information about himself. This may occur directly, for example in filling in a form, or indirectly as when goods or services are purchased. This in itself does not represent a novel development; what is new is the efficiency with which this information is processed. In the past it would have been available to very few persons, for example, if goods were purchased from a shop with payment made in cash only the customer and the sales assistant would normally know the nature of the purchase. In most cases although the latter would have knowledge of the nature of the purchase they would not know the identity of the buyer and, in any event, it would be likely that they would very soon forget about the transaction. Where details of the transaction are recorded on paper, or if payment is made by cheque, the life span of the information will be considerably extended as is the possibility of its being made available to other parties. Even paper records have a limited life span and their area of publication is normally limited. If details of a transaction are recorded on computer, as is the case where a credit card is used, their life span becomes virtually indefinite and there are few technical obstacles

preventing the spread of the information. A similar situation arises in most areas of life. The problem may not be new but its significance has expanded immeasurably. It appears an inevitable consequence of the emergence of an "information society" that the informational trails which individuals leave as they move through life, trails that can tell a good deal about their life style, actions, movements and, indeed, beliefs, will become more and more extensive and the conclusions that can be drawn from the processing of the information will become more and more detailed. More and more reliance will be placed upon these records and in view of the potentially unlimited life-span of much computerised information it may become increasingly difficult for an individual to live down his past. It has been commented that

> "..the Christian notion of Redemption is unknown to the computer."(73)

In addition to the consequences following from the accurate recording of information there must also be the danger that inaccuracies will creep into records. As more and more reliance is placed on such records the consequences for an individual of any inaccuracy may be substantial.

The effects of this increase in the amount and quality of personal information available would appear to be

twofold. Firstly the information may be used to the detriment of its subjects. At this stage the problem may be seen as moving beyond the bounds of invasion of some nebulous right of privacy to encompass more tangible issues of individual liberty. If an individual is arrested and imprisoned because he is mistakenly identified on a police computer as a suspected criminal the question whether the act of recording the information constituted an invasion of a right to privacy may not be uppermost in the individual's mind. It may be argued that a distinction may be drawn between the acquisition or collection of information, actions which may well have privacy implications, the storage of the information which may affect the subject's perceptions of his status and of his freedom to think and act as he would wish and the use of the information which affects, either beneficially or detrimentally, the individual's position. Assuming that information is used to the detriment of an individual, this may come about either through deliberate design on the part of those collecting it or through social or political changes intervening to change the nature of information previously acquired. Hondius, for example, recounts how the elaborate population registers maintained by the Dutch authorities prior to the Second World War (no doubt with the best possible motives) were used by the invading Germans to facilitate the deportation of thousands of people.(74) In this case, as in any similar case it is clear that it was not

information *per se* that harmed individuals, rather it was the use that was made of it. In this sense information is a tool; but a very flexible tool, and whenever personal information is stored the subject is to some extent "a hostage to fortune". Information which is freely supplied today, and which reflects no discredit in the existing social climate, may be looked upon very differently should circumstances change. It may, of course, be questioned how far any legal safeguards may be effective in the situation of an external invasion or unconstitutional usurpation of power. In discussion of this point in Sweden it has been suggested that:

> "Under a threat of occupation there may be reason to remove or destroy computer installations and various registers in order to prevent the installations or important information from falling into enemy hands. An enemy may, for example, wish to acquire population registers and other records which can assist his war effort... There may be reason to revise the plans as to which data processing systems should be destroyed or removed in a war situation."(75)

Whilst such plans and procedures might appear to afford protection against the possibility of outside intervention it must be recognised that, in the past,

the use of personal information as a weapon against individuals has not been the exclusive province of totalitarian states. Again, during the Second World War the United States government used information supposedly supplied in confidence during the census to track down and intern citizens of Japanese ancestry.(76) More recently it has been reported that the United States Selective Service system purchased a list of 167,000 names of boys who had responded to a promotion organised by a chain of ice cream parlours offering a free ice cream on the occasion of their eighteenth birthday. This list of names, addresses and date of birth was used in order to track down those who had failed to register for military service.(77) Such practices illustrate, firstly, the ubiquitous nature of personal information and, secondly, that no clear dividing line can be drawn between public sector and private sector users as information obtained within one sector may well be transferred to the other. At a slightly less serious level it was reported in the United Kingdom that information supplied in the course of the 1971 census describing the previous occupations of respondents was passed on to health authorities who used it to contact retired nurses with a view to discovering why they left the profession and to encourage them to consider returning to work.(78) Whilst it may be argued that no harm was caused to the individuals concerned by this use of information it provides further evidence of the ubiquitous nature of

information and of the ease with which information supplied for one purpose can be put to another use.

The second effect of modern informational practices is less tangible. It is clear that individuals do modify their behaviour if they feel that they are being watched. Knowledge that details of all our actions are being recorded may well influence their nature. One aspect of this was described by the Russian author Solzhenitsyn:

> "As every man goes through life he fills in a number of forms for the records, each containing a number of questions.... There are thus hundreds of little threads radiating from every man, millions of threads in all. If all these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialised as rubber bands, buses, trams and even people would lose the ability to move.... They are not visible, they are not material, but every man is aware of their existence ...Each man, permanently aware of his own invisible threads naturally develops a respect for the people who manipulate the threads."(79)

The effect of this must be to ensure that behavioural patterns will change as individuals attempt to

demonstrate conformity with the standards expected by those in authority. Whilst it may be argued that there are many forms of behaviour which it is in society's interest to change, for example, if knowledge of an improved crime detection rate resulting from an extension of police record keeping served to deter those contemplating committing criminal offences most citizens might consider a dimunition of their privacy a small price to pay. The step from using such records to prevent crime to using them to ensure conformity in other matters is such a short one that even this equation is not as straightforward as might initially appear. All forms of planning involve a degree of prophecy but there does not appear to have been adequate discussion in the United Kingdom of the long term implications of the development of more and more extensive personal registers. The former Attorney General of the United States, Ramsay Clark, was undoubtedly correct when he stated that:

> "Few conversations would be what they are if the speakers thought others were listening. Silly, secret, thoughtless and thoughtful statements would all be affected. The sheer numbers in our lives, the anonymity of urban living and the inability to influence things that are important are depersonalising and dehumanising factors of modern life. To penetrate the last refuge of the individual,

> the precious little privacy that remains, the basis of individual dignity, can have meaning to the quality of our life that we cannot forsee. In terms of present values that meaning cannot be good."(80)

Although the words are couched in terms of the more physical acts of surveillance they are equally apposite in relation to data surveillance. It must also be recognised, however, that modern society cannot function without sophisticated information systems. Assuming that the maintenance of institutional structures is considered to be in the best interests of society generally, it is clear that there may be conflicts between the desire of an individual to be 'left alone' and the demand of government that he conform with their record keeping procedures. In this regard a distinction may perhaps be drawn between those aspects of the state which are fundamental to its very being and those which are more peripheral in their significance. In the case of the former it appears reasonable that conformity should be demanded of citizens and that necessary information may be collected, either from the individuals concerned or by other methods. Examples of this category would clearly include information held for national security purposes, for policing purposes and for revenue gathering. In the second category conformity should be seen more as a matter of agreement with the possibility

for an individual to "contract out". Examples might include health and education where the individual may choose to make provision for his own needs outside the facilities provided by the state. In both cases, however, the rights of the state cannot be seen as absolute and there is a need for controls to ensure that proper safeguards are provided for individuals and that the risks of misuse of information are minimised. In particular, regulation should specify the nature of the information that may be collected, the manner by which it may be obtained and the uses to which it may be put.

It is, of course not only the state that can pose a threat to the privacy of individuals. The private sector may also become involved in intrusions. The justification for intrusion here may be considered that those seeking information provide a facility or service which is of value to society generally and which normally is desired by the individual whose details are recorded. The relationship between the parties would thus appear to be akin to a contractual one. As with any form of contract, however, the terms may be inequitable and those wishing access to a facility or service may be faced with a choice of accepting the other parties demands <u>in toto</u> or of doing without. In particular the individual may be required to supply personal information in excess of that which is reasonably necessary in order to enable the other party

to make an informed decision whether to grant access to the facility and, secondly, the information supplied may be used for purposes unconnected with the original contract. The contractual analogy described above would also appear to break down when we consider those situations where information is held by an organisation concerning individuals who have had and who contemplate having, no dealings with them. There can be no question of agreement here the issue rather being whether, in providing a service which is generally valued by society, some degree of interference with the rights of dissenting individuals may be considered justified. In respect of all these issues there is clearly a substantial role for the law, particularly, it is submitted, in ensuring that the pursuit of the "greatest good of the greatest number" does not provide the excuse for oppression of the wishes of a minority.

In respect of information held by agencies in both the public and the private sector it appears clear that there is substantial public demand for the services and facilities that modern informational practices make available. If the price of obtaining access to the benefits of modern society is the volunteering of personal information then it seems that this is a price that many, perhaps most, people are willing to pay. Plisner comments that:

"..society seeks more services from both public

> and private organisations. From the government it expects social security, unemployment compensation...From business it seeks even more. People want charge cards that will give them instant credit approval, worldwide. They want the ability to make airline reservations, for any airplane, anywhere in the world, in minutes. Individuals are no longer content to receive a telephone bill with a "bottom line" charge; they want an itemized listing, so they can be sure they are not paying for someone else's calls. They want to be insured against all kinds of risks previously unheard of, and in larger amounts...All these increased services require that decisions be made quickly (often instantly) and efficiently; information must be available to allow those decisions to be made. And such services require that records be kept- many records."(81)

4. The Threat of the Computer

To a considerable extent the previous discussion has concerned issues whose significance was noted long before the appearance of the computer. The impact of the computer has served, however to radically change the dimensions of existing problems so that much legislation designed to secure individual rights in

this area is restricted in its application to the situation where computers are used to process data. Attention must, therefore be paid to those features of computer technology which should compel special consideration.

Computerisation permits the storage of vast amounts of information in a much smaller space than would be required by manual records. Campbell and Connor cite the example of a large record system consisting of some 100 words of information on each of 5,000,000 people. In manual form this would require storage space roughly the size of a tennis court with filing cabinets 6 feet high. By contrast should the records be maintained on computer a storage unit six foot high by four foot wide would suffice.(82) Further, computers make economically feasible much more sophisticated and extensive forms of processing than would be possible using manual systems. A major limiting factor in the development of manual information systems is the need to compile indexes relating to the information. The more complex the cross-referencing required the more complicated will be the indexes and, of course, the greater will be the space required by the system. Many computer systems operate on a free text basis obviating the need for indexes and permitting any combinations of items of information to be compared. Further it may be pointed out that whereas a particular record held in a manual system can only be accessed by one person at a

time, multiple access is easily possible with a computer. Indeed many computer data bases can be accessed at long range using the telephone system. This practice may affect not only individuals but also states with the international transmission of information having consequences for economic, political and, indeed, cultural sovereignty. The ease of transmission of computerised information also means that linkage between separate data bases becomes a real prospect providing the possibility of building up a complete dossier of every aspect of an individual's life.

The cumulative effect of these features ensures that any consideration of the the impact of modern informational practices must centre on the computer. Although in Orwell's '1984'(83) a totalitarian regime was maintained largely without the aid of this form of technology, and in real life the experiences of the Second World War indicated the extent to which state bureaucracy can be used as an instrument of tyranny, technological developments place more and more potent weapons in the hand of those in authority. It may be relevant to contrast the views of two authors whose visions of a society where individual privacy is regarded as undesirable have entered into folklore. In the 16th century Thomas More's 'Utopia'(84) presented an essentially optimistic portrayal of such a system with the demand for conformity aimed purely at securing

the best advantage for society as a whole. Utopia represented an ideal, a society to be strived for. By the 20th century in George Orwell's '1984' a not dissimilar society where individuals were watched to ensure their conformity with prevailing standards was seen as a nightmare. Although the motives ascribed to those in power may undoubtedly partially explain this transformation it may also be argued that More's human surveillance is intrinsically less alienating and threatening than the technology-driven spying of the later work.

If the individual is to be safeguarded then the technology must be controlled. At the same time, however, it is undeniable that information technology, properly harnessed, offers real and substantial benefits to society. Marcuse comments that:

> "..technology itself can promote liberty as well as authoritarianism, abundance as well as penury, abolition as well as intensification of work."(85)

We all stand to benefit from an increased rate of crime detection, many of us appreciate the ready access to credit facilities made available by the introduction of computerised data bases. However, the storage of personal information on computerised data banks offers, to some extent, "a hostage to fortune". Whilst there

can be no absolute guarantees that information will not be abused it must be the task of Government and Parliament to ensure that the advantages of technology are maximised whilst the inescapable risks are minimised.

5. The Legal Response to Informational Practices

The concerns described above relating to the impact of informational practices upon the individual have traditionally been based upon the concept that the individual's rights to privacy has been adversely affected. As such, the pressure for legislation can be seen as an offshoot from the general privacy debate. It may be considered, however, that privacy is only one factor to be taken into account in discussing this area and that an over emphasis on this point has served to impede the prospects of satisfactory legislation within the United Kingdom.

In considering informational practices three stages can be identified. The constituent data must first of all be acquired. The data will next be processed and/or stored. Finally, the data may serve as the basis for action. Whilst the manner in which the information is gathered may on occasion be considered intrusive and, therefore, to violate expectations of privacy in many cases the information will be handed over voluntarily

by an individual in order to obtain some benefit or service. The fact that information is held about an individual may have the behavioural impact described in the preceding section. In this area the assertion that privacy rights have been infringed appears to carry most weight although the actual effects of informational practices are at their least at this stage. It is at the final stage, when the data is acted upon, that the privacy connotations appear most stretched and unrealistic. If information is used to the detriment of an individual, no matter whether that takes the form of financial loss, denial of a benefit or even deprivation of liberty abstract considerations of privacy are likely to be far from uppermost in the individual's mind, his concern will be with more concrete liberties and freedoms. This argument appears to have been accepted in the French data protection statute(86) which establishes a "National Data Processing and Liberties Commission"(87) and which uses the expression "privacy and liberties".(88)

In addition to the involvement of other rights and freedoms excessive concentration upon the privacy aspects of data protection can be subjected to a further criticism. As will be discussed, a major component of legislative action involves the extension of the individual's ability to control the nature and extent of data handling concerning him. The notion of control may be regarded, however, as incompatible with

that of privacy. An illustration may be found in the medical field. Here it has been commented that:

> "Patients have quite rightly been described as a typical example of "captive populations". The need for medical help, as well as the hopes attached to medical intervention will, as the experiences with cancer registers show, regularly induce the patients to disclose all the information demanded and to agree to virtually every processing."(89)

In many cases, the purpose of legislation will be to attempt to restrict the demands which may be made of individuals in such a situation. Where the law, however, prevents or inhibits the voluntary transfer of personal data it may be the case that the extent of the individual's control is weakened but it is more difficult to envisage how his rights of privacy can be regarded as having been violated.

As concern at the societal impact of informational practices, especially with the quantitative and qualitative expansion in processing and storage facilities consequent upon the development of the computer, the demand for legislative intervention has mounted. Whilst a variety of approaches can be identified, within Europe the legislative response has initially taken the form of introducing data protection

statutes. The term "data protection" made its first appearance in legislation introduced in the German State of Hesse in 1970(90) and although it has been criticised as conveying the impression that the information rather than its subjects is to be protected the phrase has been widely copied. Although the connection between data protection and privacy cannot be denied it may also be argued that the former constitutes a wider concept in that it attempts to take account of other consequences which may result from data processing. If an individual suffers loss because a decision affecting him is taken on the basis of inaccurate information he has effectively suffered from a form of discrimination.

With the passage of the Data Protection Act in 1984 the United Kingdom joined the ranks of those states which have acted in this area. Although limited precedents existed for legislative intervention in the field of information handling the Act marks a significant development in the legal recognition of individual rights. In the following chapter the background to the Data Protection Act will be considered before detailed attention will be paid to the scope and extent of the concept and, in particular, to the extent to which the British legislation conforms with evolving international standards.

Footnotes

1. Religious Meditations (Of Heresies).

2. See, for example, Report of the Committee on Consumer Credit, Cmnd 4596 (1971) para. 9.1.16 .

3. Concise Oxford Dictionary.

4. Although the point whether any substantial distinction exists between the words 'data' and 'information' was the subject of a measure of debate during the Data Protection Act's parliamentary passage they will be regarded as synonymous for the purposes of this thesis.

5. The increasing economic significance of information as a commodity highlights the uncertainty which currently surrounds its legal status. Although it may be recognised that information, especially when its circulation is limited, may constitute a valuable asset, the courts in England and Scotland have shied away from a determination that information may be a species of property susceptible of ownership. A more liberal attitude has prevailed in other jurisdictions, see pp.331-3 *infra.*

6. Judge Brandeis in the United States Supreme Court decision of *Olmstead* v. *United States* 277 US 438 at 478. An extensive selection of definitions of privacy can be found in the Report of the Committee of Privacy Cmnd 5012, 1972. Appdx. K.

7. Report of the Committee on Data Protection Cmnd 7341, 1978. Para 4.05.

8. Cmnd 5012 *supra* p.239.

9. *Mill*. Works Vol 10.

10. *Ibid* p.142.

11. 381 U.S. 479.

12. 357 U.S. 449.

13. *Ibid* p.462.

14. *Ibid*.

15. *Supra* p.484.

16. *Ibid* p.485.

17. Ibid p.508.

18. Ibid p.509.

19. Ibid p.510.

20. 410 U.S. 113.

21. 389 U.S. 347.

22. 429 U.S. 589.

23. 403 F. Supp. 931.

24. Supra p.605.

25. The Commonplace Book (works, vol x, p.142).

26. Devlin, The Enforcement of Morals, Oxford University Press, 1962, pp.117-8.

27. Ibid p.118.

28. e.g. Semayne's Case (1603) 5 Co.Rep. 91 and Entick v. Carrington (1765) 19 St.Tr. 1029.

29. 1949 J.C. 101.

30. [1979] 2 All ER 620.

31. Ibid p.630.

32. MacCormick, 89 L.Q.R. 23 (1973).

33. Supra p.642.

34. Ibid.

35. [1978] 1 Q.B. 479.

36. Ibid p.488.

37. Ibid p.489.

38. Rodata in: Policy Issues in Data Protection and Privacy. Proceedings of OECD Seminar. Paris 24-6 June 1974. OECD 1976. P.133.

39. The Right to Privacy (1890) IV Harvard Law Review 193.

40. New York Times Co. v. Sullivan 376 U.S. 254.

41. 1868 6M 926.

42. Supra p.928.

43. The Law of Privacy in Scotland, 2 Cambrian Law Rev. 35 at 38.

44. A Short Commentary on the Laws of Scotland. TB Smith, Greens, 1962. P.733.

45. Inner House June 18 1957 (Unreported).

46. The Right to Privacy. Op cit.

47. See Walton, The Comparative Law of the Right to Privacy. 1931 LQR 203 at 220 and Report of Committee on Privacy op cit pp.308-10.

48. Cmnd 5012 supra pp.311-3.

49. Art.12.

50. Art.8.

51. Ibid Art.19.

52. Ibid Art.25.

53. The right of individual petition to the Commission became operative in 1955, that to the Court in 1958.

54. Lord Mancroft's Bill of 1961, Mr Alexander Lyon's Bill of 1967 and Mr Brian Walden's Bill of 1969 all intended to establish a general right of privacy. Additionally, Bills sponsored by Mr. Kenneth Baker and Lord Mansfield were concerned with the implications of computerised informational practices, whilst Mr Leslie Huckfield's Bill of 1972 proposed to regulate computerised and some manual information systems.

55. The Right of Privacy Bill, introduced on the 8th February 1967. 740 Official Report (House of Commons).

56. Clause 2.

57. Clause 1.

58. Introduced on the 26th November 1969. 792 Official Report (House of Commons). This Bill was withdrawn during its second reading on the 23rd January 1970. 794 Official Report (House of Commons).

59. Report of Committee on Privacy. Supra p.1.

60. Ibid p.1.

61. Ibid p.2.

62. Ibid para 665.

63. Ibid para 657.

64. Law Com No.110 Cmnd 8388 Scot. Law. Com. No 90 (1984).

65. Supra para 298-300. Similar proposals were also advanced in the Report of the Committee on Consumer Credit, op cit paras 9.1.16-9.1.28.

66. s.158-9.

67. Supra pp.177-92.

68. Ibid para 580.

69. PE 51.975/Ann 5.

70. Supra para 575.

71. See note 8 supra.

72. Information Technology in a Democracy. Harvard. 1971, pp.301-10.

73. The Computer and the Invasion of Privacy. Hearings before a Subcommittee on Government Operations (House of Representatives), 1966 p.12. Statement of V. Packard.

74. Emerging Data Protection in Europe. North Holland, 1975. P.41.

75. Transnational Data Report. Vol.1, No.5, p.17.

76. S W Peterson, Japanese Americans. New York, Random House 1971. Chap.4.

77. Transnational Data Report. Volume 10, No.4, p.25.

78. Madgwick and Smythe, The Invasion of Privacy. Pitman, 1974. Chap.7.

79. A. Solzhenitsyn, Cancer Ward, 1968 Bodley Head. P.208 (Penguin edition).

80. Crime in America. 1970. P.287.

81. Plishner, "Its None of Your Business." Or is it? California Addresses the Computer Age. Rutgers Computer and Technology Law

Journal Vol 8 (1981), pp236-7.

82. On the Record. Michael Joseph, 1986. Chap.2.

83. Martin Secker and Warburg, 1949.

84. First published in Latin at Louvain in 1516. First English translation published in 1551.

85. Some Social Implications of Modern Technology. 9 Studies in Philosophy and Social Science, p.414.

86. Act 78-17 of 6 January 1978 on data processing, data files and individuals (unless otherwise indicated throughout this thesis all translations of foreign statutes are taken from those supplied to the OECD and approved by the relevant authorities in the originating states.

87. s.6.

88. s.17.

89. Simitis, Sensitive Data - The Quest for a Legal Regime. Paper submitted to the Conference on the Problems Relating to Legislation in the Field of Data Protection. Athens November 1987.

90. Data Protection Act (Unofficial Translation by OECD. Informatics Studies No2 (1971), p.47.

The Move to 1984

1. Introduction

Although the introduction of data protection legislation is a relatively recent legal phenomenon, pressure for action to control data processing operations can be traced back to the 1960's. Whilst it is not intended in this thesis to present an exhaustive survey of the historical development of data protection legislation in general and the background to the United Kingdom Data Protection Act in particular, many of the aspects of current legislation can only be understood in terms of their historical context. To this end, this chapter will essay an account of the major factors prompting both the introduction and the format of legislation. In this regard account must be taken both of national and of international pressures. Although these were prompted by similar considerations, and ultimately converged as regards the essential components of legislation, it may be helpful to give separate consideration to both influences.

2. Domestic pressure

Reference has previously been made to the activities of the privacy lobby which prompted the appointment of the Committee on Privacy in 1970.(1) Co-terminously with

this general expression of concern, attention was given to the specific impact of computers upon the record keeping process. In 1969 the first attempt to introduce legislation in the field that was to become known as data protection was initiated by Kenneth Baker MP who introduced his Data Surveillance Bill.(2) This Bill was the precursor of several private members' initiatives in this field none of which seriously threatened to reach the statute book.(3) The Data Surveillance Bill contained many of the features which were subsequently to appear in the Data Protection Act, proposing, for example, the appointment of a Registrar and the imposition of a requirement that computer users notify him of the nature and extent of their activities.(4) Provision was also made for individuals to be supplied with a copy of information held concerning them.(5) Additionally, the Registrar would be provided with limited powers to intervene in the event that he considered specified purposes to be undesirable or that a user's activities were outwith the scope of those notified.(6)

It may be noted that, should the Data Surveillance Bill have reached the statute book, the United Kingdom would have led the world in this new area of the law. In the event the Bill's major significance would appear to lie in the fact that its existence drew the attention of the Committee on Privacy to the implications for individual privacy of computerised data handling. As

the report of this committee was heavily relied upon in the drafting of the Data Protection Act a clear link can be identified between the 1969 proposals and the 1984 Act. In view of the developments in computer technology which occurred in the intervening 15 years it may be considered that this similarity bodes ill for the success of the Data Protection Act.

The concern at the impact of computers was recognised by the Committee on Privacy which devoted a chapter(7) of its report to this topic. The committee's remit required it to:

> ".. consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies and to make recommendations."(8)

This remit, which restricted the committee's investigations to the private sector, was subsequently the source of considerable controversy with the committee itself making two requests for extension initially to the appointing Labour Home Secretary(9) and, subsequent to the 1970 general election to his Conservative successor.(10) A variety of reasons were put forward for rejecting such an extension. Significantly, one was to the effect that the

Government:

> "was considering the possibility of working out a code of conduct for the use of Government owned computers."(11)

As much, perhaps most, sensitive personal information is acquired or held by public agencies and as the justification for informational practices may vary between the public and the private sectors the restricted remit must limit the value of the Younger Committee's recommendation and perhaps cast doubt on the assumptions contained in the 1984 Act.

After receiving evidence as to the nature and scale of processing activities the committee delivered the verdict that:

> "We cannot on the evidence before us conclude that the computer as used in the private sector is at present a threat to privacy..."(12)

The potential dangers arising from computerisation were, however, recognised although the committee's conclusions were stated to be based on the premise that:

> "... we regard the computer here as a stage, albeit a revolutionary one, in the development

> of existing techniques for filing, retrieving, processing and disseminating information. We have, therefore, thought it right not to concentrate on the machines as such, but on the uses to which they are or could be put."(13)

Despite this, the committee identified three features of computer usage which caused justifiable public concern. First the storage capability of computer systems, coupled with increasingly sophisticated processing techniques, provided users with the capability to develop detailed profiles of individuals. The second potential danger may be considered closely and relates to the possibilities for the correlation of information from a variety of sources again to build up a more extensive picture of an individual. Finally, it was considered that the extensive and increasing amount of information held on computer created increased dangers for the individual's concerned in the event that unauthorised access was obtained to the data.(14)

In order to prevent these potential dangers from becoming real, the committee recommended that those holding personal information on computer should observe 10 principles requiring that:

> "Information should be regarded as held for a specific purpose and not be used, without appropriate authorisation, for other purposes..

Access to information should be confined to those authorised to have it for the purpose for which it was supplied..

The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose..

In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data..

There should be arrangements whereby the subject could be told about the information held concerning him..

The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information..

A monitoring system should be provided to facilitate the detection of any violation of the security system..

In the design of information systems, periods should be specified beyond which the

information should not be retained..

Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

Care should be taken in coding value judgments."(15)

The notion that generalised statements of acceptable practice should be incorporated in legislation is one which has been generally accepted in European data protection statutes although, as will be discussed,(16) there has also been a developing recognition of the need for the principles to be interpreted in the context of particular forms of data processing. Within the data handling field data protection principles could perhaps be considered to have a status analogous to that of the Ten Commandments. They attempt to encapsulate good information handling practice but require to be supplemented by more detailed explanations or requirements. With the possible exception of the provision relating to the supply of information to an affected individual it may be considered that compliance with the Younger principles need call for little amendment to existing procedures. The major omission from the principles is any provision relating to the manner in which information is acquired; instead the principles presuppose the holding

(1) Data subjects should know what personal data relating to them are handled, why those data are needed, how they will be used, who will use them, for what purpose and for how long;

(2) Personal data should be handled only to the extent and for the purposes made known when they are obtained, or subsequently authorised;

(3) Personal data handled should be accurate and complete, and relevant and timely for the purpose for which they are used;

(4) No more personal data should be handled than are necessary for the purposes made known or authorised;

(5) Data subjects should be able to verify compliance with these principles;

In the interests of users

(6) Users should be able to handle personal data in the pursuit of their lawful interests or duties to the extent and for the purposes made known or authorised without undue extra cost in money or other resources;

> the growth in and techniques of gathering personal information and processing it with the help of computers. Such machinery should take the form of an independent body with members drawn from both the computer world and outside"(20)

This independent body would collect information about computer practices and propose further legislative intervention.

The report of the Younger Committee was published in July 1972 and was debated in the House of Commons in July 1973.(21) Speaking in this debate, the Home Secretary studiously avoided expressing any views on the Younger proposals on computers but announced the publication, later that year, of a White Paper describing computer practices in the public sector and outlining the Government's response to the Younger recommendations.(22) In fact, setting a precedent which was to become depressingly familiar, the White Paper, entitled 'Computers and Privacy' was not published until some two and a half years later in December 1975.(23) As announced, the White Paper's coverage extended into the public sector with a supplement(24) detailing the extent of Government computer usage.

Whilst the White Paper reiterated the finding of the Younger Committee that little concrete evidence of

computer abuse existed it demonstrated a greater awareness both of the scale of the potential dangers and of the need for preventative legislative controls. By this time, five factors were identified which served to render computerised informational practices more threatening than their manual counterparts, the White Paper arguing that:

> "(1) they facilitate the maintenance of extensive record systems and the retention of data in those systems;
>
> (2) they can make data easily and quickly available from many distant points;
>
> (3) they make it possible for data to be transferred quickly from one information system to another;
>
> (4) they make it practicable for data to be combined in ways which might not otherwise be practicable;
>
> (5) because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in their records or what is happening to them."(25)

Although it was again stressed that no evidence could be found of actual abuse, the conclusion was drawn that:

> "In the Government's view the time has come when those who use computers to handle personal information can no longer remain the sole judges of whether their own systems adequately safeguard privacy."(26)

The White Paper accordingly indicated an intention to legislate in this area, the legislation having two main components. First, it would lay down standards and objectives to be met by those handling personal information.(27) In determining the content of these it was suggested that the principles suggested by the Younger Committee would serve as the "starting point".(28) Subsequent government actions have moved the report of the Younger Committee to the finishing post. Second, moving beyond the recommendations of the Younger Committee, machinery should be provided to ensure compliance with the statutory requirements.(29) It was further recognised that the topic was a novel one, that statements of general principles would require considerable extension and specification. Accordingly, it was announced(30) that a committee, the Data Protection Committee, was to be established with a remit to make detailed recommendations as to the scope of, and exceptions to, data protection legislation and

as to the form of supervisory mechanism which should be introduced.

With hindsight, the publication of the White Paper can be seen as marking a high water point in governmental enthusiasm for action in the field of data protection. This enthusiasm was certainly matched by that of the Data Protection Committee which, under the chairmanship of Sir Norman Lindop presented its voluminous report in June 1978.(31) As this report remains the most comprehensive and detailed survey of the impact of data processing activities upon the rights and liberties of the individual, its views and proposals will be considered throughout this thesis. For the moment it may be sufficient to note its proposal that a multi membered Data Protection Authority should be established.(32) Anyone using a computer to handle personal information would be obliged to register details of their activities with this authority(33) which would also be charged with ensuring compliance with seven data protection principles. These should be divided into three categories, designed to safeguard the interests of individuals, of those holding information and, finally, the wider interests of society. Thus, it was proposed, legislation should provide that:

"In the interests of data subjects

(1) Data subjects should know what personal data relating to them are handled, why those data are needed, how they will be used, who will use them, for what purpose and for how long;

(2) Personal data should be handled only to the extent and for the purposes made known when they are obtained, or subsequently authorised;

(3) Personal data handled should be accurate and complete, and relevant and timely for the purpose for which they are used;

(4) No more personal data should be handled than are necessary for the purposes made known or authorised;

(5) Data subjects should be able to verify compliance with these principles;

In the interests of users

(6) Users should be able to handle personal data in the pursuit of their lawful interests or duties to the extent and for the purposes made known or authorised without undue extra cost in money or other resources;

In the interests of the community at large

(7) The community at large should enjoy any benefits, and be protected from any prejudice, which may flow from the handling of personal data."(34)

In terms of their content these principles are not dissimilar from those advocated by the Younger Committee.(35) It is noteworthy, however, that the Lindop Committee grouped its principles into three categories; those designed to safeguard the interests of those who handle data, its subjects and, more novel, those of society as a whole. Such an approach provides explicit recognition of the validity of the various claims and interests involved in this area and attempts to provide a framework for the resolution of any conflicting claims. Recognising the nebulous nature of these broad statements of principle, the Committee recommended that they should be supplemented by the creation of a number, estimated at around 50, of statutory codes of practice targetted at, and providing detailed provisions relating to, particular users or categories of user.(36)

The report of the Lindop Committee received a lukewarm governmental reception. No official response was forthcoming until January 1979(37) when it was announced that a further round of consultations was

considered necessary. Twenty six months and a general election were to elapse before the subject of data protection was to reappear on the parliamentary agenda. In March, 1981, in response to a parliamentary question as to the government's intentions,(38) the Home Secretary announced that:

> "The Government has decided in principle to introduce legislation for this purpose when an opportunity occurs."(39)

In formulating the legislation, however, little weight was to be given to the recommendations of the Lindop Committee, the Home Secretary continuing to the effect that:

> "The Government accept as a starting point the principles formulated by the Younger Committee...Our intention is that the legislation should incorporate and so far as possible give effect to these principles. Consultations following the publication of the report of the Data Protection Committee.. showed broad acceptance of the need for some statutory control but less agreement about the machinery. One of the Government's objectives will be that our arrangements should keep costs down for the private sector and should contain those for the public sector within existing

planned totals. We do not therefore propose to set up an independent data protection authority."(40)

With a Government which had come into office pledged to cut public expenditure and reduce the numbers and influence of Quango's it was perhaps inevitable that the extensive supervisory authority envisaged by the Lindop Committee should be rejected. It was subsequently indicated(41) that although the concept of registration was to be retained, responsibility for this, and for the subsequent supervision of data users, would be vested in the Home Office. The inevitable conclusion from this must be that budgetary considerations were to take precedence over the libertarian concerns at the heart of the concept of data protection. Such a view is strengthened by the suggestion that the Home Office, which enjoys at least a measure of responsibility for some of the most sensitive computerised informational practices involving the police and national security agencies, could constitute a satisfactory public guardian against any abuse emanating from these quarters. The point must also be reiterated that although the statements of principle formulated by the Younger Committee are not radically dissimilar from those advocated by the Lindop Committee, the former's remit was restricted to the private sector. As the basis for, and justification of, informational practices differs between the public and

private sector views expressly limited to the one may not constitute the most apposite precedent for the other.

The Home Secretary's statement concluded by promising that:

> "there will be full consultation with trade associations and other bodies.."(42)

In view of the extensive consultative exercises conducted by the Lindop Committee this conclusion served to further highlight the Governmental rejection of its findings and also to cast doubt upon the priority which was afforded to legislation in this area. By this time, however, international pressure for action was growing, pressure which was reflected in domestic lobbying from commercial interests concerned at a possible loss of business in the mushrooming field of data processing resulting from the lack of satisfactory legal controls. In 1980 a letter to the 'Times' from a leading industrialist expressed concern at the situation, and called for urgent legislative action, arguing that:

> "Lack of computer privacy legislation may seriously affect our overseas trade. Of the nine EEC countries only Italy, Ireland and the United Kingdom have no laws or firm legislative

> programme. Britain is regarded as becoming a "pirate offshore data haven" by countries that have legislated on computer privacy."(43)

Continuing, he expressed concern at the possibility that privacy considerations might serve as a smokescreen for the imposition of data sanctions against the UK.

> "It is difficult to distinguish between private and commercial data when it is being transmitted between countries. It would be all too easy for foreign data inspection boards to forbid export or import of data ostensibly to protect its citizen's privacy but in reality to protect employment or revenue by restricting trade with Britain."(44)

In several well documented instances, for example, British companies had been prevented from carrying out data processing or related activities on behalf of Swedish companies owing to the Swedish authorities' concern at the lack of legislative safeguards.(45) The nature of the international pressure for action will be discussed more fully in the next section but the effect was to forge a somewhat unholy alliance between those whose concerns were with the civil libertarian impact of data processing and those data users who were concerned at the commercial implications resulting from

the absence of data protection legislation. The further round of consultations announced by the Home Secretary were speedily conducted and a White Paper published in April 1982.(46) By this time the Lindop report was reduced to the status of:

"..very helpful background information.."(47)

In one fundamental respect, however, the Governmental view had changed. Following substantial criticism of its proposal that the Home Office should operate the registration scheme the need for independent supervision of data users was recognised. The Lindop suggestion of a multi-membered Data Protection Authority was not, however, accepted, instead it was proposed to appoint a single Data Protection Registrar.(48)

A Data Protection Bill based on the provisions of the White Paper was introduced in the House of Lords in November 1982.(49) It successfully passed through this House but fell at the Committee stage in the House of Commons when Parliament was dissolved prior to the 1983 general election. An amended Bill was speedily introduced(50) by the incoming Government receiving the Royal Assent on the 12 July of the Orwellian year, 1984. Although the Act's parliamentary passage produced some heated debate, conducted largely although not exclusively on party political lines, these centred

largely on particular issues rather than on the general concepts. The timetable behind the legislation with proposals extending through the lifespan of four governments would appear to indicate that the subject enjoyed a low priority on the agenda of the major political parties. The fact that the 1984 Act is not radically dissimilar to the 1969 Bill must be a cause for some concern. Fifteen years of computer development appear to have made little impact on the legislature's consciousness and, as will be discussed in the following chapters, many of the Act's concepts could be considered obsolete or inappropriate even as it reached the statute book.

2. International Influences

In commending the first Data Protection Bill to the House of Commons the Home Secretary commented that it was designed:

> "..to meet public concern, to bring us into step with Europe and to protect our international, commercial and trading interests."(51)

Whilst undoubtedly civil libertarian concerns are fundamental to the concept of data protection it is clear from the above quotation that international pressures and the threat of economic sanctions also lay

behind the decision to legislate in this field.

In chronological terms, the first data protection statute, was enacted in the German Land of Hesse in 1970(52) with the first national statute being the Swedish Data Act passed in 1973.(53) Although similar in concept and content the motives underlying the passage of legislation within these two territories can be distinguished. The Swedish legislation has to be placed in the context of an established system of public access to information(54) coupled with the development of substantial population registers.(55) Reference has previously been made(56) to the Swedish fiscal system which considers details of each individual's income to properly be a matter of public record. The Swedish tradition of public administration may be considered as one where the state makes considerable demands upon the individual, where the right to be let alone is afforded low priority, but where a culture of openness and accountability is recognised as an essential check to prevent abuses and to promote public confidence in the activities of public agencies. The Data Act may be seen as providing for the application of these principles in the situation where information is held on computer. In view of the fact that much public information, for example that held in population registers, would also be useful to organisations operating within the private sector the extension of data protection legislation to such users

acquires an air of inevitability. If the Swedish legislation can be seen as continuing a lengthy tradition the Hessian statute must be considered more innovative being based upon an awareness, born from hard experience during the Second World War, of the extent to which the systematic acquisition and storage of seemingly innocuous items of personal information may provide a powerful weapon to a totalitarian government. In this context, data protection can be seen as a somewhat negative response to the problems of informational abuse with the immediate motive for legislation being directed specifically at computer abuse coming from the introduction of computerised data processing by the state authorities in pursuance of the administrative responsibilities vested in them under the federal constitution.(57) With the creation of such facilities being sanctioned by law the contemporaneous establishment of legislative safeguards would clearly serve to promote both operational efficiency and public confidence.

Even prior to the first national interventions pressure had been exerted for international action in this field. In addition to a concern over the extent to which the application of computer technology could serve to threaten human rights the justification for the intervention of international agencies was seen as being twofold. Firstly, on account of the international trade in computerised information it could place

impossible burdens upon multi-national enterprises were they to be required to comply with differing standards in every country in which they acquired, stored or processed data or through which they transferred such data. A second factor which appears to underpin international action lies in a realisation that, in the information age, national boundaries have become almost redundant. One nation's efforts to protect its citizens' liberties by placing restrictions upon the forms of data processing that may be carried out could easily be nullified were the data to be transferred abroad for processing. Fear of the establishment of data havens undoubtedly prompted much international action in this field.

In considering the role of international organisations in the field of data protection the activities of three bodies are of particular relevance within a European context, viz the Council of Europe, the Organisation of Economic Cooperation and Development and the European Community.(58)

In 1968 the Parliamentary Assembly of the Council of Europe addressed a request to the Committee of Ministers that they consider the extent to which the provisions of the European Convention on Human Rights safeguarded the individual against the abuse of modern technology.(59) The Assembly noted particular concern at the fact that the European Convention, together with

its United Nations predecessor, the Universal Declaration of Human Rights had been devised before the development and widespread application of the computer.

The Committee of Ministers passed this request to its Committee of Experts on Human Rights which in 1970(60) reported its view that the protection offered under existing conventions was inadequate. In particular it was pointed out that the European Convention and similar documents were based largely on the premise that individual's rights might be infringed by the actions of public authorities. The advent of the computer placed a significant weapon in the hands of private agencies.

Whilst identifying the dangers of computer abuse, the Committee's report also drew attention to the paradox whereby one person's claim to prevent or restrict the collection or dissemination of information relating to him might conflict with another's claim to be allowed access to information under the European Convention on Human Rights.(61) This provides:

> "Everyone has the right to freedom of expression. This shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."(62)

Whilst declining to express any definitive view as to which fundamental right should be afforded precedence in the situation where personal information is held on computer the Committee were of the view that individuals should be given a right to ascertain what information was held concerning them.

Subsequent to this report a further Committee of experts was directed to draw up recommendations for legislative action in this field. These recommendations were subsequently adopted by the Committee of Ministers in two separate resolutions dealing, respectively, with the private(63) and the public(64) sectors.

In respect of the private sector the Council of Europe recommended that Member States ensure that their domestic laws required computer users to comply with 10 principles. These principles were very much in line with those advocated by the Younger Committee containing a mixture of provisions placing restrictions upon the user's freedom of action and conferring rights, principally that of obtaining a copy of information held concerning him, upon affected individuals. In particular, the principles stated that:

> "1. The information stored should be accurate and kept up to date. In general information relating to the intimate private life of persons or information which might lead to

unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2. The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3. The information should not be obtained by fraudulent or unfair means.

4. Rules should be laid down or specify the periods beyond which certain categories of information should no longer be kept or used.

5. Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6. As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7. Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

8. Precautions should be taken against any abuse or misuse of information. Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.

9. Access to the information should be confined to persons who have a valid reason to know it. The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10. Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person."(65)

Similar principles were advocated where data banks operated within the public sector.(66)

The initial Council of Europe resolutions did not attempt to prescribe the means by which member states should give effect to the principles contained therein. During the 1970's, however, an increasing number of European States promulgated data protection

legislation. Following the Swedish Data Act, legislation was introduced in Norway,(67) France,(68) Denmark,(69) Austria,(70) Luxembourg(71) and on both a Federal(72) and a State(73) basis in the Federal Republic of Germany. In addition, the Portuguese Constitution,(74) coming into force in 1976, elevated data protection to the status of a fundamental human right.

As more and more countries enacted data protection legislation so the problems resulting from the international trade of information, frequently referred to as transborder data flows(TDF), became more acute. Owing to the ease with which data could be transferred using the normal telecommunications network it became feasible for multi-national companies to centralise their data processing activities in one location. This would have the effect that data relating to the nationals of one country might be processed in another. Such a practice could diminish the effectiveness of data protection legislation introduced by the first state and where the transfer of data takes place on a sufficiently extensive scale can serve to undermine the economic independence of the donor state. Particularly in the third world, transborder flows have been seen as ushering in a new era of economic colonialism.(75) Even in the developed world, however, concern has been expressed at the extent of American dominance in this sector(76). Two consequences could follow from the

export of data. In an effort to prevent evasion of its domestic controls the first state might attempt to place legal or practical restrictions upon the export of data whether on a general basis or to specified countries. Although such restrictions might nominally be imposed in order to preserve the rights of individuals the economic significance of data processing is such that a professed indication of concern for individual rights might mask motives of economic protectionism. Secondly, it would not be surprising were undertakings wishing to engage in data processing to attempt to locate a host country whose laws placed the fewest restrictions on their activities, ie who were willing to provide a data haven. It has, for example, been reported that:

> "A diversified consumer products company rented a house which straddled the border of two European countries to maintain the option of having computer tapes in the venue most expedient to management purposes."(77)

In addition to these difficulties it also became apparent that were different states to adopt fundamentally different forms of data protection legislation this could pose substantial problems for multi-national undertakings who carried out their data processing activities in a number of states.

The international problems posed by the transfer of data appear to require international solutions. Such solutions inevitably require that a balance be struck between competing and frequently conflicting interests. It has been commented that:

> "It seem to be a paradox, but nevertheless the free flow of information probably has to be regulated by international agreements in order to be kept free."(78)

In an effort to avert restrictions on the free flow of information, and in the hope of preventing major discrepancies between the national data protection laws, the Council of Europe moved beyond its earlier recommendations to sponsor, in 1981, the 'Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data'(79) (hereafter, "the Convention").

The Convention can be seen as offering a carrot and threatening a stick to member states. In its preamble the Convention reaffirms the Council of Europe's

> "commitment to freedom of information regardless of frontiers."

And proceeds to explicitly prohibit the erection of national barriers to information flow on the ground

that this would infringe the individual's right of privacy.(80) This prohibition only, extends, however, where the information is to be transferred to another signatory state. Impliedly, therefore, the Convention permits the imposition of sanctions against any state whose domestic law contains inadequate provision regulating the computerised processing of personal data. A recalcitrant state could effectively be placed in data quarantine. The standards required of domestic laws are laid down in Chapter 2 of the Convention and its requirements will be considered in detail when considering the substantive aspects of data protection.

Although the Convention provides:

> "After the entry into force of this convention, the Committee of ministers..may invite any State not a member of the Council of Europe to accede to this Convention.."(81)

it must be seen as essentially a Western European device. The work of the Council of Europe was, indeed, viewed with considerable suspicion by the United States. Here, a sectoral approach has been adopted towards legislative intervention with a variety of pieces of legislation intended to regulate specific activities identified as posing a threat to privacy. Thus the Privacy Act of 1974 regulates the federal Government's record keeping practices whilst the Fair

Credit Reporting Act of 1970 controls the activities of credit reference agencies. Additionally a number of State legislatures have passed statutes dealing with specific aspects of the problem, e.g. the Californian Information Practices Act of 1977. In one respect the United States approach can be seen as offering wider protection to the individual as legislation typically applies to all records coming within a specified category regardless of whether the information is held on computer or in manual form. Against this, the individual's rights are dependent upon whether a law has been promulgated in a particular area.

Faced with this divergence of approach the view has been expressed by several American commentators that the provisions of the Convention were motivated more by considerations of commercial expediency and economic protectionism than by a genuine concern for individual privacy.(82) In the course of a meeting of the Committee of Experts, the United States observer contrasted the sectoral approach adopted in that country with the omnibus data protection legislation envisaged under the Convention, and concluded that:

> "the draft convention appears to regulate a function, that is, it appears to regulate automated or electronic data processing and what the automated data processing industry may do with records about individuals. To our mind

> the draft convention is, in essence, a scheme for the regulation of computer communications technology as it may be applied to personal data record-keeping. The establishment and exercise of individual rights and the privacy of the individual seem to be treated in a secondary fashion .. I would note particularly that the word "privacy" is rarely mentioned in the Convention and is not included in its title."(83)

The point has previously been made(84) that the individual interests affected by computerised data processing extend beyond the realms of privacy. The omission of this word from the title of the Convention cannot, therefore be seen as proof of a lack of concern for the individual.

Although a representative of the United States was afforded observer status at the meetings of the Council of Europe's committee of experts, its major input in this area has been through its involvement in the activities of the Organisation of Economic Cooperation and Development. This organisation's efforts in the field of data protection parallel those of the Council of Europe and in 1980, the Council of the OECD agreed 'Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data' (hereafter 'the Guidelines').(85) As approved, the Guidelines are

broadly in line with proposals submitted by the United States delegation. At first glance the scope of the Guidelines appears wider than that of the Convention. The latter applies only in the situation where personal information is subjected to automatic processing whilst the latter are to:

> "apply to personal data, whether in the public or the private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."(86)

Despite this discrepancy there was close cooperation between the Council of Europe and the OECD in the drafting of their respective instruments and, insofar as substantive provisions are concerned, there is a considerable degree of overlap between the Convention and the Guidelines. Generally, though, the particular provisions of the Guidelines are less precise than their equivalents in the Convention. Thus, in relation to the question of transparency of data processing, the Convention provides that:

> "Any person shall be enabled .. to establish the existence of an automated data personal data file, its main purposes, as well as the identity and habitual residence or principal

> place of business of the controller of the file."(87)

whilst the Guidelines merely advocate that:

> "There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."(88)

The difference in approach between the Council of Europe and the OECD approaches has been explained in terms of the differences in approach existing between the civil and common law systems of law. Thus it has been stated that:

> "In the final result, although substantially similar in core principles, the Convention and the Guidelines could be analogised, albeit in a rough fashion, to the civil and common law approaches, respectively. Common law systems proceed pragmatically formulating the rules of legal behaviour as they acquire experience, while the civil law tradition tends to rely upon codification of rules in advance of

action."(89)

The true distinction between the Convention and the Guidelines is, it is submitted, more than a divergence of approach. Whilst the proposition that power - of whatever description - should not be abused is one that would find few dissenters; this initial unity will inevitably splinter should an attempt be made to define the concept of abuse and to provide mechanisms to prevent its occurrence. Although it would be naive to dismiss the existence of commercial motives as a consideration behind the Convention and although it is difficult for any international agreement to operate on any basis other than that of the lowest common denominator; the Convention does attempt to prescribe positive standards, in certain areas in advance of those which might previously have been characterised as good informational practice, coupled, albeit in an imprecise fashion, with mechanisms for their enforcement. The Guidelines, by contrast, represent little more than general exhortations to avoid informational abuse. Although the provisions of the Convention can be criticised in several respects it does provide a more satisfactory basis for the legal regulation of informational power than that of the Guidelines. The suggestion that standards can be devised in the light of experience conflicts with the fundamental tenet underlying much national action in this field, that the consequences of abuse would be so

severe that they must be anticipated and prevented.

Finally, in considering international action in the field of data protection, attention must be paid to the activities of the European Communities. In 1973 the European Commission published a report entitled 'Community Policy in Data Processing'.(90) Although this was chiefly concerned with the technical and economic issues involved it also referred to the need to protect the individual against the abuse of computers. This point was taken up by the European Parliament which, following debates in 1974(91) and 1975,(92) passed a Resolution in April 1976 in which it instructed its Legal Affairs committee to report:

> "..on Community activities to be undertaken or continued with a view to safeguarding the rights of the individual in the face of developing technical progress in the field of automatic data processing."(93)

The resulting report was published in 1979.(94) In it the Committee recognised both the dangers to individual privacy resulting from computer data bases and also the implications of divergent national provisions for the Community's competition policy and for the creation of a common market in data processing. It accordingly proposed that a Community directive be prepared:

> "..on the harmonization of legislation on data protection to provide citizens of the Community with the maximum protection."(95)

It was also recognised, however, that work was being carried out by the Council of Europe in the field of data protection and that in order to avoid wasteful duplication of effort Member States should:

> "..coordinate their efforts in all the international forums where these questions are discussed and, once the Council of Europe Convention has been signed, to work for the accession to that Convention of the greatest possible numbers of third countries subject to reciprocity."(96)

Additionally, the Commission was requested to report to the Parliament:

> "on the progress made by the Working party on Data Protection set up by the Committee of Ministers of the Council of Europe, on which it is represented as an observer, and on the circumstances in which the Community as such might become a signatory to the Convention."(97)

In the Parliamentary debate(98) which followed the

publication of this report the Commission representative expressed his sympathy with the motives behind the proposals but argued that no Community action should be taken until there was a clearer indication of progress at the Council of Europe.(99)

Despite this show of reluctance, at the close of the debate Parliament passed a resolution adopting the views of the Legal Affairs Committee and recommending the preparation of Community legislation.(100) In particular it was considered that there should be established a Community control agency to oversee transborder data flows. In respect of intra community transfers users would be required only to notify the agency but its sanction would be required for any external transfers. Over the following year, however, in response to a series of parliamentary questions,(101) the Commission reiterated its view that further study of the adequacy of the Council of Europe's Convention was necessary before Community action should be undertaken. In June, 1980 Parliament once again referred the topic of data protection to its Legal Affairs Committee.(102)

The Committee submitted its report in October 1981,(103) by which time the Council of Europe Convention had been approved. After considering the terms of the Convention, the OECD Guidelines and the laws which had been adopted in several Member States of

the Community the view was taken that there remained a need for Community action as:

> "the Council of Europe Convention represents, admittedly, the most far-reaching arrangement at international level for instituting or harmonizing data protection legislation in the signatory states, but it falls short of the European Parliament's ideas to date on the Community provisions required."(104)

In particular it was argued that:

> "many of the provisions of the European Convention for strengthening data protection are only optional and permit restrictions by individual states."(105)

In subsequent Parliamentary debate(106) the Commission restated its view that the Member States should sign and ratify the Council of Europe Convention pointing out that it had addressed a Recommendation to Member States(107) to this effect during 1981(108). Whilst recognising that the Convention laid down minimum standards, the difficulties facing Community action were stressed with particular reference being made to the limited manpower available to the Commission and the possible problems in securing the agreement of the Governments of all Member States to such an initiative.

It is perhaps somewhat surprising that, in view of the lengthy period over which the data protection debate had been conducted throughout the European Community and in view of the previous activities of the Commission and its encouragement of Parliament's previous initiatives that shortage of resources should at this point be put forward as a stumbling block to legislation. It does appear, however, that the Commission's lukewarm response has effectively served to terminate any immediate prospect of Community action in the field of data protection, although the Parliament passed a resolution in 1982(109) calling upon the Commission to prepare a Directive providing the individual with a superior level of protection to that contained in the Convention. The Parliament's initiatives in this field may, however, be considered indicative of evolving standards in this area suggesting that the minimalist approach favoured by the United Kingdom authorities may not be considered acceptable on a long term basis.

3. The Data Protection Act

The chronology of events surrounding the introduction of the Data Protection Act indicates the variety of objectives and motives underlying its passage. The continuing national and international debate concerning the appropriate legal response to the problems

resulting from modern informational practices has resulted in a measure of agreement as to the need for some form of legislative intervention but less as to its proper scope and content.

Initially, in this thesis, consideration will be given to the scope of the concept of data protection and the question which users should be regarded as coming within the scope of legislation. Imposing substantive requirements upon data users cannot, in itself, be considered a satisfactory response to the problems arising in this area. Standards require to be enforced and considerable debate surrounds the manner in which this should be accomplished. Given that the legislation is intended to benefit individuals, it may be argued that they should be expected to act in their own cause. Against this, the operations of data users, both in the public and the private sector, have implications for the whole of society. Protection of the general interest cannot satisfactorily be delegated to individual initiatives and the need has been identified for the establishment of some form of public supervisory agency. The nature of such an agency and its relationship with government has proved one of the key issues within data protection.

For the purposes of this thesis, attention will be focused primarily upon the United Kingdom's Data Protection Act of 1984. This will be considered from

two perspectives, first the question whether its provisions comply with the requirements of the Convention and, second, the intrinsic merits of its various provisions. In attempting to assess this latter issue account will be taken, where relevant, of the legislative provisions applying in other member states of the Council of Europe.

Footnotes

1. Cmnd 5012. See pp.28-9 Supra.

2. 783 Official Report (House of Commons) Col 288 (May 6, 1969).

3. The Control of Personal Information Bill, 822 Official Report (House of Commons) Cols 487-502 (July 27,1971) introduced by Mr Leslie Huckfield and the Data Protection Bill, 16 Official Report (House of Commons) Cols 291-3 ((January 20, 1982) introduced by Mr Michael Meacher.

4. Supra clause 1.

5. Ibid.

6. Ibid.

7. Supra Chapter 20.

8. Ibid para 1.

9. Ibid para 4.

10. Ibid para 5.

11. Ibid para 4.

12. Ibid para 619.

13. Ibid para 573.

14. Ibid para 582.

15. Ibid para 591-600.

16. Infra pp.491-3.

17. For example, the doctrine of breach of confidence serves to limit the uses to information may be put by its recipient whilst the law of defamation provides a remedy for an individual who is harmed by the dissemination of false information.

18. Supra paras 601-3.

19. Ibid paras 604-612.

20. Ibid para 621.

21. 859 Official Report (House of Commons) 13 July 1973.

22. Ibid Col 1956.

23. Computers and Privacy. Cmnd 6353. Although the White Paper was issued under the imprimatur of the Home Office it was largely the work of an outside consultant, Mr Paul Sieghart, who was later to serve as a member of the Committee on Data Protection.

24. Cmnd 6354.

25. Supra para 6.

26. Ibid para 30.

27. Ibid.

28. Ibid para 33.

29. Ibid para 30.

30. Ibid para 31.

31. Report of the Committee on Data Protection. Cmnd 7341. Owing to delays at the printing stage the report was not published until December 1978.

32. Ibid para 20.21.

33. Ibid para 19.62.

34. Ibid para 21.09.

35. Supra pp.62-4.

36. Supra para 19.26.

37. Speaking on behalf of the Home Secretary, Lord Boston, a Minister of State at the Home Office announced to the conference Computers, Records and the Right to Privacy, organised by the National Council for Civil Liberties and held in London on 24-25 January 1979 the Government's view that "The report raises questions with very wide implications for people in this country .. we intend to give all those a reasonable - not protracted - opportunity to give their views .. We expect to be writing to the main interested bodies in the next two weeks to offer their comments before the end of April." (Transnational Data Report Vol.1 No.8 p.3.)

38. 1 Official Report (House of Commons) Col 161 (March 19, 1981).

39. Ibid.

40. Ibid.

41. Although no parliamentary statement was made concerning the government's intentions, a number of comments were made on this point. See, for example, Transnational Data Report Vol.4 No.8 p.3.

42. Supra.

43. The 'Times', 3 March 1980.

44. Ibid.

45. See, for example, Bing, A Decade of Computers and Law. Universitetsforlaget, 1980, pp.70-1 describing how British companies lost contracts involving the processing of health and financial data relating to Swedish citizens because of the lack of satisfactory data protection legislation.

46. Cmnd 8539. An alternative explanation has been proferred for the appearance of the White Paper at this time. In February the 'Sun' newspaper published a feature on the Labour MP Michael Meacher. At that time Mr Meacher was standing for election to the post of deputy leader of the Labour Party. As part of their investigations they hired a private detective with instructions to gather as much information on his personal life as possible. The detective subsequently obtained access to the MP's health record, copies of his bank statements and other items of sensitive information. As none of the information obtained proved to be detrimental the story was published as an expose of the extent to which unauthorised access could be obtained to personal information.

Subsequent to the publication of this feature Mr Meacher took the opportunity to question the Prime Minister in the House of Commons:

"Is the Prime Minister aware that for a mere £500 snoopers will be able to obtain private and confidential information from personal, medical, financial or police records on her or on any Member of the House or indeed any citizen of this country? Is that not utterly wrong? Will the Prime Minister give a guarantee that

the Government will not only introduce a White Paper on this subject, but will also legislate on this matter within the next 12 months?"

The response was unequivocal, the Prime Minister responding that she:

".. saw the newspaper report this morning. I share the hon. Gentleman's distaste that this information should be available. My right hon. Friend the Home Secretary will be introducing a White Paper this year. We agree that legislation is urgent. I hope that it will come forward in the next Session of Parliament." Official Report (House of Commons) Cols. 857-8 (9 February 1982)

As the only White Paper and the only legislation remotely connected with the MP's complaint appeared in the field of data protection it must be assumed that such action was regarded as satisfying the Prime Minister's undertaking. It is noteworthy, however, that most of the intrusions to Mr Meacher's privacy appear to have centred around unauthorised access to manual records. As such, the Data Protection Act does nothing to minimise the possibility of further exposes of the private lives of MP's.

47. Supra para 4.

48. Supra paras 9-11.

49. 437 Official Report (House of Lords) 21 December 1982 Col 926.

50. 443 Official Report (House of Lords) Col 21.

51. 40 Official Report (House of Commons) Col. 562 (April 11, 1983).

52. Data Protection Act. This Act was initially replaced by the 1976 Act of the same name which, in turn was repealed by the 1986 Act.

53. Data Law. This statute was amended in 1976.

54. See Galnoor, Government Secrecy in Democracies, Harper 1977, pp 257-9.

55. See Hondius, Emerging Data Protection in Europe, North Holland 1974, pp 44-5.

56. See p.6 *supra*.

57. *Hondius op.cit.* p 35.

58. Reference should also be made to the studies carried out by other international organisations such as the United Nations and the International Bureau of Informatics and regional organisations such as the Union of American States. To date, however, these efforts have failed to bear fruit.

59. Recommendation 509/1968.

60. DH/EXP (70) 15.

61. This Convention was opened for signature on and entered into force on the 3rd September 1953.

62. *Ibid* Art 10.

63. Resolution (73)) 22.

64. Resolution (74) 29.

65. *Supra* Annex.

66. *Supra* paras 1-8. The two documents are not identical in their terms. Once again, the number of the principles varies, ten in the former document and eight in the latter.

67. Personal Data Registers Act 1978.

68. Data Processing, Data Files and Individual Liberties Act 1978.

69. Private Registers Act 1978, Public Registers Act 1978.

70. Federal Act on the Protection of Personal Data 1978.

71. Act Organising the Identification of Physical and Legal Persons by Number 1979, Act Regulating the Use of Nominal Data in Electronic Data Processing 1979.

72. Federal Data Protection Act 1977.

73. In general terms, the provisions of state legislation are concerned with data processing within the private sector and processing carried out by or on behalf of the state authorities.

74. Article 35.

75. Transnational Data Report Vol.3, No.4 p.32 (1980).

76. Cundliff, Issues in Canadian/US Transborder Data Flow. Computer Decisions August 1978 p.1.

77. Patrick, Privacy restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines, Jurimetrics Journal, Summer 1981 405 at 406.

78. Freese, Transnational Data Regulation: the Realities. Online Conferences, 1979. P.7.1.

79. The Convention was opened for signature on January 28, 1981 and entered into force on October 1, 1985 upon receiving its fourth ratification.

80 Ibid Art.12(2).

81. Ibid Art.20.

82. See, for example, Epperson, Contracts for Transnational Information services; Securing Equivalency of Data Protection, 22 Harv. Int'l. L.J. (1981) 157 at 159.

83. Text of United States Department of State Telegram, quoted in Transnational data Report Vol 1 No 7 p22 at 23.

84. Supra p.37 et seq.

85. The Guidelines were approved at the meeting of the Council held on September 23, 1980.

86. Ibid para 2.

87. Supra Article 8.

88. Supra Para. 12.

89. Kirsch, The Protection of Privacy and Transborder Flows of Personal Data: the Work of the Council of Europe, the Organization for Economic Co-operation and Development and the European Economic Community, Legal Issues of European Integration, 1982, 21 at 45.

90. SEC (73) 4300 Final.

91. OJ Debates No 179 p.55.

92. OJ Debates No 186 p.256.

93. OJ No C100/27.

94. PE 56.386/fin Doc 100/79.

95. Ibid p.6.

96. Ibid p.7.

97. Ibid.

98. OJ Debates No 245 p.19.

99. Ibid p.20.

100. OJ No C140/34.

101. See, for example, OJ No C86/26, C245/15, C255/16, and C283/20.

102. EP Doc 1-116/80.

103. PE 70.166/fin EP Doc 1-548/81.

104. Ibid p.32.

105. Ibid.

106. OJ Debates 1-281/18.

107. OJ Debates 1-282/6.

108. OJ 1981 L246/31.

109. OJ 1982 C87/37.

Chapter Three

The Scope of Data Protection

The Scope of Data Protection

In the opening chapter, the concept of data protection was identified as a major part of the legislative response to the threats to individual rights and freedoms perceived as arising from the use of the computer for data processing purposes. Although the involvement of international organisations such as the Council of Europe and the OECD and the negotiation of international agreements has served to bring a measure of uniformity to the various national initiatives in this field, there remains considerable debate and dispute as to the extent to which the law should seek to regulate informational practices and as to the form which such intervention should take.

A variety of issues arise in considering the scope of data protection. Chief amongst these are questions as to the forms of activities which should be regulated and as to the means by which compliance with the substantive requirements of the law should be monitored and secured. To a considerable extent, these issues are interdependent. A decision as to the range of activities to be regulated will affect the number of parties who will come within the statute's province and will, in turn, determine the level of supervision which may be practicable.

In considering the scope of legislation the first topic to be considered concerns the question whether provisions should be restricted to the situation where information is held on computer or whether, at least some, manual record systems should be included. As was stated in the opening chapter,(1) the argument for establishing a regime regulating solely computerised data banks is based upon considerations of the increased potential for the abuse of individual rights which may arise where information is stored and processed upon computer. Against this it may be argued that we live in an "information society". Although the creation of such a society may have been fuelled by the arrival of the computer in terms of the significance of informational practices for the individual's quality of life it has become largely irrelevant whether a computer is involved. On this argument, the law should look at the ends to which information is put rather than to the means by which this is achieved.

This latter approach has been adopted to a considerable extent within the United States where a variety of federal and state statutes attempt to regulate specific aspects of informational practices. The best known example is perhaps to be found in the Privacy Act of 1974 which establishes a right of individual access to a variety of records held by federal agencies.(2) These rights are unaffected by the fact whether information is held manually or as part of a computerised system. A

similar approach was adopted under the British Consumer Credit Act of 1974, a statute which, within its limited sphere of application (credit reference agencies), can be seen as a precursor to the Data Protection Act. As the 1970's progressed, however, an increasing tendency could be identified within Europe(3) to enact legislation targetted at data banks regardless of the purpose for which the information was held. In some cases, the legislation is restricted to the situation where information is held on computer but, in others, portions apply to specified forms of manual records. The divergence of approach within the European countries is reflected in the wording of the Convention. This requires that signatories apply its provisions:

> ".. to automated personal data files and automatic processing of personal data in the public and the private sectors."(4)

for the purposes of the Convention, personal data is defined as:

> ".. any information relating to an identified or identifiable individual."(5)

whilst automatic processing is to include the following functions:

> "..[the] storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination."(6)

when these are carried out wholly or partly by "automated means".

It is further provided, however, that signatory states may declare, either at the time of signing or subsequently, that they:

> ".. will also apply this convention to personal data files which are not processed automatically."(7)

Despite strenuous lobbying the British government insisted that the Data Protection Act should not apply to manual records. The Act's application, accordingly, is restricted to the situation where "personal data" is:

> ".. processed by equipment operating automatically in response to instructions given for that purpose."(8)

These phrases are almost identical to those found in the Convention. For the purposes of the Act it is provided that "personal data" is to consist of:

> ".. information which relates to a living individual who can be identified from the information, including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual."(9)

The data will be processed when any of the following operations are carried out by reference to the individual:

> ".. amending, deleting or re-arranging the data or extracting the information constituting the data."(10)

It will be recognised that in neither the Convention nor the Act is there specific reference to computerised processing. Indeed, in the Act the word "computer" is only referred to tangentially.(11) The absence of a definition is no accident. Whilst it is clear that the legislation is intended to regulate the use of the computer the question; "What is a computer?", is one that admits of no easy answer. This point can be best illustrated by reference to the provisions of the Police and Criminal Evidence Act 1984, a measure which passed through Parliament coterminously with the Data Protection Act. As originally introduced this defined a computer as;

> "..any electrical device for storing, processing and retrieving information."(12)

Although this definition appears exceptionally broad it was considered that it offered too great a hostage to technological progress. Research is currently taking place into the possibility of producing chemical or biological computers. Such devices would not rely on electronics in order to perform their functions. Ultimately, the view was taken that the Act should eschew any attempt at definition, the Minister of State commenting that:

> "Ossifying a definition of "computer" on the face of a bill at the present stage of technological development might in the medium term, and possibly in the short term, be more of a nuisance than an advantage."(13)

Whilst the refusal to essay a precise definition as to the subject matter of the legislation may be considered a reasonable response the result provides a graphic illustration of the problems encountered by the law in attempting to regulate fast evolving technology. The approach further has the result of ensuring that a potentially vast number of items of equipment are likely to be caught by the statute. Disregarding the few forms of non-computerised automated equipment which may come within the Act's province virtually every form

of computer will be capable of processing personal data. In 1987, the 'Sunday Times'(14) reported the concerns of educational authorities at the marketing of "computerised wristwatches" which would be capable of storing the equivalent of some 500 words of text any portion of which could be recalled "at the discreet touch of a button". Assuming that the stored text related to a living individual and that it could be recalled by reference to that person then the Act will apply and the owner of the watch will be required to register and comply with the data protection principles. Again, an electronic "calculator" is being marketed for less than £20 which provides, additionally, the facility to store "over 2,000 characters of personal data."(15) The publicity material specifically states that the device can be used as a "directory of names and addresses" with the facility to select a name or address required "and go straight to it". Clearly, putting the device to such a use will constitute processing of personal data. If reference is made to the justifications put forward for the introduction of legislation targetted specifically at computer users it will be recalled that these related largely to the increased scale of record keeping made feasible and as to the possibilities for data to be transferred from one system to another. It is difficult to conceive how the fact that 2,000 characters of information (equivalent to perhaps a page of text) can pose such a threat to individual liberties

as to require a special regulatory regime when even the largest manual system of records is regarded as innocuous. Accepting the difficulties of definition faced by the legislature, the scope of the Act appears excessive and likely to discredit rather than advance the concept of data protection.

Even without taking account of devices such as the watch and the calculator described above, it has been estimated that some 1,500,000 business computer systems will be installed by the end of the decade.(16) This explosion of numbers was not anticipated by the pioneers in the computer industry. One early authority, indeed, expressed the view that the requirements of the UK could be met with one computer. By 1973, the latest figures available to the Younger Committee indicated that some 6,075 computers were either at work or on order in the UK.(17) In 1978 when the Lindop Committee recommended the introduction of a system of registration for data users even though this figure had increased substantially, the age of the micro computer was only dawning.(18) Although, numerically, the majority of computers in use may be classed as personal computers whose processing power is comparatively small by modern standards, and although many of these devices may be used purely for recreational purposes the fact remains that even the smallest modern computer has a processing capability not greatly less than that of the largest computer in use during the early 1970's when

the basic data protection principles were being formulated. At that stage it was comparatively easy to consider the computer per se as a threat. Today, it will be argued, a more selective approach is required.

Although it may be accepted that even the most basic form of computer is capable of processing data as defined in both the Act and the Convention two further requirements will have to be satisfied before the legislation will apply. Firstly, the processed data must constitute personal data, i.e., relating to a "living, identifiable individual".(19) This definition, and the interpretation placed on it within the legislation, raises a variety of issues of considerable importance requiring detailed analysis. Secondly, the processing must be carried out by reference to the individual concerned.(20)

In considering the requirement that an individual be identifiable it is significant to note that this does not require that the subject be referred to by name on the computer record. It will suffice if the user possesses other, identifying, material even though this is not held on computer. An example of this might be seen in the case of a computer system which is designed to log telephone calls emanating from particular premises and which indicates the extension used. If the computer record merely details the source and destination of the telephone call no individual can be

identified from that record. If each telephone extension is the responsibility of a particular individual, however, and the user has a list - perhaps in the form of a telephone directory - of names and extensions then particular individuals will be identifiable from a combination of the computer and the written record. In such a case the Data Protection Act may well apply to the computer system. The application of the Act may extend even where most extensions are shared by two or more individuals. In these cases there can be no identification of the particular individual who made a particular call. If only one person in an entire undertaking, however, has exclusive use of a telephone extension then the requirement for the Act's application will be satisfied. No distinction is drawn between the situation where information relating to one living, identifiable individual is processed and that where computerised records are maintained on the entire population of the country.

A similar comment may be made concerning the requirement that information relate to living individuals. A data user may process as much information as he might wish relating to deceased individuals without being required to register. Should, however, one individual remain alive registration will be necessary. Should, for example, a data user wish to place on computer details of all birth certificates issued in the period up to 1875 he may feel reasonably

confident that the vast majority of data subjects would be deceased. If this is indeed the case then the Act will not apply but only one example of extreme longevity will be required in order to change the situation.

Two further questions arise from the definition of personal data. It has been stated that an individual may be identified from other information which is in the possession of the data user. Possession would appear to require some degree either of ownership or of physical control. This criteria would appear susceptible to two objections. Firstly, it may offer a loophole for data users who wish to avoid the requirement to register by placing information and identifying codes on their own computer, ensuring that individuals could not be identified from that information alone, and making arrangements with another computer user to the effect that the linking information will be held by him - either in written form or on computer - with provision for the first user to be allowed access to these details as and when required. It would even be possible to arrange that the user's computer would automatically be able to interrogate another computer, perhaps located in another country, whenever it was desired to link information and identity. The problems in this area may be more directly applicable in the field of subject access than in relation to the requirement to register

but it may be that a user could, by entering into an agreement of the kind described above, ensure that he never came to possess the linking data.

Assuming that an individual can be identified by a data user, a distinction is drawn between factual information relating to that individual, statements as to the user's opinions of the individual and those referring to any intentions held by the user towards that individual. The Act provides that the phrase "personal data" is to include:

> "any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual."(21)

The justification for such an approach appears somewhat obscure despite the subject being extensively debated in Parliament. Arguing in favour of exempting statements of intention from the definition of personal data the Minister of State at the Home Office commented during the Committee Stage that:

> "We do not regard the intentions of one person in respect of another as being personal to that other person. If they are personal at all, they are personal to the holder of the intention."(22)

Whilst there is force behind this analysis it may be argued that similar considerations apply in respect of statements of opinion. Indeed, in terms of the impact upon the data subject, it is submitted that the action of forming the intention to behave in a particular way is a stage in advance of the formation of an opinion. Once again the point assumes crucial significance in the area of subject access, but there appears little logic in a situation where an individual can be told what a user's opinion is concerning him but not receive details of any intentions that the user may have formulated towards him. In justifying their approach the government argued that;

> "There are some intentions that it would be unreasonable for a person to divulge, and a good example involves personnel.....I am told that it is common practice to plot senior staff changes some years ahead as an aid to managerial planning. A user may hold on computer the information that he believes that in five years time X should fill such and such a job, Y another job and Z yet another job. A month later, the scene could change and anyone who saw the original intentions would have been seriously misled. That persons motivation and morale might have been seriously damaged."(23)

Much the same argument would appear to apply in respect

of statements of opinion in personnel records. These may change with time and with further evidence becoming available to the user. The wording of the Act itself serves to further destroy any logical distinction between statements of opinion and intention. In the example quoted above the data referred to the user's future intentions. When asked whether the exemption would also be applicable to the situation where intentions had been held but where the situation in which it was envisaged that they would be put into effect had passed the Governments initial response was a clear negative:

> "I have no hesitation about this because clause 1(3) says that:
>
> > "any indication of the intentions of the data user"
>
> are excluded from the scope of the Bill. That cannot be read as an indication of five years ago when the person applies for his rights under the Bill."(24)

By the time of the Committee's next session this view had been changed with the Minister remarking that:

> "A famous judge, Lord Bramwell, once said that the matter did not appear to him now as it

> appeared to have appeared to him then. I have had an opportunity of considering this matter...I have taken some persuading, but having spent a great deal of the past two days having conversations with officials and correspondence with the parliamentary draftsmen, I must tell the Committee at this late hour that I am firmly persuaded that there is nothing in the wording of subsection (3) to suggest that any indication of the data user's intention is not apt to cover even an indication that an intention was once held by him."(25)

It would appear that this latter interpretation is in conformity with the wording of the Act which contains no reference to time. Such an approach serves to destroy the initial rationale behind the provision. It is clear that no immutable distinction can be drawn between statements of opinion and those referring to intentions. Any categorisation can only be made on the basis of semantics as opposed to sentiments; a situation which serves only to place additional burdens upon those users who wish to comply with the requirements of the Act whilst allowing considerable scope for evasion by those whose motives are less altruistic.

Whilst much data may fall to be regarded as personal

data, in order for the legislation to apply it is necessary that this should be processed by reference to the individual concerned. Once again, this may be considered a definition which is apposite in relation to traditional forms of record keeping but which may be less appropriate for the computer age. Making reference to those operations which may be taken to constitute processing by reference to an individual the Data Protection Registrar has advised users that:

> "For the present you should consider that any personal data are processed by reference to a Data Subject if your equipment can be instructed to locate automatically information about the individual concerned and you use, or intend to use, that facility.
>
> Where you are deliberately keeping data on an individual and your equipment has the facility described there seems little doubt that you will use or intend to use it and will therefore be processing by reference to the Data Subject. This could be expected to be the case even though the data may be only one of a number of fields within a record which is kept for a purpose not primarily concerned with the individual in question (e.g. the name and address of a policy holder's doctor in a record concerning a life insurance policy).

> On the other hand you, may, without specific intention, accumulate data on individuals at random within records which are apparently unconnected with those individuals (e.g. names appearing within the text of a series of stored magazine or newspaper articles). It may require certain facilities (e.g. word search) which you do not use or intend to use to locate automatically these data. In this case you would not be processing by reference to any of the Data Subjects concerned."(26)

It is not required that the act of processing be carried out by reference to a single individual. It will suffice if it is conducted by reference to some attribute that may be shared by a number of data subjects. The Registrar has indicated, for example, that should the data held on a computer include reference to the hair colouring of individuals and the computer be instructed to compile a list of ~~of~~ all the red haired people on file, this would be regarded as constituting the processing of personal information, the processing in this case being carried out by reference to all of the individuals whose details are extracted from the computer.(27)

Once again, it is submitted, technology may serve to render the Act's definition obsolete. Traditionally, processing of the kind referred to by the Registrar has

required an element of forward planning with data being divided into appropriate fields. The layout of the data base will normally be indicative of the user's intentions. With the development of full text data bases(28) this element of predestination is lacking. Invariably, a program permitting free text retrieval will have the technical capacity to permit the extraction of personal information by reference to the data subject but it will be more difficult to gauge the user's intentions. As will be discussed later,(29) the Registrar's investigative powers are limited and, in particular, he has no power to require that a user respond to any enquiries that he might wish to make. It may be considered that free text retrieval systems pose a particular problem for individual liberty. Whereas with a field based system, information has to be subjected to a degree of scrutiny prior to being placed on the data base in order to determine its location therein, this preliminary processing is not necessary with a free text system. It may even be that, through the use of an optical character reader, there will be no need for the data to be inputted manually. Unverified and inaccurate information may thus be considered more likely to appear on the data base thereby increasing the possibility that its use may be to the detriment of the data subject.

In considering the scope of data protection legislation the point must be constantly borne in mind that the law

attempts to regulate the uses to which information and technology is put rather than the information or the technology per se. The ownership of numerous computers all possessing sophisticated processing facilities will not bring the legislation into play unless and until personal data is processed. In deciding whether this criteria has been satisfied, the United Kingdom legislation generally adopts an exceptionally broad approach. Although the distinction between statements of opinion and those of intention appears to introduce an element of unnecessary complexity into the situation the legislation will apply as soon as a single item of data is processed. Whilst several other states have imposed a requirement that data must be stored in a systematic fashion or as part of a file(30) such an approach runs the risk of being rendered obsolete by developments in storage and retrieval techniques such as the full text retrieval systems described above. A price has, inevitably, to be paid for such broad coverage. The definition adopted under the Data Protection Act makes neither a quantative nor a qualitative judgment concerning the societal impact of processing and is equally applicable to the most simple and to the most sophisticated computer system. Given the explosion in the computer population, a vast number of applications are certain to come within the province of the legislation. As with most rules, however, the impact of data protection legislation is invariably subjected to a number of exceptions the extent and

rationale of which will be considered at a later stage.(31) In the following section consideration will be given to the initial obligation which may be imposed upon data users, that of seeking the permission of a supervisory agency to commence or to continue data processing activities.

2. Supervision of Users

In the previous section one of the consequences of the enormous expansion in the numbers of computers was identified; namely, that any legislation in this area is likely to affect a considerable number of persons. The question inevitably arises how their compliance with the legislation's requirements can best be assured. It may be argued that, as data protection legislation is primarily intended to protect individual's interests, responsibility for securing these should be left to those same individuals. An alternative approach proposes the establishment of a public supervisory agency. As will be discussed the existence, form and role of such an agency constitutes one of the most controversial aspects of data protection.

3. The Supervisory Agency

Within Europe the establishment of a public supervisory agency has come to be regarded as an essential feature

of legislation. It must be noted, however, that the Convention does not specifically require the creation of such an agency, contenting itself with the requirement that signatory states render each other assistance in the implementation of the Convention.(32) To facilitate this it is further provided that:

> "..each party shall designate one or more authorities, the name and address of which it shall communicate to the Secretary General of the Council of Europe."(33)

Although this requirement could be complied with through the nomination of an existing body, (and, indeed, at one stage it was proposed that the Home Office should perform this function(34)) all signatory states have established a specialist agency with the remit to supervise the compliance of data users with the requirements of the legislation. This approach has been justified on the basis that:

> "Data protection presupposes .. the establishment of an independent control authority. Experience confirms what was already stated in the earliest debates: It is not enough to trace a mandatory framework for data processing. The legislator must also secure the monitoring of the processing conditions. Neither the participation of the data subject

> nor any of the traditional means of control guarantees, however, adequate supervision. Even if the data subject is entrusted with a series of rights he remains an outsider, deprived of the necessary information permitting him to analyze and to evaluate the activities of the various public and private agencies."(35)

This view conflicts with the prevailing attitude in the United States where a more frontier orientated mentality places responsibility for his own protection upon the individual. It has thus been commented that the:

> "US approach towards privacy protection is designed to put the individual in the centre of the action, to let him have a large voice in decisions as to what information will be collected used and disseminated about him. The Europeans take a paternalistic approach choosing to vest enforcement in bureaucracy."(36)

In part this view may arise from the sectoral approach adopted in the United States. Here, the legislature identifies particular categories of information and, more significantly, particular relationships, where the results of information handling, whether by computer or otherwise may prove detrimental to an individual's

interests. Because of the limited application of the law and because the sectors of application are considered to be those which are especially important or sensitive it may not be unreasonable to expect an individual to ascertain and pursue his rights. Additionally, the question of the accessibility of the courts has to be considered. In this respect the Lindop Committee commented that:

> "There are substantial differences between the UK and the USA in the usefulness of a right to initiate legal process in the courts. The risk to a litigant in the UK of having to pay not only his own but also his plaintiff's costs (the "indemnity rule") forms a powerful disincentive to litigation, especially in view of the limited eligibility for legal aid. The indemnity rule does not apply in the USA and plaintiff's lawyers there are also allowed to charge contingency fees whereby they are paid only out of damages recovered."(37)

Even within the United States, however, there appears to be a growing awareness of the fact that it is not sufficient for the legislature merely to grant rights to the individual but that, at least in the public sector, there is a need to monitor compliance with these. Thus Miller, whilst recognising the historical suspicion of administrative bureaucracy, has commented

that:

> "..administrative regulation has fallen into considerable disfavour in the United States because it frequently has taken on a highly bureaucratic character. All too often administrative action has become synonymous with delay, red tape, and arbitrariness, with the hoped for supervision by an informed cadre giving way to the reality of politicized administrators who have little understanding of the complex problems left to their governance. The situation frequently is made worse by inadequate staffing and funding which prevent most agencies from acquiring the expertise necessary for rational decision making."(38)

Equally, he accepted the need for a specialised regulatory agency to operate in the area of computerised data banks. He proceeded to argue further that this task could not adequately be fulfilled by any existing body stating that:

> "Testimony indicating that agency personnel- admittedly few in number- systematically engage in mail cover operations, electronic bugging, wiretapping, harassment of citizens and other invasions of privacy demonstrates that governmental officials who deal with personal

> data often become too orientated toward the objectives of their own institutions or too vulnerable to pressures from other organizations (both inside and outside government) to be entrusted with primary responsibility for preserving the privacy of others."(39)

Further support for public intervention within the United States became apparent during the passage of the Privacy Act of 1974 when the Senate Committee on Government Operations(40) advocated the creation of a Privacy Protection Commission arguing that:

> ".. effective legislation must provide standards for and limitations on the information power of government. Providing a right of access and challenge to records, while important, is not sufficient legislative solution to threats to privacy .. it is not enough to tell agencies to keep and gather which is reliable by their rights and for whatever they determine is their intended use, and then to pit the individual against government, armed only with the power to inspect his file, and the right to challenge it in court if he has the resources and the will to do so."(41)

Within the United Kingdom there has been a developing recognition within the field of consumer protection that the creation of individual rights and remedies may provide an inadequate response to the dangers of abuse in a particular area. In general terms, it has been commented that:

> "No consumer legislation, however sophisticated, is likely to have more than a marginal impact if not under-pinned by effective enforcement machinery."(42)

A variety of enforcement techniques have been adopted, thus statutes such as the Trade Descriptions Act, 1968, provide for criminal sanctions to be imposed, the Consumer Credit Act, 1974, introduces a system of licensing whilst the Fair Trading Act,1973, vests administrative powers in the Director General of Fair Trading.

Within the field of data protection there has been, both in Britain and in the other Convention signatories, a general recognition of the need for the establishment of some form of enforcement machinery but less unanimity as to the form that this should take. A variety of issues arise relating to the composition of the supervisory agency, its relationship with government and other public agencies and as to the powers which it should possess and the role which it

should play.

4. The Form of the Authority

In considering the form of a supervisory agency two options are available to the legislature with the choice lying between the establishment of a multi-membered authority or the appointment of a single officer with executive responsibilities in this area. The former approach has been followed in countries such as Sweden, Denmark, Norway and France with the latter being adopted in West Germany and the United Kingdom.

In part the choice between the single and multi-membered forms of authority may be seen as reflecting existing procedures in the various states. In France, for example, a collegiate system of administrative tribunals provides a vehicle for citizens to pursue complaints against the activities of public authorities.(43) Although few precedents exist in the UK for the establishment of an agency designed to monitor the compliance of public or private agencies with general or specialised legal provisions, the appointment of the Parliamentary Commissioner for Administration(44) and the Director General of Fair Trading(45) provide some evidence of a preference for a single source of authority. It may be noted, however, that the Lindop Committee favoured the appointment of a Data Protection Authority consisting of a Governing

Board and an Executive. The Board would essentially consist of part time appointments, whereas the Executive would be a full time body. In considering the role of the Governing Board Lindop recommended that:

> "The Board should be responsible for the Authority's policy and major decisions, and for providing panels to deal with internal reviews in cases where users or data subjects are in dispute with the Executive. We suggest that the Board might consist of a Chairman and between 8 and 12 members, with the Chief Executive as a member ex officio.
>
> The purpose of dividing the authority into a board and an executive is mainly to ensure that it is governed by a group of people who are seen to be widely representative of the country at large, and this means that at least some of the members should be lay people.."(46)

The arguments in favour of the multi membered approach, with members chosen because of their expertise and identification with particular interest groups have been cogently stated by Professor Simitis:

> "The choice of a Commission rather than a Commissioner is not purely fortuitous. It, on

> the contrary, reflects the wish to entrust an admittedly most sensitive task to persons familiar with the interests and expectations of both the political authorities and the societal groups. Conflicts over the collection and the retrieval of data are thus deliberately internalized. Control measures are constantly filtered by a compromise reached within the commission and at the same time a public discussion of the processing policies is at least partially inhibited."(47)

Reversal of the above arguments serves to adequately put the case for the single member approach.(48) Whilst the merits of reducing public debate and discussion of data practices may be questioned - one of the underlying purposes of legislation is surely to inculcate a sense in individuals that they possess a degree of control over their own records. Therefore any form of monopolisation of debate by a public agency, however benevolent its motives and actions may be, must be regarded with a measure of suspicion. Nevertheless, the basic thesis appears to contain considerable merit, that the supervisory agency, in formulating its policies and exercising its functions must benefit by an input from representatives of the various interests involved in data protection. Again the spirit of compliance engendered in data users may be enhanced if they consider that they have been involved in the

decision making process. Against this, it may be argued that the representation of the various interests at the level of policy formulation might lead not to the positive resolution of conflicts but rather to delay and compromise.

In the event, the Data Protection Act places executive responsibility entirely in the hands of the Data Protection Registrar. This remained the Government's position despite an attempt during the Act's parliamentary progress to provide a statutory consultative mechanism. An amendment introduced in the House of Lords proposed the creation of a "Data Protection Advisory Committee". The membership of this body would include persons having:

> "..professional knowledge or experience of health care, scientific research, statistics, the prevention and detection of crime, employment, public administration, the law and the use, design or manufacture of data equipment."(49)

This suggestion was rejected by the Government on the basis that the freezing of the categories of membership envisaged by the amendment might prove unsatisfactory in the light of changing computer practices. Lord Elton commented that:

> "I remind the Committee that the registrar will be perfectly free to consult and to take advice without a statutory mechanism to do so. The types of advice that he is going to want are almost totally unpredictable because one does not know in what direction the new technology is going to be pointed. For instance, seven or 10 years ago it was unthinkable that there would be databanks used for introducing people for the purposes of marriage. Maybe there will be some new departure like that; there probably will be almost annually. The composition of the advisory body therefore is something which will almost certainly have to fluctuate if it is going to be appropriate."(50)

Whilst the wisdom of permitting the Registrar discretion as to the nature and extent of consultations undertaken in the exercise of his functions may be accepted, the debate does highlight one of the major factors inevitable in the concentration of powers in the hands of a single individual; that the effectiveness of the Office will be heavily dependent upon the abilities and inclinations of its holder. Sieghart has argued that:

> ".. it would in theory - and I am not suggesting that it would happen in practice - be possible to take, let us say, a recently

> retired deputy secretary from the Home Office with a good taste in sherry and in non-intervention in the citizen's affairs, put him in charge of this job, and give him a staff of about twenty, which is all he is going to be allowed. He could then say to them, 'Look set up this Register, that is really your job. And would you mind once a year drafting me an annual report to send to Parliament? And I shall now put my feet up and enjoy my sherry."(51)

The above may well represent both an extreme and a cynical view but it appears an inevitable feature of the single member approach that the success or failure of the regulatory system will be heavily dependent upon the attributes and abilities of the person charged with its operation. It is one of the more notable features of the regulatory system contained in the Data Protection Act that whilst the Registrar is granted substantial powers comparatively few duties are imposed upon him.(52) Considering the complex technical issues involved in data processing and range of purposes for which information may be sought, processed or used it appears unreasonable to expect any single individual, however assiduous or gifted, to acquire expertise across the broad spectrum of computer activities. As has been seen, in this area every argument has its counter. In this context it may be argued that the fact

that the Registrar is to be appointed on a full time basis, whereas most members of multi-membered authorities serve on a part time basis, might facilitate the acquisition of expertise whilst the presence of a sizeable support staff provides the means for his office to develop any required specialist expertise.

To some extent the Registrar's activities are subject to a measure of scrutiny through the creation of a Data Protection Tribunal.(53) This body consists of a legally qualified Chairman and an unspecified number of similarly qualified Deputy Chairmen together with a number of members, the numbers of which are again not specified in the Act, representing the interests of data users and of data subjects.(54) This formulation marks a move from the original proposals in the Bill that the members of the Tribunal should:

> "... include persons appearing to the Secretary of State to have professional knowledge or experience of the use, design or manufacture of data equipment."(55)

Following protests that the interests of these technical experts could be regarded as synonymous with those of data users and therefore the membership could be regarded as biased against data subjects the membership was extended to include:

"persons to represent the interests of data subjects."(56)

this approach was itself the subject of criticism from representatives of data users arguing that not all technical experts were either inclined or, indeed, capable of representing their interests(57). Once again account was taken of this complaint(58) and, as enacted, the Act provides for the Tribunal's membership to consist of:

"(a) persons to represent the interests of data users; and
(b) persons to represent the interests of data subjects."(59)

One consequence of these amendments is that there can no longer be any guarantee that the membership of a Tribunal will possess any technical expertise and it would appear from the list of members of the Tribunal that no member has been appointed on the basis of his or her technical expertise.(60) The rules of procedure laid down in the Act,(61) however, provide for the Tribunal to summon witnesses to assist with its deliberations and there appears no reason why the Tribunal should not call technical experts to act in this capacity. As constituted, the membership of the Data Protection Tribunal consists of one chairman and two deputies together with 28 members. All appointments

are on a part time basis. Whilst there might be difficulties in securing the attendance of part time members it may be doubted whether such a large membership is justified. It appears to be envisaged that the Tribunal will not sit in plenary session but rather that three members (the Chairman or one of his deputies, a user representative and a member representing the interests of data subjects) will deal with any particular business. Whilst much will clearly depend upon the number of cases brought before the Tribunal, and it is perhaps relevant to note that to date, almost four years after the Act received the Royal Assent, the Tribunal has not yet met. It may be expected that the composition of any particular tribunal will be dependent upon the nature of the business before it but the existence of such a large membership may prevent individual members from obtaining experience and expertise through its deliberations.

The purpose of the Tribunal is to dispose of appeals by data users or the operators of computer bureaux against adverse decisions of the Registrar. In particular, appeals may be brought against the refusal of an application for registration(62) or the service of an enforcement, transfer prohibition or de-registration notice.(63) Although the decisions of the Tribunal will be binding in a particular case and will undoubtedly serve to influence the approach of the Registrar in any

future cases which may arise, the Tribunal has no formal advisory role.

As constituted, the task of the Tribunal is to offer a safeguard to data users against unreasonable actions by the Registrar. There is, however, no provision for the Tribunal to act on the complaint of a data subject that either the Registrar has failed to act or that a decision to accept an application for registration has been wrongly made. Whilst the Tribunal can safeguard data users against an excessively zealous Registrar, it can do nothing to protect data subjects in the event that the Registrar is unwilling to take action or acts in a manner which is detrimental to their interests.

Although no formal consultation procedures exist the need to consult with interested groups appears to have been accepted and acted on by the Registrar who has commented that:

> "The Data Protection Act 1984 touches virtually every aspect of the economy and society. No organisation as small as the Registrar can hope within itself to have detailed knowledge and understanding of such a breadth of activity. It is essential, therefore, to establish a continuing dialogue with organisations which can express the needs, problems and practicalities of the different economic

> sectors and interest groups. These groups must be representative of individuals as well as data users."(64)

Whilst it may well be undesirable to create a definitive list of those interests which must be consulted it is submitted that a statutory duty to consult could usefully be imposed on the Registrar. Assuming that technical experts could be appointed to the Tribunal under the category of user representatives, it would appear that it would be capable of performing such a function. The Data Protection Act does not specify any maximum number of members for the Tribunal and although the point has been made that in relation to its present reactive role, the Tribunal's membership may be overlarge, this factor may not be significant were it to be given a more positive role.

Whilst the questions of the supervisory agency's constitution and its modus operandi may provide an indication of the attitude of the legislature and the executive towards the concept of data protection, a more significant factor concerns the status of the supervisory agency vis a vis the government. As many sensitive aspects of data processing are carried out within the public sector, the promotion of public confidence requires that the agency be seen to enjoy a considerable measure of independence from the dictates

of those governmental agencies whose processing activities appear most likely to affect the individual. The issue is perhaps not as clear cut as might initially appear to be the case. It may be doubted whether any legislature or executive would wish to so abdicate their functions as to transfer total discretion and complete decision making power to an external unelected agency. One approach to this problem might involve permitting the decisions of the supervisory agency to be subjected to review by the executive. Whilst such an approach undoubtedly compromises the status of the supervisory agency, it does recognise that the extent to which data processing should be regulated raises political as well as legal questions.

In this respect the agency may be seen to have acquitted its functions by placing sensitive or controversial aspects of the activities of public sector data users into the political arena. A further point which may be raised in this context, suggests that there may be an increased willingness on the part of the executive and legislature to extend the sphere of the supervisory agency's operations and to increase its powers if they retain final control over areas which are considered to lie within the remit of government. A distinction may be drawn between the formal control and regulatory measures which may be available to an agency and as to the extent of the

influence which it may be able to exert in a less formal manner. A closer connection with government may be seen as restricting its independence, have implications for its decision making powers, but may serve to extend its sphere of influence. It may be argued that the notion of a form of partnership between supervisory authority and government may be more easily achieved where the agency is composed of a number of members. Such an approach allows for representation of a variety of interests - including those of the government - and, conversely, may also be considered to enhance the degree of practical independence enjoyed by the agency. This would be on the basis that it may be considered more difficult to influence a number of members, each of whom may serve on a part time basis than to affect the judgement and actions of a single person who may well wish to make a career out of his office.

Constitutionally, the Data Protection Registrar enjoys a considerable degree of autonomy. The legislation provides that he be appointed by Letters Patent and have the status of a corporation sole.(65) The effect of this is that he is appointed by the Crown and may only be removed from office by the Crown upon receiving an address passed by both Houses of Parliament requesting such action. In this respect the Registrar's status is equivalent to that of the Parliamentary Commissioner for Administration (the Ombudsman). Indeed

it was stated that this office served as a model for that of the Registrar. In several important respects, however, the terms and conditions of employment of the two officers differ normally, it is submitted, to the detriment of the Registrar's independence.

Section 1(2) of the Parliamentary Commissioner Act of 1967 states:

> "Her Majesty may by Letters Patent from time to time appoint a person to be the Commissioner and any person so appointed shall (subject to subsection (3) of this section hold office during good behaviour."(66)

The aforementioned subsection (3) provides for the Commissioner's retiral at 65 years of age and for the possibility of his being removed from office pursuant to Addresses from both Houses of Parliament.

In contrast to this comparatively open ended term of office the Data Protection Act provides that the Registrar is to be appointed for a, renewable, period of 5 years.(67) The comment has previously been made that few duties are imposed on the Registrar.(68) It may be that the knowledge of a comparatively short term of office will spur the holder to an energetic use of his powers but it may also be the case that the need to seek renewal of his tenure might expose the Registrar

to a degree of governmental influence. It is relevant here to note the controversy which arose in West Germany following the decision of the Federal Government not to renew the appointment of the Federal Data Protection Commissioner. This step was regarded both as punishment for his enthusiastic pursuit of individual complaints and as a warning to future holders of the office.(69)

In respect of financial matters, also, it might be argued that the Registrar's independence is subject to considerable qualification. Whilst the Parliamentary Commissioner Act specifically provides a salary for the Commissioner with the proviso that this may be increased (but not reduced) from time to time by Resolution of the House of Commons;(70) the Data Protection Act contents itself with stating that:

> "(1) There shall be paid -
>
> (a) to the Registrar such salary, and
>
> (b) to or in respect of the Registrar such pension,
>
> as may be specified by a resolution of the House of Commons."(71)

Such salary will to be voted annually. Unlike the 1967 approach which specifies an initial salary for the Commissioner and provides the mechanism by which it may be increased the Data Protection Act leaves the

question of salary totally to Parliament which may fix, increase and reduce it as it thinks fit. Whilst the point will hopefully remain academic, the more transitory nature of the arrangements for the Registrar's salary may serve to undermine his independence.

Although executive power for his office is vested in the Registrar alone he will clearly have to employ a staff to assist him in his functions. The Act provides that:

> "(1) The Registrar -
>
> (a) shall appoint a deputy registrar; and
>
> (b) may appoint such number of other officers and servants as he may determine."(72)

The Registrar is authorised to determine the terms and conditions of employment of his appointees. All of these powers, however, may only be exercised upon receiving the approval of the Secretary of State who, in turn, will require the consent of the Treasury.(73) This provision was subjected to severe Parliamentary criticism on the ground that the approving Minister would be the Home Secretary and that in view of the scale of data processing carried out under the aegis of the Home Office there should be no question of the

Registrar being dependent upon this Department.(74) Whilst recognising that the Registrar could not be given unlimited discretion as to the numbers of staff appointed and as to their terms of employment, it was argued that he should have to seek the approval of the Treasury alone for his actions in these respects. In support of this argument it was pointed out that the 1967 Act provides that the Commissioner may:

> "..appoint such officers as he may determine with the approval of the Treasury as to numbers and conditions of service."(75)

In response it was argued that the change in terminology merely reflected an inter departmental transfer of functions during the intervening years. Thus whereas in 1967 the Treasury had enjoyed overall responsibility for policy matters in addition to those of financial control, the former function had now been transferred to the Home Office.(76) In addition it was pointed out that in the case of the Local Government Commissioners, appointed under the Local Government Act of 1974 questions as to their appointment and remuneration were subject to the approval of the Secretary of State for the Environment, the Minister responsible for local government matters. It was argued that this arrangement had not been seen as an impediment to their independence.(77)

Although such a precedent may appear to offer a favourable prognosis it is not certain how far it can be considered relevant. In comparing the roles of the Ombudsmen, whether concerned with central or with local government it must be borne in mind that their functions are those of investigating and reporting.(78) The Registrar on the other hand is given power to make binding determinations (subject to the possibility of appeal to the Data Protection Tribunal). The similarity between the two offices is not, therefore absolute and it might be argued that there is less need for the government to try to influence the work of the Ombudsmen as they may simply ignore their recommendations. Again, it may be argued that in the case of the Local Authority Ombudsmen a considerable number of commissioners are appointed, many on a part time basis.(79) This factor alone must make it more difficult for any Secretary of State wishing to influence their determinations. Most fundamentally, the staffing needs of the Ombudsmen in terms both of the number and the range of expertise required would appear to be less than those reasonably required in order to permit the Registrar fully to exercise all of the powers conferred upon him by the Act. In March 1986, as the registration procedures built to a peak, the Registrar had appointed 83 staff, 40 of whom had been engaged on a temporary basis.(80) In the case of the Registrar control of the purse strings will determine the effectiveness of his operations. Whilst there is,

to date, no evidence of restraint being placed on the Registrar in relation to the appointment of staff the precedents of the Ombudsmen do not reflect the situation where a single official is appointed for a fixed term with a need for substantial assistance and where this requires the sanction of that Department of State which may constitute the subject of some of his most sensitive investigations.

In the final analysis it may be concluded that the position of the Registrar vis a vis other governmental authorities is unsatisfactory. Constitutionally, the Registrar occupies a position of considerable independence but, by limiting his term of office and subjecting his financial and staffing requirements to the need for governmental approval, the Act places weapons in the hands of the Government which may enable it to directly or indirectly influence the manner in which the Registrar performs his functions. Although the Registrar's independence may be to some extent illusory, a price has been paid for this in terms of the powers and functions which he is permitted to exercise. In the vital area of national security the reluctance of the Government to delegate responsibility to an independent external agency has resulted in data held for national security purposes being totally excluded from the Act's scope. Whilst this decision has to be placed in the context both of the traditional British governmental concern at the implications of

external access to official records and the reluctance of the judiciary to interfere with the government's actions in the sphere of national security, the extent of the Registrar's formal separation from the machinery of government may have prompted the decision to render the exemption absolute. Whilst the presence of an independent Registrar possessing decision making powers offers considerable safeguards to the individual this is at the cost of a limitation of his powers and, more subjectively, a perception on the part of those in government that data protection constitutes an isolated subject rather than one whose tenets should permeate into every area of governmental and legislative activity. There would already appear to be some evidence to support this suggestion. The Registrar has used the pulpit of his annual report to Parliament to voice concern at several instances where he considered that his views concerning the implications of governmental actions had not been taken adequately into account. In particular he cited the practice of selling computer compatible versions of electoral registers and the failure to consult with his office prior to the enactment of legislation introducing the system of community charges into Scotland.(81) Although the Registrar's annual report may well provide a useful vehicle for the ventilation of his grievances the illustrations cited above demonstrate the deficiency of such a device, that the Registrar is compelled to respond to an unsatisfactory situation rather than to

prevent that situation arising initially.

5. Identification of Data Users

Assuming the existence of a supervisory agency, the questions arise as to who is to be supervised and as to the appropriate form of supervision. To a considerable extent these two questions are linked as the form of supervision adopted will be largely dependant upon the nature of the activities and the users which are to be subjected to scrutiny. In considering the form of supervision a variety of approaches can be identified. At the level of minimal intervention, data users may be required to comply with the substantive provisions of the legislation with the supervisory agency intervening only in the event of a suspected breach of these requirements. Moving beyond this, it has been considered beneficial for the fact and nature of processing activities to be made a matter of public record. Such notification may of course be given without the intervention of a supervisory agency. In the United States, for example, it is provided in the Privacy Act of 1974 that all federal agencies which maintain information on individuals must publish details as to the scope and extent of their record keeping activities in the Federal Register.(82) Assuming that the requisite information is supplied by an agency appearance in the Register is automatic. Making this list a matter of public record serves the

twin purposes of providing information upon which an individual can base further action and also serves to ensure that processing is carried out under conditions of openness or transparency. This point was well made by the United States HEW Committee which argued that there should be:

> "..no record system whose very existence is a secret."(83)

It must be noted, however, that although the establishment of a list of data users may serve a variety of valuable purposes, such a procedure is not required under the Convention. This states merely that:

> "Any person shall be enabled:
>
> (a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or place of business of the controller of the file.."(84)

Although the use of the word "enabled" might convey the suggestion that appropriate facilities should be made available to individuals it is significant that the explanatory report to the Convention notes that:

> "The wording of this litera takes into account

> the variety of rules of domestic law giving effect to this principle. There are States where the name of the controller of the file is listed in a public index. In other States which have no such publicity rule, the law will provide that the name of the controller of the file must be communicated to a person at his request."(85)

It would thus appear that national legislation is required only to give individuals the right to approach anyone they had reason to believe engaged in data processing with a view to obtaining the information specified in the above provision. Indeed, this was the case under the earliest European data protection statute; that of the German Land of Hesse. As originally enacted, this appointed a data protection commissioner who was charged with the duty of ensuring that those who engaged in data processing complied with an obligation to ensure that data be obtained, stored and transmitted in such a way that it be not susceptible to consultation, alteration or destruction by unauthorised persons.(86) Although data users were obliged to cooperate with any enquiries made by the commissioner(87) there was no obligation upon them to register details of their activities.

Although the Convention does not impose any formal requirement that a Register be established the

existence of such a document may be of considerable utility, both to the enforcement authority in the pursuance of its duties and to the wider interests of society in that it constitutes a, hopefully, definitive survey of computer practices within a particular country. Additionally, of course, the existence of a public record may be of assistance to an individual wishing to exercise rights granted to him under data protection legislation whilst, finally, a more cynical motive can be identified in ~~it~~ that a fee might be charged as a pre-requisite for admission to a register. This point is significant in view of the Government's desire, as expressed in its 1982 White Paper,(88) that the Data Protection Registrar's activities should be self-financing. The imposition of such a fee upon data users would appear to provide the only mechanism by which such a target could be reached. This was the view of the Lindop Committee which in considering the alternatives of an advisory regulatory agency along the lines of the Hessian commissioner and a regulatory body commented that:

> "It is not clear, however, how a purely advisory DPA could be made financially self-supporting: indeed we have come to the conclusion that this could not be done."(89)

The procedures under which such a public record may be created will be considered in the following section.

For the present, the role of the supervisory agency in controlling admission to this record will be examined. The above quotation from the Lindop Committee linked the establishment of a decision making supervisory agency with that of the creation of a public register. If the agency possesses powers it appears inevitable that these will be used in the compilation process and that applications will be submitted to a measure of vetting. Within Europe, debate has increasingly centred not on the question whether the supervisory agency should possess discretion as to whether a user should be admitted, or permitted to remain on such a public list, but as to the extent of this discretion. Systems can be divided into two categories, registration and licensing, although the terminology in this area is imprecise.(90) Registration may be seen as conferring a prima facie right upon a data user to have an application for admission accepted. This right can be challenged by the supervisory agency in the event that it possesses information suggesting malpractice on the part of the applicant. A system of licensing may impose a heavier burden upon the applicant, requiring that he satisfy the supervisory agency as to his suitability to be permitted to commence or to continue data processing.

6. The Registration Process

Within the United Kingdom, the approach adopted under

the Data Protection Act is classed as one of registration. The Act obliges the Data Protection Registrar to:

> "..maintain a register of data users who hold, and of persons carrying on computer bureaux who provide services in respect of, personal data and shall make an entry in the register in pursuance of each application for registration accepted by him under this Part of this Act."(91)

The register, the Data Protection Register, is to be a public document. In justifying the establishment of the Data Protection Register the government were at pains to minimise the effect that registration would have upon the activities of data users. In the House of Commons, the Home Secretary explained that:

> "The process of registration will not be onerous. It is important to make that clear. Registration will entail no more than answering half a dozen questions and paying a small fee and acceptance onto the register will in most cases be automatic. Thereafter, the vast majority of users will not be bothered again by the Registrar. We have deliberately kept the requirements of registration to a minimum to ensure that users do not face unreasonable

> burdens. The registration process will require data users to specify the purposes for which they hold data ... and bring into the open the processing of personal data, thereby meeting the fear of unknown activities taking place in secret. The establishment of a register to which anyone can go to discover the use being made of automatically processed information is a key feature of the scheme."(92)

In assessing the value of the registration process attention must be paid to a number of issues. These include the extent of the burdens which the registration process may impose upon data users - especially those engaged in small scale or non contentious activities - the question whether the resources of the Data Protection Registrar, especially in terms of staff, can be considered sufficient to allow effective use of the discretion afforded to him by statute, the extent to which the compilation of a register will be of significant benefit to data subjects and whether the sanctions provided in the event that a user fails to register details of his activities are sufficient and apposite for such an eventuality.

Under the provisions of the Data Protection Act, all data users and those operating computer bureaux were required to submit registration applications within the

six month period from November 1985 to May 1986.(93) Any person who controls personal data which is intended to be subjected to automated processing will, prima facie, be regarded as a data user.(94) By referring to the issue of control, the definition has the effect of potentially classifying as data users persons who do not own or have access to a computer. An example might relate to a businessman who prepares his accounts in manual form and submits them to his accountant who subjects them to automated processing. In this situation the businessman will be regarded as having control over the data and hence as the data user even though he may not be aware of the fact of the processing. In addition to data users the Act regulates the activities of those who operate computer bureaux. This will be the case where a person:

> "provides other persons with services in respect of data"(95)

These services may consist either of processing data as the agent of the other person or, alternatively, of allowing them to use equipment in his possession to conduct processing. Thus, in the example given above, the accountant will be regarded as operating a computer bureau and will be required to register as such. Additionally, should two data users, operating similar computer equipment, enter into even the most informal agreement providing for access to the other's equipment

in the event of a breakdown, both users will also be required to register as operating a computer bureau. Finally, it may be speculated that with the proliferation of micro computers in the workplace and the increasing user friendliness of these machines it may often be the case that equipment supplied by an employer is used by employees for purposes unconnected with their employment. In the event that these activities come within the ambit of the Data Protection Act the employees in question will be required to register as data users, and in the event that the employer can be regarded as allowing them, the employer will additionally be required to register as a computer bureau.

The breadth of these definitions, coupled with those relating to the nature of processing discussed previously, serve to ensure that an enormous number of data users and computer bureau will be required to register. In an effort to reduce the numbers somewhat, the Data Protection Act provides that a number of data users are to be exempted from its provisions. The exemptions applying under the Act will be discussed at a later stage(96) but an initial problem can be identified. The notion of a public list is intended to inform the public, to provide an initial check upon the suitability of data users and to assist the continuing supervision of users. These benefits may be swamped in a numerical sea of data users.

Having determined that a person should be classed as a data user or as the operator of a computer bureau, and having ascertained that none of the exemptions provided for in the Act are applicable the registration procedures will come into play.

The basic form that these procedures should take are laid down in the Data Protection Act. This requires that, a data user must divulge the following items of information:

> ". a description of the personal data to be held by him and of the purpose or purposes for which the data are to be held or used;
> .. a description of the source or sources from which he intends or may wish to obtain the data or the information to be contained in the data;
> .. a description of any person or persons to whom he intends or may wish to disclose the data;
> .. the names or a description of any countries or territories outside the United Kingdom to which he intends or may wish directly or indirectly to transfer the data; and
> .. one or more addresses for the receipt of addresses from data subjects for access to the data."(97)

In the case of the operator of a computer bureau the

Act requires only that he supply details of his name and address.(98)

In large part, the information supplied at registration will constitute the content of the Data Protection Register. The task of compiling the register began on the 11th of November 1985, that being the date fixed by the Secretary of State for the commencement of the registration exercise. Failure to make timeous application would render any processing carried out after the 11th of May, illegal and subject to criminal sanctions.(99) The prospect of criminal prosecution might have been expected to encourage users to register. In fact, however, the registration exercise has proved far from successful.

Estimates as to the numbers of those liable to register have varied widely over the years. Throughout the Act's parliamentary passage, Government spokesman quoted Home Office estimates that the number of data users would be in the region of 60-80,000.(100) Subsequently, this figure was raised to 200,00.(101) Even at the higher level these estimates were considerably out of line with those put forward by other authorities whose figures varied from 400-600,000 users.(102) When account is taken of the breadth of the definitions contained in the Act, the limited scope of the exemptions and the qualifications which hedge many of these coupled with the huge numbers of computer and

computer related equipment which is capable of being used in a manner likely to bring the Act into play, it would appear certain that the number of data users amounts to several hundred thousand. In planning for the registration process the Registrar estimated that some 300,000 users would be required to register during the initial 6 month period.(103) In the event, on the 10th of May 1986 only 110,000 applications had been received.(104) Even including in the figures some 26,000 applications received in the month following the deadline it seems that as from that date the criminal fraternity of the UK received at least 160,000 additional members. The reasons for the failure of individual users to apply for registration may be many and various but it would appear that a major factor arose from a general perception of the inappropriateness of the process from the perspective of small scale users. Although it had been proclaimed that:

> "We have deliberately kept the requirements of registration to a minimum to ensure that users do not face unreasonable burdens."(105)

and that:

> "Registration will entail no more than answering half a dozen questions.."(106)

In the event anyone wishing to register as a data user was required to complete a two part application form extending to 12 pages. In order to assist users this form was accompanied by a 45 page explanatory booklet. Whilst in large part, the application forms required the user merely to tick appropriate boxes and, indeed, applicants were specifically discouraged from straying beyond the standard purposes specified in the application form applicants being advised that:

> "In each section .. you may use standard descriptions to provide the detail required. Although you also have the option of writing your own descriptions in free text, you are strongly encouraged to use the standard description approach. Applications containing text will be closely scrutinised by the Registrar and are more likely to require further clarification."(107)

In view of the limited resources available to the Registrar reliance upon standard descriptions may be seen as essential if applications are to be subjected to any degree of scrutiny. Even so, it must be noted that the "half a dozen questions" referred to in Parliament had become a much more complex exercise. In particular it may be noted that all applicants are required to sign a declaration to the effect that:

"I have read the **Notes** booklet and understand the Registrar's conditions which it contains."(108)

In considering the success or failure of the UK's registration exercise it is instructive to draw a comparison with the experiences of other countries which had previously introduced data protection legislation. On the basis of the raw figures the UK performance does not appear discreditable. In France it has been estimated that fewer than 10% of data users made timeous application for registration, in Sweden around 50% with only Austria and Norway achieving compliance rates in excess of 50%. The general experience on the continent would appear to suggest that ensuring compliance with the registration procedures is a lengthy process with up to 3 years being required in order to achieve an estimated compliance rate of 90%. In the light of these figures a poor take up rate was not unexpected. Where, however, the UK approach can be criticised is in its failure to learn from this continental experience. Faced with an initially low take up rate the inevitable approach has been to offer a simplified registration scheme to small scale users. The results of this have been impressive. In France a mere 11,939 applications for registration had been received by 1980. At this stage simplified procedures were made available with the result that by 1982 102,000 applications had been received only 6,300

of which required to comply with the full procedures, the remainder utilising one of 25 simple declarations devised for particular applications.(109) It appears to demonstrate a remarkable degree of chauvinism that, faced with a considerable body of evidence suggesting that a complex registration procedure would be doomed to failure, the UK should persist in this approach. At the present time this has produced a situation whereby a multitude of data users commit a criminal offence every time they use their equipment and yet, except in the case of any large scale or high profile users, seem unlikely to face prosecution. Such a result reflects no credit on the law in general or upon the concept of data protection in particular. Given the reluctance with which the Data Protection Act was introduced and the government's steadfast resistance to any amendments intended to extend the scope of the measure it may be queried whether the failure of the registration came as either a surprise or a total disappointment to the government.

A partial reaction to the poor response to registration has come with the introduction by the Registrar of alternative registration forms for certain categories of data user. Essentially, these forms are pre-completed for specified standard activities. It may be doubted, however, whether the task facing a data user is noticeably simplified in that he still has to make the decision whether his activities come within the

specified categories. Any advantages obtained through the introduction of the new forms may be minimised by the decision that the registration fee should be increased from £22 to £40.(110) This decision was prompted by the lower than expected number of registrations which served to reduce the Registrar's income and thereby threaten the Government's proclaimed objective that his office should be self financing. Whilst the increase in fees can thus be justified by reference to financial considerations it cannot be considered likely to encourage recalcitrant users to repent and provides a further indication of the Government's attitude towards the concept of data protection.

A governmental refusal to learn from experience is apparent not only in the imposition of an excessively and unnecessarily complex registration scheme, but also in the decision that registration should be a one off exercise. In their report, the Lindop Committee recommended that their proposed Data Protection Authority should enjoy a measure of discretion both as to the scope and the timing of the registration exercise.(111) It was envisaged by the Committee that all data applications carried out within the public sector should be registered in an initial phase with private sector users required to register according to a timetable to be laid down by the Authority. As with many of the recommendations of the Lindop Committee,

this approach did not commend itself to the Government. In rejecting an amendment intended to give the Registrar discretion to specify categories of users who would require to register at a particular time. In the House of Lords Lord Glenarthur stated that:

> "Why do we need to place on the registrar the burden of deciding who should register first, who later? What yardsticks is he to use, what limit should the time - scale have, how does he deal with multiple users?"(112)

The answer to these questions must surely lie in the Government's own words, that the "registrar is a person of considerable standing" who should be allowed discretion as to the manner in which he performs his functions. If the Registrar is considered capable of exercising discretion whether to accept an application from a user who does not comply fully with the data protection principles it might not be considered unreasonable to allow him discretion in this respect.

Apart from the recommendations of the Lindop Committee, a direct precedent exists for the operation of a similar regulatory scheme under the provisions of the Consumer Credit Act 1974. This Act requires that anyone operating a credit related business must obtain a licence from the Director General of Fair Trading.(113) Although this scheme is classed as one of licensing,

its practical application is not dissimilar from that applying under the Data Protection Act. Under the 1974 legislation specific provision is made for the phasing in of the licensing scheme.(114) Six categories of licence are provided for, consumer credit businesses, consumer hire businesses, credit brokerage businesses, debt adjusting and counselling businesses, debt collecting businesses and credit reference agencies.(115) The Secretary of State being empowered to fix the dates for the commencement of the licensing scheme it was provided that, in respect of businesses coming within the final three categories, applications were to be lodged between 2nd February and 3rd August, 1976.(116) In the case of the first two categories the commencement of licensing was delayed until 1st of October 1977.(117) In total somewhere in excess of 150,000 licences have been issued(118) with the details recorded in a public register created and maintained by the Director. Bearing in mind that the number of applications received under the Consumer Credit Act is considerably less than that estimated as due under the Data Protection Act, it is relevant to note the admission of the Director that the exercise has not been a tranquil one and that:

> "(t)here have at times been serious delays in handling these applications because administrative resources have not always matched demand."(119)

Under the Consumer Credit Act, in contrast to the position under the Data Protection Act, no time limit is fixed for the director to make a decision whether or not to grant a licence and, therefore, delay may be equated to some extent with comprehensive scrutiny of an application. The evidence from the credit field would appear to suggest that the introduction of a system of regulation in a single operation must minimise any possibility of genuine scrutiny and control of applications. Consideration of the logistics behind the initial registration exercise would appear to support such a view. Upon receipt of an application the Registrar is obliged to notify the applicant of his decision whether to accept or reject the application within 6 months.(120) Although the Act provides that this period may be extended where the Registrar considers that an application requires further study than would be possible during the 6 months(121) it would appear that such a decision has to be founded in the complexities of a particular application and cannot be used in the event that the volume of work exceeds the Registrar's capabilities.

Of the 110,000 applications initially received by the Registrar, no fewer than 89,000 arrived in the period from 1st of April to 11th of May 1986.(122) Decisions concerning the acceptability of these applications would have to be notified to applicants by, at the latest, 10th November 1987. In May 1986 the

registration department of the Data Protection Registry employed 56 staff.(123) Allowing for holidays it may be calculated that perhaps 115 days would be available for consideration of the applications. Further estimates would suggest, therefore, that each employee would have to process some 10 applications a day allowing perhaps 45 minutes for consideration of each application. Within this time the 12 pages of the application forms will have to be scrutinised and arrangements made for the relevant information to be entered in the Data Protection Register. As many large users will hold data for numerous purposes, each of which will have to be registered, it appears that there will be little scope for the Registrar to achieve anything other than to ensure that the form is correctly completed. This in itself raises the spectre of incorrectly completed application forms. The Registrar has reported that errors have been detected in 8% of application forms at the stage of initial clerical checking. At the subsequent stage of computer processing of applications discrepancies are identified in a further 17% of forms. Finally, the Registrar has estimated that in 13% of cases, although the form may technically be correctly completed that the stated sources, uses and disclosures of data may not be those which are most appropriate to the particular users needs and may require to be altered at some future date.(124) Even disregarding these last figures on the basis that amendment need not be completed within the six month period for

consideration of applications, it would appear that the workload of the Registrar's staff may be increased by a figure of some 25% due to users' errors in completing the necessary documentation. Doubts concerning the efficacy of the scrutiny which may be afforded to applications do not arise solely in respect of the original registration exercise. As the Act provides that a registrations is to be valid for three years unless the user specifically requests a shorter period of validity(125) the effect must be that every three years the Registrar will be faced with a huge number of registration applications all of which will have to be processed within a short period of time. A phased registration scheme would serve to spread this future workload.

The statistics referred to above would indicate that, as a matter of logistics, there may be little likelihood of a user's application for registration being rejected. Such a result appears even less likely when consideration is given to the legal basis of the Registrar's ability to reject an application. The Data Protection Act provides three grounds for rejection; firstly that, in the Registrar's opinion:

> ".. the particulars proposed for registration..will not give sufficient information as to the matters to which they relate."

additionally an application may be refused if the Registrar:

> ".. is satisfied that the applicant is likely to contravene any of the data protection principles or
>
> .. he considers that the information available to him is insufficient to satisfy him that the applicant is unlikely to contravene any of those principles."(126)

Under the Act's transitional provisions it was provided that only the first of these grounds might be invoked by the Registrar during the first two years of the registration process, i.e. until 10th November, 1987.(127) The scope of this ground for rejection would appear extremely limited, a suggestion which would appear to be supported by the fact that only one application was formally rejected during the transitional period.(128) Given the existence of an extensive application form requiring that specified pieces of information be provided, it may be argued that the requirement amounts to little more than the obligation to fully complete the documentation. Whilst, as was stated above, a large proportion of forms have been incorrectly completed, the Registrar has indicated that his response here would be to return the form for completion and resubmission rather than

formally rejecting it. The extent to which the Registrar may refuse an application when, prima facie, it has been completed is less certain. In respect of several categories of purpose the application form requires that the user submit further information as to his intended practices. Thus where a user indicates that he holds data for research purposes the Notes of Guidance indicate that he should specify the area of research involved whilst where an entry appears under the purpose "policing" the 'Notes' require further details but give an illustrative list of typical activities such as:

> "maintaining details of offenders, suspected offenders, offences, victims, witnesses and other relevant persons.."(129)

It is uncertain, however, whether the requirement is merely that additional information is given or whether the Registrar is given power under this heading to make a value judgement as to the acceptability of a particular application. It is submitted that this is not the case and that at the present, the Registrar may only refuse an application upon technical grounds. To this extent it may be argued that those data users whose activities may conflict with the principles have enjoyed a 2 year respite from the threat of realistic sanctions against their activities. Whilst it may be acknowledged that one of the purposes of the

transitional period is to allow users time to bring their systems into line with the requirements of the Act the data protection principles are so fundamental and have so frequently been described as statements of existing good data practices that there seems no good reason why a user should not be expected to comply with them from day one. The only principle which might cause technical problems to certain users would be that of subject access and the requirement that data subjects be supplied with a printout of any personal data. The introduction of subject access was deferred until November 1987, two years after the beginning of registration so compliance with this principle would not appear to be an issue at the time of initial registration. In the event that a user is unable to comply with any of the remaining principles in a minor respect the Registrar will, even after the transitional period, have discretion whether to reject an application when he has evidence of a breach of the principles. The value of this discretion was stressed by the Minister of State in rejecting Opposition arguments that a refusal to register should be an inevitable consequence of the Registrar obtaining evidence of a breach of the principles, stating that:

> "After all, we are appointing a person of considerable standing- a person of the same standing as the Parliamentary Commissioner. There is no need to impose on such a person a

> duty in all circumstances to act in a particular way. We should be ensuring that that man has the necessary powers to carry out his general duties."(130)

Nonetheless, it appears illogical that the Registrar should be regarded as capable of exercising discretionary powers in 1987 but not in 1985. It has been pointed out that should a user demonstrate a disregard for the data protection principles during the currency of the initial registration period this may be taken into account by the Registrar when an application is made for renewal of the registration and also that the Act empowers the Registrar to serve enforcement or de-registration notices during the interim period although these could not take effect until November 1987.(131) It is unfortunate, however, that at the time of initial registration, when the profile of the legislation reached a peak, that any attempt to scrutinise the behaviour of users should be eschewed.

To date, as has been stated, only one application has been formally rejected by the Registrar. Given the initial limitations upon his powers so to do this fact may be of little significance. If consideration is given to the likely long term effect of the Registrar's powers, the position appears somewhat pessimistic. Again the provisions of the Consumer Credit Act are of direct relevance and it is instructive to give further

consideration to its operations. This Act provides that a licence shall be granted if an applicant satisfies the Director General that, inter alia, he is a fit person to engage in the activities covered by the licence.(132) In making this determination it is provided that the Director General is to have particular regard to the facts whether the applicant or any of his employees has been convicted of any offence involving fraud, dishonesty or violence, has contravened any provision of the Consumer Credit Act or of any statute concerned with the supply of credit to individuals, has practiced discrimination on racial or sexual grounds in connection with any business activity or has:

> "engaged in business practices appearing to the Director to be deceitful or oppressive, or otherwise unfair or improper (whether unlawful or not)."(133)

Although it might appear from this formulation that the onus is on the applicant to provide proof of his suitability and, therefore, that the requirement imposed on the applicant is more onerous than that applying under the Data Protection Act, such a consequence is avoided by the Act's provisions requiring that the Director, should he be minded to refuse an application, give his reasons for such a conclusion to the applicant. The Director has commented

that:

> "If in any individual case I were unable to quote adequate reasons for refusal, etc., backed up by the relevant evidence, I would be bound to grant the application."(134)

To a considerable extent, therefore, the powers and duties of the Director can be equated with those of the Registrar, but only on the assumption that the latter's full powers to reject applications for registration have come into force although the provision in the Consumer Credit Act permitting the Director to refuse an application on the basis of previous criminal convictions is not replicated in the Data Protection Act. The significance of this provision has been recognised by the Director who has stated that:

> "The least easily refuted evidence likely to be cited in an MTR [minded to refuse notice] consists of details of convictions and convictions which are not spent."(135)

It must be noted, however, that although the application form for a licence under the Consumer Credit Act specifically requires details of any criminal convictions involving "fraud or other dishonesty or violence" the Director has no right of access to police records in the event that an applicant

fails to disclose such a conviction. Although applicants are warned that:

> "The Consumer Credit Act provides that a person who in connection with any application, knowingly or recklessly gives information to the Director general which, in a material particular, is false or misleading commits a criminal offence."(136)

in the vast majority of cases the Director will have to base a decision upon the information supplied in the application form and, if this appears to be correctly completed, will have no option but to accept an application. Even in the event that complaints have been furnished to the Registrar concerning a data user's activities, the precedent of the Consumer Credit Act may cast doubt upon the weight which may be attached to these. The Director has commented that:

> "It is in the nature of complaints, even where these take the form of formal witness statements, that they comprise only one side of the story and are in a form where the applicant or his legal representatives are often unable to test their veracity and accuracy during the course of representations. It is also in the nature of complaints that, whilst the complainant considers that he remembers very

> clearly the transaction he is complaining about - because to him it is a special transaction - to the trader that transaction may be just one of very many and he may not be able to recollect it at all. It follows that counterstatements designed to show that the complaint is mis-conceived may raise sufficient questions about the validity of the complaint that we are unable to make a finding of fact on the issues raised. In short, it is very difficult for me to arrive at a decision which is **not** favourable to the applicant in those cases which are comprised solely of complaints."(137)

Although the Director went on to indicate that he felt that such cases would be comparatively rare the point appears apposite in the data protection context. As will be discussed later(138) the Registrar's investigative powers are closely circumscribed, data users are under no duty to comply with any requests for assistance which the Registrar may make and whilst the Registrar is empowered to approach the Sheriff with a view to obtaining a search warrant in an effort to obtain evidence of a breach of the Act he must first of all possess evidence sufficient to satisfy the Sheriff that he has "reasonable grounds for suspecting" that an offence has been committed under the Act(139). It may be noted, however, that the Registrar will have power

to refuse an application for registration if he considers that:

> "the information available to him is insufficient to satisfy him that the applicant is unlikely to contravene any of these principles."(140)

It may be hoped that the Registrar will rely on this power in the situation where he has received a complaint about a user and where the user has taken no steps to counter the allegation.

In attempting to assess the significance of the registration exercise the point may be made that the number of registration applications formally rejected may be an inadequate guide. It may be hoped that users whose previous activities might be considered to breach the data protection principles will modify their actions so as to remove the possibility of rejection. Nonetheless, if the statute is to have such a deterrent effect, users must be faced with a realistic prospect of being apprehended. The fact that only one application has been rejected makes this appear an unlikely prospect.

Judged by any criteria, it is submitted, the arrangements for registration made under the Data Protection Act are found wanting. From the data user's

standpoint the procedures will all too often appear excessively bureaucratic. Whilst the fee may be comparatively small the task of completing the documentation is a more complex one. The Registrar has reported that:

> "It is not clear what the full cost of registering is. Estimates others have made for small companies suggest at least half a day of management time."(141)

Whilst the size of an organisation can provide only a limited guide as to the sensitivity of the information held, even the expenditure of half a day appears excessive in relation to the potential dangers posed by the computerised information held by such an undertaking. As will be discussed in the following section, the approach of the Data Protection Act is flawed by its determination that whilst some users are to be totally exempted from its scope the remainder are to be subjected to its full rigours. Against this, the vast numbers of those liable to register means that there can be little realistic possibility of unacceptable data practices being identified. The high proportion of data users failing to register also has consequences for the future operation of the Act. The task of prosecuting all those who failed to register is too vast to receive serious consideration. Limited prosecutions may give the impression that those

involved have been treated as scapegoats whilst the introduction of a new system, with what must appear as the grant of immunity to those who have hitherto failed to register can only serve to foster the impression that compliance with the requirements of the legislation is a matter of small importance. To date only one prosecution has been reported of an unregistered data user, that of a garage owner who maintained computer records of his customers and their vehicles.(142)

It may also be doubted how far the existence of the Register will benefit data subjects. Even with its limited coverage, the Register is a massive document. Held in micro-fiche form its contents are equivalent to some half a million pages of text.(143) Such a work cannot be considered user friendly, a point exacerbated by the somewhat idiosyncratic indexing system adopted in the Register. If one of the aims of the Register is to assist data subjects who may be contemplating a request for subject access a much simpler document would appear perfectly adequate giving the name of the user, a contact address and a brief statement of the data held.

Legally, it must be doubted whether a scheme of registration is required under the Convention. Nonetheless, a substantial case exists for a scheme of selective registration with those users whose data

practices possess substantial implications for individual rights either on account of the scale of their activities or by reason of the nature of the data held. Once again, it is submitted, the concept of universal registration has been overtaken by technology. A system which was appropriate for first and second generation computers is less so in the third and fourth generations.

7. Exemptions

The scope of the Data Protection Act is defined by reference to the registration procedures. The Act regulates data users with data users being regarded as those who are required to register. Inevitably, certain activities and actors are excluded from the province of the legislation. In considering the scope and significance of these exemptions they may helpfully be divided into two categories. First, those justified by reference to the small scale or non-threatening nature of processing activities. The second category concerns those areas where considerations of public policy led to the determination that certain activities be carried out in conditions of such secrecy as to be incompatible with the transparency of data processing which constitutes an integral component within the concept of data protection. In respect of both of these categories, it is submitted, the approach of the legislation is open to criticism, on grounds both of

principle and of practice.

8. Minor and Technical Exemptions

The exclusion from the scope of data protection legislation of those data users perceived as operating on a small scale or whose activities pose no perceptible threat to the individual constitutes a major feature of the United Kingdom legislation. The rationale behind such a move appears to stem partly from the desire to reduce the workload of the Data Protection Registrar and also from a recognition of the bureaucratic burdens that accompany the registration process. Whilst the exemptions arising under this heading may be of limited intrinsic significance the approach adopted, when compared with alternative techniques, provides eloquent testimony concerning the motives underlying the introduction of the legislation, the perceived role of data protection and the significance afforded to the protection of individual rights.

The possibility of excluding certain categories of data user from the province of legislation is recognised in the Convention which provides for signatory states to give notice that they:

> ".. will not apply this convention to certain categories of automated personal data files..

> In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions."(144)

A list of any files so exempted is to be deposited with the Council of Europe.

Whilst the Convention places no formal limits upon the extent to which such derogation may be permitted the fact that a state making use of the above provision may not claim the application of the Convention as against other States in respect of excluded files must place limits upon the scope of its application.

Whilst recognising the malleability of information with the use to which it is put, determining whether it can confer benefit or cause harm to individuals - in the House of Lords, the Government spokesman, Lord Elton, frequently compared the quest to identify "harmless data" with a hunt for a unicorn - the justification for exemption effectively arises from a form of cost-benefit analysis with the cost of compliance being considered to outweigh the benefits provided to individuals by the legislation. Whilst this argument is not without merit its practical application, it is submitted, has proved seriously flawed.

Under the Data Protection Act data users whose

activities come within four categories are totally exempted from the requirement to comply with its requirements. These exemptions can be divided into two categories, unconditional and conditional. An unconditional exemption is offered to any individual who processes personal data purely in connection:

> "with the management of his personal, family or household affairs or ... for recreational purposes."(145)

This exemption will serve to benefit many individuals whose computer use takes the form of a hobby. But for the exemption, for example, a horse racing fan who fed details of the past form of horses and riders into his personal computer with a view to forecasting the winner of a forthcoming race would be obliged to apply for registration. The question may arise in many cases, however, where the boundary lies between a hobby and a business. If the racing information discussed above were to be used for gambling purposes then, depending upon the scale of gambling, it might be arguable that the dividing line had been crossed. Apart from the question of a user's status as an individual or as a businessman there may on occasion be difficulty in establishing whether an employee who uses his own computer for purposes related to, but not directly connected with his employment. An example might involve a policeman maintaining his own list of suspected

criminals on his own computer. Assuming that this is not done at the request of his employer it might be argued that he is pursuing his hobby and that the data is processed for "recreational purposes". Whilst this example may be somewhat extreme, the proliferation of computers has resulted in the divide between home and work becoming less and less distinct and the Data Protection Act may have difficulty in coping with the case of an individual whose work is his hobby.

In two further situations, a user will be offered exemption from the Act should he substitute an alternative form of public notification for that involved in registration. The first is dependent upon the status of the user, applying in respect of an unincorporated members club which holds data relating to its members.(146) The second applies to any user who holds such details as are necessary to distribute "articles of information" to individuals, ie a mailing list relating to magazines or other forms of publication.(147) In both cases, in order to benefit from the exemption the user will have to give every individual whose data is recorded the opportunity to object to this fact. If objection is taken the data must be removed from the record. It must be doubted to what extent use will be made of this provision. Even accepting the complexities and deficiencies of the registration process, if a user chooses to register the purposes described above he will be entitled to

continue his operations without any requirement to seek a data subject's permission or consent. Under these circumstances, registration may well be considered the preferable option. In respect of mailing lists, the point may also be made that these frequently possess economic value so that the compiler may wish to sell or rent the information contained therein. Such behaviour will be outside the scope of the exemption.

Although some doubt may be expressed concerning the utility of the preceding exemptions it is with further categories of conditional exemptions that fears concerning the adequacy of the Act's approach become most pronounced. Exemption is offered in respect of data held for one or more specified purposes, viz:

> "calculating amounts payable by way of remuneration or pensions in respect of service in any employment or office or making payments of, or sums deducted from, such remunerations or pensions; or
>
> (b) keeping accounts relating to any business or other activity carried on by the data user or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments are made by or to him in respect of those transactions or for the purpose of making financial or management

forecasts to assist him in the conduct of any such business or activity."(148)

The apparent breadth of these exemptions is mitigated by the fact that information held under these headings may only be used for that particular purpose and may only consist of such information as is necessary to attain those purposes. Thus if accounts are maintained on computer the user may benefit from the exemption. If, however, these accounts identify debtors and that information is used to determine whether, or to what extent, credit should be extended to particular debtors this purpose will move outside the scope of the exemption and the user will be required to register.

From the perspective of an employer-employee relationship, the fact that the former holds information relating to the payments made to the latter (and as to other matters arising in the course of employment which might affect such payments) is an inevitable consequence of the relationship and the fact that this information may be maintained on computer cannot, per se, affect adversely the employee's position. Information relating to financial status may be considered, however, to possess a degree of sensitivity,(149) and in recognition of this fact restrictions are put upon the disclosure of the data to a third party. Disclosures may only be made if specifically sanctioned in the legislation. In some

cases the disclosure appears unobjectionable. Thus data held for payroll purposes may be disclosed:

> "to any person other than the data user, by whom the remuneration or pensions in question are payable."(150)

This covers the situation where an employer has an arrangement with his bank whereby the payroll data is supplied to the bank which subsequently ensures that requisite payments are transferred to each employee's bank account. Such an approach reflects existing practice and would not appear intrinsically threatening to the individual. Concern may, however, be expressed at two further enabling provisions. The first applies in respect of payroll data and permits information held for this purpose to be disclosed:

> "for the purpose of giving information as to the persons in any employment or office for use in medical research into the health of, or injuries suffered by, persons engaged in particular operations or working in particular places or areas"(151)

In Parliament, it was stated that payroll records would frequently contain details of employees' absences from work due to illness and would specify its nature. Such information can clearly be of value in identifying

occupational hazards. The fact that such information may be recorded on payroll records coupled with the exemption offered to such records may be a cause of some concern. Although it must be conceded that the circumstances under which such data may be disclosed are limited; and although the recipient of the data will, assuming that he wishes to subject it to further processing, be required to register as a data user, the approach adopted may be contrasted with the provisions of the Convention. This recognises that medical data is possessed of a degree of intrinsic sensitivity and sanctions the introduction of additional controls relating to its use.(152) By contrast, albeit in limited circumstances, the United Kingdom approach removes items of medical data from the province of the legislation. Such an attitude appears to demonstrate a reluctance to take seriously the potential dangers for individuals arising from the fact that data is stored and disseminated. Whilst the context in which information is held and used undoubtedly constitutes a significant factor in assessing the scale of any threat it cannot constitute the sole factor. Once again, criticism is based not on the basis that the provision is likely to harm the individual but that it demonstrates a failure to comprehend the true nature of the informational threat.

A further exception to the prohibition against transfer of payroll or accounting data arises where:

> ".. the data subject (or a person acting on his behalf) has requested or consented to the disclosure of the data either generally or in the circumstances in which the disclosure in question is made."(153)

It is further provided in this context that the user will not violate the terms of the exemption if he makes a disclosure having reasonable, albeit mistaken, grounds for believing that the user has consented or requested that information be disclosed.(154)

At first sight, this provision appears unobjectionable. Circumstances can readily be identified in which the subject may wish that the disclosure be made, for example, a reference referring to an employee's earnings may be supplied to a bank from which the employee has requested credit. To this extent the exemption appears in the data subject's interest. Of more concern is the fact that the employee may give a general consent to disclosure. This would appear to leave the way open for an employer to require as a condition of employment that all prospective employees sign a general waiver permitting him to disclose payroll data at will. It is, of course, the case that prior to the passage of the Act there would have been no need for the employer to seek the employee's consent for any data transfers. To this extent, the Act does not weaken the individual's position. It must be,

however, a valid criticism of a measure, allegedly prompted by concern for the individual, that it does not sufficiently improve its beneficiary's position.

While the fact that certain applications are totally removed from the remit of the legislation has been criticised from the individual's standpoint, it may also be argued that the exemptions may provide comparatively little benefit to users. In relation to payroll or accounting data it has been stated by the Registrar himself that the exemptions:

> "..are likely to apply only to small businesses. Such businesses might have their own microcomputers or may have work undertaken through a general computer bureau or possible a professional accountancy firm. More sophisticated users - which will inevitably include the majority of large businesses as well as some small ones - will find that the exemption does not apply to them because they are unable to observe the conditions as to use and disclosure of the data."(155)

Given the facts that a user will have to make an initial determination whether his activities lie within or without the terms of an exemption and that he may face criminal prosecution in the event either that his initial diagnosis proves mistaken or a subsequent

action takes him outside the exemption, registration may well appear a safer option although the figures previously cited concerning the number of applications received might suggest that evasion constitutes the most "popular" option.

Consideration of the above exemptions leads to the conclusion that the United Kingdom legislation demonstrates a lack of understanding of, and committment to, the principles of data protection. In this area, the Act fails to recognise and remove potential dangers to individuals but imposes unnecessary burdens upon users. The preferable approach, it is submitted, involves not the total removal of any data user from the scope of the legislation but, rather, a tailoring of its requirements to match the scale and significance of his operations. That the legislation fails so to do is due, it is submitted, to a fundamental misapprehension concerning the requirements of the Convention.

In Parliament, an amendment was moved to the Bill which would have had the effect of exempting such data users from the requirement to register but would have obliged them to comply with the substantive provisions of the Act including the data protection principles.(156) This proposal was rejected by the Government on the basis that Article 3 of the Convention requires that a list of derogations be deposited with the Council of Europe

but that this list:

> "shall not include, however, categories of automated data files subject under its national law to data protection provisions."(157)

This provision, it was argued, required either that users be required to register or that they be totally exempted from the legislation. Such a conclusion is based upon the proposition that a scheme of registration is required by the Convention. On this analysis, whilst users could be totally exempted from the legislation the Convention would not permit exemption where some controls were imposed upon users but where these fell short of the level required under the Convention. As has been stated, it must be doubted whether the Convention imposes any such requirement and, indeed, by recognising that certain categories of data should be considered as intrinsically sensitive it provides for the level of control to be tailored by reference to the data and the category of user involved. It may be further noted that under the West German federal statute a public list is compiled only of those data users operating within the public sector. Private sector users need only comply with the substantive provisions of the statute.

The question whether a user's details should appear on a public register or be supplied only upon request

cannot be regarded as fundamental to the concept of data protection. In respect of the vast majority of data applications coming within the categories described above it must be accepted that no threat will be posed to the individual and that the fact of the involvement of the computer in relation to such activities may be considered virtually irrelevant. Throughout the debate relating to the threat of the computer the point has been made time after time that evidence of actual harm is scanty but that the task of legislation is required on a preventative or precautionary basis. Given this context it must be a cause of some dismay that the United Kingdom legislature should display such a lack of committment to the ideals of the subject. In particular, it may be considered somewhat ironic that the provisions of a Convention which is intended to promote the individual's right of access to information should be prayed in aid in order to limit accessibility.

9. Public Policy

In the previous section, consideration was given to those situations where particular categories of user, or particular forms of data processing, might be removed from the province of data protection legislation under arguments relating either to administrative convenience or the innocuous nature of the activities in question. Although the approach

adopted by the Act in utilising the provisions of Article 3 of the Convention in this respect may be contentious there is little argument against providing a less strict regime in respect of the activities in question. It is in respect of a second category of exemptions, those justified by considerations of public policy, that most controversy arises. The argument in favour of exemption can be simply put. Data protection attempts to ensure openness and accountability in respect of data processing. Some forms of processing are, however, so closely linked to the vital interests of the state that they require to be undertaken away from the public gaze. In these situations the arguments in favour of secrecy outweigh those of transparency. This claim may be most strongly advanced where the activities in question impinge upon questions of national security. As detailed in the Convention, however, the scope of public policy considerations extends beyond those of national security, it being provided that:

> "Derogation from the provisions of Articles, 5, 6 and 8 of this convention shall be allowed when such derogation is provided by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
>
> a. protecting State security, public safety, the monetary interests of the

State or the suppression of criminal offences.

b. protecting the data subject or the rights and freedoms of others."(158)

It may be noted that the Convention refers to "derogation" from its provisions. This word is defined as including the:

"partial repeal or abrogation of a law."(159)

Such terminology would appear more consistent with the limitation of the application of data protection legislation within specified circumstances rather than its complete exemption or exclusion. Such an interpretation would appear to be supported by the fact that, as will be discussed later, the phraseology of this provision is modelled on that appearing in the European Convention on Human Rights. In interpreting this document the European Commission and Court of Human Rights have on several instances refused to accept that a total withdrawl of convention rights can be justified by recourse to the dictates of national security.(160)

Although the Convention provides for special treatment to be afforded to a variety of informational practices, chiefly lying within the public sector, it is only in

respect of information held for the purposes of national security that the United Kingdom legislation totally excludes the application of the Data Protection Act. In respect of the other specified areas of activity the Act provides for limited or partial exemption from some of its provisions. The scope of these amendments will be considered in detail in the following chapter.

In respect of national security the Act provides that:

> "(1) Personal data are exempt from the provisions of Part II of this Act and of sections 21 to 24 above if the exemption is required for the purpose of safeguarding national security.
>
> (2) Any question whether the exemption mentioned in subsection (1) above is or at any time was required for the purpose there mentioned in respect of any personal data shall be determined by a Minister of the Crown; and a certificate signed by a Minister of the Crown; certifying that the exemption is or at any time was so required shall be conclusive evidence of this fact."(161)

The effects of this provision are profound. Where data

is held for national security purposes the Act is to have no application whatsoever. Although the Convention clearly provides considerable scope for exemption in this area it may be doubted whether this extends to the blanket exclusion provided under the Data Protection Act.

Initially, it may be noted that the Act essays no definition of the scope of national security. This is in line with the practice of Governments throughout the years. The traditional response of Prime Ministers faced with a Parliamentary question seeking explanation as to the scope of national security interests has been on the lines:

> "This term has been in general use for many years in a variety of contexts and is generally understood to refer to the safeguarding of the state and the community against threats to their survival or well being. I am not aware that any previous Administration has thought it appropriate to adopt a specific definition of the term."(162)

It is only in comparatively recent times that the very existence of national security agencies such as MI5 and MI6 has been officially recognised.

Data held by national security agencies can, when acted

upon, produce serious consequences for its subject. The literature and the Parliamentary debates during the passage of the Act contain numerous examples of individuals being barred from employment or subjected to minute scrutiny by customs officers when entering or leaving the country due to inaccurate information having been recorded on computer. Although few official announcements have been made concerning the informational practices carried out by national security agencies, unofficial reports indicate that the computer facilities directly available to them permit sizeable records to be maintained on a considerable proportion of adult citizens.(163)

Under the Data Protection Act any Government Minister is empowered to certify that any personal data held by any data user is held for the purpose of safeguarding national security. The breadth of this provision is in direct conflict with the recommendation of the Lindop Committee that any use of this power should be carried out by the Home Secretary as the Minister primarily responsible for internal security.(164) In principle, national security is to be regarded as anything which any government Minister considers it to be. A further cause for concern follows from the fact that certificates to this effect will only be issued after the question whether data is held for national security purposes has been raised. Whilst it may be considered undesirable that details of the categories of

information held by national security agencies and of the uses to which it is put should be available as a matter of public record it does appear unreasonable that no advance indication need be given to the Registrar of at least the organisations which are considered to operate in this field. The Act itself appears to contain what would appear a partial solution to the problem providing that the Registrar may accept an application for registration containing particulars which are expressed in general terms where:

> "..he is satisfied that more specific particulars would be likely to prejudice the purpose or purposes for which the data are to be held."(165)

Such an approach in relation to data held for national security agencies would appear capable of protecting essential secrecy whilst subjecting the operations of these agencies to a degree of accountability.

Whilst the nature of the activities of national security agencies often requires that their operations be shrouded in a deal of secrecy the UK appears unusual in the extent to which this principle is applied. Excessive secrecy may be seen as operating to the detriment of the agencies involved as well as to those who may constitute the subject of their attentions. In considering the possibility of including the operation

of national security agencies under data protection legislation the Lindop Committee identified particular problems as arising for the agencies themselves resulting from this secrecy. Whilst recognising the need for secrecy it commented that this:

> ".. leaves the security services in a hermetic compartment where they can never discuss their problems with anyone outside their own tight community; they are thus not open to the healthy - and often constructive - criticism and debate which ensures for many other public servants that they will not stray beyond their allotted functions."(166)

In order to alleviate this tendency it was suggested that:

> ".. it would be wise for the DPA to have at least some influence on any automatic processing of personal information.."(167)

Accordingly it was recommended that whilst the subject access provisions should not extend to information held by a national security agency and, whilst details of the informational practices of these bodies would not appear on the Data Protection Register, it should be ensured that:

> "... the DPA has at least one senior official with a security clearance sufficiently high for him to be able to operate in effect as a privacy consultant to the Home Office and the security services, and to work out with them the appropriate rules and safeguards for their systems."(168)

With the proposed data protection authority being replaced by a single Registrar, attempts were made in Parliament to have this function assumed either by the Registrar or by a specially appointed Deputy Registrar (Exempt Systems) whose duties would include:

> "Applying the subject access provisions .. to personal data exempted from subject access.. after representations received from a data subject."

This proposal was rejected by the Government on the ground that responsibility for national security was a governmental one and could not in any way be delegated to a non-governmental body or individual.(169) Such an approach has, however been adopted in several continental states with, for example, the French legislation requiring that all public data processing activities be notified to the National Data Processing and Liberties Commission.(170) This body is composed of 17 members consisting of members of parliament,

nominees of the government (excluding government ministers), members of the judiciary and experts in the technical aspects of data processing, the latter being appointed by parliament.(171) The Commission, having been informed of the fact that processing of personal data is carried out will make regulations laying down the conditions under which this may take place. These regulations are normally published but a power is vested in the Conseil d'Etat to ensure that:

> ".. regulations relating to certain processing affecting national security, defence and public safety shall not be published."(172)

In relation to the granting of subject access the legislation states that:

> "With regard to processing activities affecting national security, defence or public safety, the application shall be made to the Commission, which shall nominate one of its members who is or has been a member of the Conseil d'Etat, Cour de Cassation or Cour de Comptes, to conduct any appropriate investigations and order the necessary alterations. Such member may be assisted by a member of the Commission's staff.
>
> The applicant shall be advised that checks have

been made."(173)

There would appear no compelling objection as to why a similar provision should not be introduced to the UK where the provisions of the Interception of Communications Act 1985 would appear to provide an apposite precedent. This Act prescribes the circumstances under and procedures by which an individual's communications, whether transmitted by post or through the telecommunications system, may lawfully be intercepted by public agencies. As part of this system a Tribunal was established(174) consisting of 5 members each of whom being a barrister or solicitor of at least 10 years standing. Any person believing that they have, unjustifiably, been the victim of interception may request the tribunal to investigate.(175) So long as this request does not appear to be frivolous or vexatious the Tribunal must investigate with a view to determining, first whether the substantive provisions of the Act, requiring the grant of a warrant by the Secretary of State as a condition precedent for legitimate interception,(176) have been complied with and, if so, whether that grant was justified. If after investigating the complaint (utilising those principles applied by a court in determining an application for judicial review)(177) the Tribunal consider that there has been no malpractice they are to inform the complainant accordingly. This reply will be given in the event that

there is no evidence of interception or if the Tribunal consider that a warrant has been properly issued.(178) Should the Tribunal discover evidence of a breach of the Act's provisions they must so inform the applicant and, additionally, submit a report to the Prime Minister.(179) Further, they may quash any warrant which has been issued, order the destruction of any material which has been obtained pursuant to the interception and order that compensation be paid to the complainant.(180)

In addition to the Tribunal, the Interception of Communications Act establishes a Commissioner(181) who is required to monitor the operation of the warrant system. This official, who must either hold or have held high judicial office and who is appointed by the Prime Minister, may also intervene in the event that he feels that the Tribunal have inadequately investigated any complaint of unauthorised or wrongful interception, reporting his conclusions to the Prime Minister.(182)

Whilst the interception of communications is, hopefully, carried out on a smaller scale that is the case with data processing and the impact upon the individual concerned may be significantly greater, the fact that even warrants issued under the heading of national security are subject to the scrutiny of the Commissioner and Tribunal indicates that the absolute exemption contained in the Data Protection Act is not

required in the interests of operational efficiency. Rather it, once again, demonstrates a lack of committment on the part of Parliament towards the concept of data protection. Even assuming that the Registrar may not be regarded as having a sufficiently high security clearance to receive access to national security records, and even accepting that financial constraints might prevent the appointment of a full time official to investigate complaints in this area, it would appear that the membership of the Data Protection Tribunal, in particular the requirement that its Chairman and Deputy Chairman should be legally qualified, would enable these persons to perform a function similar to that of the Tribunal under the Interception of Communications Act. It may well be that some of the substantive requirements of the Act may not be appropriate where information is processed for purposes connected with national security and that partial exemption may be justified, the approach adopted in the Act is insupportable.

Turning from domestic considerations, it is necessary to consider the extent to which the approach of the United Kingdom legislation can be regarded as complying with the provisions of the Convention. In this context it is relevant to give further consideration to the background to the Interception of Communications Act. The introduction of this statute was required following the decision of the European Court of Human Rights in

the case of Malone v. United Kingdom(183) where it was held that the previous system of authorising interception of communications was in breach of the European Convention on Human Rights. The Convention requires that states respect the privacy of an individual's correspondence. Any interference with this right must be:

> ".. in accordance with the law and .. necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."(184)

Additionally, the Convention provides that:

> "Everyone whose rights and freedoms as set forth in this Convention shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."(185)

In the Malone case the Court found against the UK on the narrow ground that interceptions were sanctioned by administrative feat rather than by any legal provision.

No examination was, therefore, required of the substantive aspects of the interception procedures. The Interception of Communications Act represented a minimalist approach to this decision by creating a legal regime for authorising interceptions. The Act, however, made few substantive changes to existing practice other than establishing the Tribunal to investigate complaints of illegal interception. The extent of the requirement imposed by the Convention was at issue in the later case of Klass and Others v. Federal Republic of Germany(186) in which the defendant state's procedures were subjected to detailed scrutiny. In particular, the Court considered the extent to which an individual, whose correspondence had been intercepted, could be informed of this fact. Such a procedure is necessary if the right of redress provided by the Convention is to be of any effect. Under the relevant provisions of German law, it was required that an individual who had been subjected to surveillance was to be informed of this fact as soon after its termination as could reasonably be done without prejudicing the purposes of the investigation. In addition, all interceptions must be sanctioned in advance by an independent Commissioner who is appointed by a parliamentary committee, albeit after consultation with the government. Any material obtained through the interception is not to be handled directly by the investigating officers but is submitted first to an official, qualified to hold judicial office who will

pass on only such material as is considered relevant to the purposes of the investigation.

Considering these points, the European Court held that the German system complied with the requirements of the Convention. It recognised the legitimate call for secrecy where national security interests were concerned and that requirements of notification could not be elevated into an inviolate principle, pointing out that:

> "The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification of each individual affected by a suspended measure might well jeopardise the long term purpose that originally prompted the surveillance."(187)

Nonetheless, the Court was not uncritical of aspects of the German system(188) and it would appear from the judgment that the question of compliance was a finely balanced one. The implications of this decision for the United Kingdom and, in particular, the question whether the procedures introduced under the 1985 Act comply with the Convention are, fortunately, outside the scope of this thesis. The central issue concerns the fact that the Court were of the view that national

legislatures do not enjoy unfettered discretion in the area of national security. Whilst it was accepted that:

> "It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field."(189)

national provisions would be scrutinised in the light of the Convention's provisions. This point was also at issue in the case of Sunday Times v. United Kingdom(190) the Court considered the question whether the law of contempt of court as applied in the United Kingdom constituted a necessary restriction upon the freedom of information. Holding that it did not do so, the Court held that although national governments possessed a "margin of appreciation",(191) and that a provision would not be regarded as unnecessary "simply because it would not have been granted under a different legal system",(192) the question of necessity had to be determined in relation to the Convention with the Court subjecting the national provisions to an objective assessment as to their acceptability. More recently, in the case of Barthold v. Germany(193) the Court considered whether controls on advertising by members of a profession constituted a necessary restriction upon freedom of expression. In finding against the German government the Court referred back

to its previous decisions and commented that:

> ".. whilst the adjective 'necessary' within the meaning of Article 10(2) of the Convention is not synonymous with 'indispensible', neither does it have the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'; rather, it implies a 'pressing social need'. The Contracting States enjoy a power of appreciation in this respect, but that power goes hand in hand with a European supervision which is more or less extensive depending upon the circumstances; it is for the court to make the final determination whether the interference in issue corresponds to such a need, whether it is 'proportionate to the legitimate aim pursued' and whether the reasons given by the national authorities to justify it are 'relevant and sufficient'."(194)

Similar considerations may well apply in relation to the Data Protection Act. The provisions of the Convention on Automated Processing of Personal Data are founded in large part on the terms of Article 8 of the Human Rights Convention and permit derogation where this:

> "..constitutes a necessary measure in a

democratic society in the interests of:

(a) protecting state security, public safety..."(195)

It may be argued that the terms of the Data Protection Act, by providing for total exemption when data is held for purposes connected with national security must be regarded as unacceptably broad, especially when account is taken of the lack of parliamentary control over the operation of national security agencies and, indeed, of any definition as to what is a matter affecting national security and what agencies should be regarded as operating in this area. It would not, however, appear that such complaints could be ventilated in the forum of the European Court of Human Rights. Unlike the position under the Human Rights Convention(196) the Convention on the Automated Processing of Personal Data contains no provision for the submission of individual petitions to the Commission and the Court of Human Rights.

Finally, in considering the exemption offered in the interests of national security account must be taken of one further matter in which the provisions of the Data Protection Act are in conflict with the recommendations of the Lindop Committee. Whilst that body was prepared to afford at least a degree of immunity in respect of national security matters it recommended that where

information was disclosed to them by a third party that:

> "no exemptions should be available, even in the interest of national security, from restrictions on the disclosure of data to third parties."(197)

As enacted, the Act provides that:

> "Personal data which are not exempt under sub-section (1) above are exempt from the non-disclosure principle in any case in which the disclosure of the data is for the purpose of safeguarding national security."(198)

Once again it is provided that the issue of a certificate by a Minister of the Crown is to constitute conclusive evidence whether a disclosure was for this purpose.

Whilst the Lindop proposals may be considered unduly restrictive, the effect of the above provision is to give national security agencies, which are not subject to any form of scrutiny under the legislation, access to any information held by any user on the ground that this is for the purpose (not even that it is considered necessary to safeguard) of national security.

10. The Future of Control

The processing power of large scale computer systems is, today, such as to create a vast imbalance of power between the individual and those who control the record keeping process. The portability of computerised data serves to break down barriers which might previously have existed between the public and the private sectors with information originally collected for the purposes of one subsequently being transferred to another. In an effort to reduce imbalances of power and to alleviate public fears concerning the development of a 'Big Brother' society, data protection legislation contains, as a major component, provisions designed to develop a measure of public accountability and control. These take two forms. Firstly, the appointment of a supervisory agency. A variety of approaches have been advocated delineating the composition, the role and the powers of such an agency. The solution arrived at will depend in large part upon the political and legal traditions of the particular state but it seems clear that the greater the independence of the agency and the more substantial are the regulatory powers vested in it, the more restricted will be its remit. As the British experience demonstrates, there is a reluctance on the part of Government to transfer powers, or even influence, in matters of national security to a non-governmental agency. The resultant restriction of the scope of the legislation may serve to undermine public

confidence in the effectiveness of the supervisory agency if it is unable to intervene in matters which may have the most severe consequences for affected individuals.

If comment concerning the scope of the legislation and the remit of the supervisory agency has to be moderated by recognition of the fact that data protection has to co-exist with existing constitutional and administrative arrangements, a more critical view can be taken of the introduction of systems of licensing or registration. The registration scheme adopted in the Data Protection Act, in common with those applying in other European states, has been overtaken by the remorseless advance of computerisation. The notion of registration, with its concentration on the use to which computers are put rather than to the equipment involved or the scale of the operations, may have been appropriate in the era of mainframe machines but cannot be so regarded in the age of the personal computer. In the early stages of the data protection movement computerised data banks were regarded as posing particular threats to individual privacy and liberty. At that stage the storing and processing capabilities of computers could only be economically or efficiently utilised by large scale users for significant purposes. The link between computers and the danger of informational abuse was thus clear and unbroken. Even in the 1970's, however, it could be argued that the

argument ran from conclusion to theory; that much sensitive information was held on computers by agencies who could use this information to the detriment of individuals, that the storage and processing capabilities of computers placed more power in the hands of those agencies and, therefore, that the computer posed a novel threat to individual privacy. As we move towards the 1990's a different picture emerges. The use of computers has become the rule rather than the exception. The steady reduction in the cost of computer power and the increase in the user friendliness of the equipment has served to introduce the computer to the most mundane areas of life. The basic thesis remains valid. Where information is placed in the hands of those who are in a position to use it, whether by accident or design, to harm others; the capabilities of the computer add a powerful weapon to their armoury. In this situation the case for stringent legal controls, perhaps extending beyond registration towards licensing, is unanswerable.

Whilst the argument might be put that certain forms of small computer should be excluded from the scope of the legislation it must be recalled that even the smallest personal computer may have a processing capability equivalent to that of the mainframe machines of the previous decade. If these earlier machines were considered sufficiently threatening to call for the imposition of legal controls it can hardly be argued

that the threat has become any less. What may more convincingly be challenged is the view that systems of universal registration or licensing imposed on computer users provide the optimum, or even a credible, solution. Any exemption from registration cannot be based on considerations of the particular equipment used but if regulation of those data users whose activities are capable of threatening individual privacy is to be in any way meaningful the limited resources of the Registrar must be targetted on them.

It may well be that a logical and consistent form of control over data users may prove a chimera. If, however, consideration is given to the situation with manual records a partial solution may begin to appear. The fact that the Data Protection Act applies only to computerised records has been a source of considerable controversy. In addition to the argument that some forms of manual records may themselves pose dangers, problems arise through the use of hybrid systems where part of the information - often in the form of an index - is stored on a computer with the remainder recorded in manual form. In such a situation only the computerised part of the record will be subject to the constraints of the Data Protection Act. In resisting moves to extend the scope of the Act to cover manual records the Government argued that the registration scheme provided for in the Act would be incapable of coping were the controllers of manual records to be

required to register. This must be the case but the effect of this treatment is to provide an incentive to users either to develop hybrid systems with sensitive or controversial data being maintained in the manual component or, alternatively, to withdraw such information from a computerised data base and institute a parallel manual system. In France, the approach which has been adopted to this problem has been to exempt manual systems from any requirement to register but to require that they comply with certain of the statutory data protection principles. Such an approach recognises the fact that, today, the medium upon which records are stored has become almost immaterial in determining the extent of the threat which they may pose but that the registration process cannot be universally applied. A similar approach could pay dividends for both data users and data subjects within the UK, although this may require a degree of modification in respect of some of the data protection principles, for example, that restricting disclosures of data to those coming within the range specified at registration. Were the requirement to register to be limited to large scale data users, with a discretionary power vested in the Registrar to extend the requirement to register to users coming within specified other categories, it would be possible to exempt the remaining users from the requirement to register but retain the requirement that they comply with the data protection principles. Any breach of these would bring the panoply of the

Registrar's powers and sanctions into play. For the future, it is submitted, just as the level of any threat posed by information can only be determined by reference to the context within which it is held or used, so the level of supervision needs to be tailored more precisely to particular informational practices. Currently, the inappropriateness of the definitions contained in the Data Protection Act (in common with those found in other statutes) result in an over-emphasis on the technology and inadequate regard to the uses to which information is put.

Footnotes

1. Supra pp.45-9.

2. S.2(b) adding a section 552a to Title 5 United States Code.

3. Supra p.37.

4. Art 3(1).

5. Art 2(a).

6. Art.2(c).

7. Art.3(2)(c).

8. S.1(2).

9. S.1(3).

10. S.1(7).

11. The Act is stated as applying to data users and to those operating a "computer bureau". This phrase is defined as encompassing the provision of facilities permitting personal data controlled by another person to be processed.

12. Clause 62.

13. Official Report (Standing Committee E) 6 March 1984 Col 1759.

14. Sunday Times 10 May 1987.

15. Datacard 8000. It is a minor indication of technological progress that a similar product was marketed in 1987 with a 4,000 character memory. In the course of less than a year, the size of the memory doubled whilst the price of the unit remained constant.

16. Quantum Science Corporation report, published in 1985.

17. Cmnd 5012 Supra para 578.

18. Supra paras 3.01-3.21.

19. S.1(2).

20. S.1(7).

21. S.1(3).

22. Official Report (Standing Committee H) 9 February 1984 Col 46.

23. Official Report (Standing Committee H) 14 February 1984 Cols 49-50.

24. Official Report (Standing Committee H) 9 February 1984 Col 34.

25. Official Report (Standing Committee H) 14 February 1984 Col 52.

26. Guideline No.1 p.13.

27. Questions and Answers on the Data Protection Act. Q.15 p.11. See also, Official Report (Standing Committee H) 21 February 1984 Cols 124-5.

28. A full or free text data base permits data to be entered in an unstructured form with the program being capable of searching all the data with a view to finding those items which correspond with a user's commands.

29. Infra pp.291-4

30. The Norwegian Data Protection Act states in paragraph 1 that it is to apply when "personal information is systematically stored".

31. Infra p.186 et seq.

32. Art.13(1).

33. Art.13(2).

34. Supra p.76.

35. Simitis Data Protection - Experiences and Tendencies. 1985 Law/Technology 3 at pp 11-12.

36. Hummer, in Transnational Data Regulation, the Realities. Online Conferences 1979.

37. Cmnd 7341 Supra para 19.18

38. Miller. The Assault on Privacy. Ann Arbor Press 1970. p.229.

39. Ibid p.230.

40. US Congress. Legislative History of the Privacy Act of 1974 s.3418 (Public Law 95-379) Washington DC September 1976.

41. Ibid p.169.

42. Goode. Consumer Credit Legislation. 1980 p.I/103.

43. For example, the Conseil d'Etat.

44. Established under s.1 of the Parliamentary Commissioner Act 1967.

45. Appointed under s.1 of the Fair Trading Act 1973.

46. Supra para 20.21.

47. Simitis Supra Note 39 at p.13.

48. See Flaherty. On Making Data Flow Effective. 9 Transnational Data and Communications Report (1986) 15; in which it is argued that the model of a single commissioner possessing advisory power constitutes the most effective form of supervisory regime.

49. 443 Official Report (House of Lords) 19 July 1983 Col 1376.

50. 438 Official Report (House of Lords) 10 February 1983 Col 1381

51. Sieghart, in Data Protection - Perspectives on Information Privacy, Bourn and Benyon (Eds) University of Leicester, 1983 at pp.43-4.

52. Beyond compiling and maintaining the Data Protection Register and submitting an annual report on his activities to Parliament, there would appear to be no further precise and unqualified duties imposed upon the Registrar.

53. S.3.

54. S.3(5).

55. Cl.3(5) (1982 Bill).

56. Cl.3(5) (1983 Bill as introduced in the House of Commons).

57. 61 Official Report (House of Commons) 5 June 1984 Col 220.

58. A Government amendment was tabled at the Report stage.

59. S.3(5).

60. Second Report of the Data Protection Registrar, pp.41-2.

61. Schedule 3 and the Data Protection Tribunal Rules SI 1568, 1985.

62. S.13(1).

63. S.13(2).

64. First Report of the Data Protection Registrar, p.4.

65. S.3(2) and Schedule 2 Para.1(1).

66. S.1

67. S.3 and Schedule 2 Paras.1-7.

68. Supra Note 52.

69. See 9 Transnational Data and Communications Report (1986) 16.

70. The underlying purpose behind this provision is to render the Parliamentary Commissioner immune from criticism during supply debates in the House of Commons.

71. Sch.2 para.3.

72. Sch.2 para.4.

73. Sch.2 paras.4(2) and (5).

74. Official Report (Standing Committee H) 1 March 1984 Cols 223-4.

75. S.3.

76. Official Report (Standing Committee H) 1 March 1984 Col 229.

77. Ibid.

78. There would appear some evidence of a desire on the part of the local government Commissioners for an increase in their powers. See 'Your Local Ombudsman.' Report for the year ended 31 March, 1984 and, e.g., investigation 994/C/81..

79. Local Government Act 1974 S.23. In Scotland, a single Commissioner has been appointed under s.21 of the Local Government (Scotland) Act 1975.

80. Third Report of the Data Protection Registrar p.49.

81. Ibid pp.3-6.

82. S.2(4).

83. Report of the DHEW's Advisory Committee on Automated personal data Systems. DHEW Publication No. (OS)73-97. 1973.

84. Art.8.

85. Explanatory Report.

86. Sec.10.

87. S.13.

88. Cmnd 8539 para.23.

89. Supra para 19.07.

90. A comparison may perhaps be drawn between the conditions under which driving and television licences may be obtained.

91. S.4(1).

92. 40 Official Report (House of Commons) 11 April 1983 Col 558.

93. S.42 provided for the Secretary of State to fix the date for commencement of the registration process. The Data Protection Act (Appointed Day) Order 1985 SI No.1055 performed this function.

94. S.1(5).

95. S.1(6).

96. Supra p.186 et seq.

97. S.4((3).

98. S.4(4).

99. S.5(5).

100. Official Report (Standing Committee H) 21 April 1983 Col 39.

101 Second Report of the Data Protection Registrar p.5.

102. Institute of Data Practitioners and Managers. Cited in Official Report

(Standing Committee H) 6 March 1984 Col 271.

103. Second Report of the Data Protection Registrar p.5.

104. Ibid.

105. Supra Note 94.

106. Ibid.

107. Notes of Guidance p.7.

108. Application Form Oct(86).

109. 9 Transnational Data and Communications Report (1986) No. 8 p.26.

110. Data Protection (Fees)(No.2) Regulations 1987 SI 1507 s.3.

111. Supra para 19.67.

112. 439 Official Report (House of Lords) 22 February 1983 Col 740.

113. S.21.

114. S.192 and Sch.3.

115. S.21 and s.145.

116. Consumer Credit (Commencement No 1) Order 1975 SI 2123.

117. Consumer Credit (Commencement No 2) Order 1977 SI 323.

118. 13th Report of the Director General of Fair Trading. June 1987.

119 Borrie. The Development of Consumer Law and Policy - Bold Spirits and Timorous Souls. Stevens 1984.

120. S.7(1).

121. S.7(2).

122. Second Report of the Data Protection Registrar p.22.

123. Ibid p43.

124. Ibid p.23.

125. S.8(2).

126. S.7(1).

127. S.42(2).

128. Third Report of the Data Protection Register p.8.

129. Supra p.35.

130. Official Report (Standing Committee H) 8 April 1984 Col328.

131. S.42(2)(b).

132. S.25.

133. S.25(2)(d).

134. Borrie. Licensing Practice Under the Consumer Credit Act. 1982 JBL 91 at pp93-4.

135. Ibid p.95.

136. See, for example, application form (Oct 86) p.8.

137. Supra Note 134 at pp95-6.

138. Infra pp.291-4.

139. Sch.4.

140. S.72(c).

141. Second Report of the Data Protection Registrar p.7.

142. 4 Applied Computer and Communications Law No.9, p.8 (1988).

143. First Report of the Data Protection Registrar p.8.

144. Art.3(2)(a).

145. S.33(1).

146. S.33(2)(a).

147. S.33(2)(b).

148. S.32(1).

149. Supra p.6

150. S.32(3)(a).

151. S.32(3)(c).

152. Art.6.

153. S.32 (3)(d).

154. S.32(3)(e).

155. Guideline No.6 p.13.

156. 443 Official Report (House of Lords) 21 July 1983 Col 1328.

157. Art.3(2).

158. Art 9(2).

159. Shorter Oxford English Dictionary.

160. See Infra pp.211-16.

161. S.27.

162. 56 Official Report (23 March 1984) Col 591.

163. See, for example, Campbell and Connor op cit Chap.10.

164. Supra para 23.22.

165. S.7(3).

166. Supra para 23.21.

167. Ibid para 23.22.

168. Ibid.

169. Official Report (Standing Committee H) 28 February 1984 Cols 184-208.

170. S.15.

171. S.8.

172. S.20.

173. S.39.

174. Schedule 1.

175. S.7(2).

176. S.7(3).

177. S.7(4).

178. S.7(7).

179. S.7(4)(b).

180. S.7(5).

181. S.8.

182. S.8(5).

183. 7 E.H.R.R. 14.

184. Art.8.

185. Art.13.

186. 2 E.H.R.R. 214.

187. Ibid p.236.

188. Ibid pp.234-5.

189. Ibid p.232.

190. 2 E.H.R.R. 245.

191. Ibid p.275.

192. Ibid p.277.

193. 7 E.H.R.R. 383.

194. Ibid p.402.

195. Art.9(2).

196. Art.

197. Supra para.23.25.

198. S.27(3).

Chapter Four

The Data Protection Principles

The Data Protection Principles

1. Background

Assuming that a data user is able to secure admission to the register his major continuing obligation will be to conduct his data processing in a manner which is compatible with eight data protection principles laid down in the Act. These principles mirror to a considerable extent those recommended by the Younger(1) and Lindop(2) Committees and are also intended to satisfy the requirements of the Convention. The principles cover matters which are fundamental to the concept of data protection and, as such, can be regarded as the technological equivalent of the ten commandments. It is perhaps a mark of technological progress that whilst ten rules should be required to regulate human conduct eight are considered to suffice for computers. Given the significance attached to the principles it may be a cause for some surprise that, although reference is made to them throughout the Act - and two of the principles are further defined within the main text of the legislation - the principles themselves are relegated to one of the Schedules. Although the approach of compiling a discrete collection of statements of acceptable processing practice is in line with that adopted by the Younger and Lindop Committees (and, indeed, with the original

Council of Europe Recommendations) the approach of the United Kingdom legislation must be contrasted with that of the Convention where provisions, equivalent to those found in the Data Protection Act, constitute an integral part of the text.

Reference has previously been made to the basis and content of the principles advocated by the Younger and Lindop Committees.(3) It is significant to recollect that the Younger Committee envisaged that compliance with their principles would be voluntary and, to this extent, their recommendations sought to encapsulate the best of existing industry practice. Although the imposition of a legal obligation to comply with the principles may well require changes in practice for some users, in terms of their general impact they may be seen as an evolutionary rather than a revolutionary development.

As contained in the Data Protection Act, but taken almost verbatim from the Convention, the principles require that:

> "1. The information to be contained in personal data shall be obtained, and personal data shall be processed fairly and lawfully.
> 2. Personal data shall be held only for one or more specified and lawful purposes.
> 3. Personal data held for any purpose or

purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes

4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

5. Personal data shall be accurate and, where necessary, kept up to date.

6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7. An individual shall be entitled-

(a) at reasonable intervals and without undue delay or expense

(i) to be informed by any data user whether he holds personal data of which that individual is the subject; and

(ii) to access to any such data held by a data user; and

(b) where appropriate, to have such data corrected or erased.

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data."(4)

It is, additionally, provided that:

> "The Secretary of State may by order modify or supplement those principles for the purpose of providing additional safeguards in relation to personal data consisting of information as 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.."(5)

The extent to which certain items of data should be regarded as possessing an exceptional degree of sensitivity and whose processing should, therefore, be subjected to exceptionally stringent controls constitutes a significant issue within the context of data protection legislation. Although it is a basic tenet of the legislative approach that information, per se, is a neutral concept with any harm or benefit arising from the use to which it is put it seems apparent that some forms of information are more sensitive and potentially harmful to the individual than others. As with definitions of privacy, however, a major difficulty arises in attempting to specify the scope of the concept of sensitive data.(6) Although individual and national perceptions will vary, the

Convention identifies a number of categories of information as being of particular sensitivity and provides that:

> "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."(7)

The above provision is not as restrictive as might initially appear to be the case; it having been interpreted as permitting the imposition of additional safeguards but, requiring, only that the general provisions of data protection legislation should be enforced in these areas. To date, it is the latter approach which has been adopted under the United Kingdom legislation with the power to supplement the principles only being exercised in one area. An alternative approach has been adopted or has been proposed in several other signatory states. Under the Greek Data Protection Bill, for example, information is divided into three categories, personal data, confidential personal data and strictly personal data. Whilst personal data may be processed in a relatively unrestricted fashion, that of confidential personal

data is subjected to a substantial measure of restriction and in respect of strictly personal data, defined as including:

> ".. all personal information relating to to political and philosophical convictions, sentimental and sexual life, as well as membership and involvement in political parties and in political and trade union organisations."(8)

it is provided that processing:

> ".. is absolutely forbidden except for those cases where express provisions of this law determine the purpose of the processing, the control body and the methods of collection and processing of the data."(9)

Whilst the significance attached to information relating to political or trade union matters under the Greek proposals may well be traced to that country's recent experience of military dictatorship, and the view that the recording of political affiliations poses a substantial threat may not be shared by many in Britain with its long and unbroken tradition of democratic political institutions, the illustration serves to demonstrate the manner in which certain forms of processing may be subjected to a special and

extremely restrictive legislative regime. Again, under the Hessian Data Protection Act of 1986 it is provided that where data is held in connection with employment the user must submit to the State Data Protection Commissioners details of the information stored and of the equipment which will be used.(10) Although the Commissioner has no power to refuse permission to process data, the statute provides that he is to be entitled to deliver an opinion on the proposed processing which, together with the details of the proposed processing is to be:

> ".. forwarded to the personnel representatives for the purposes defined in the regulations on staff participation."(11)

Under German labour law extensive rights of co-determination are granted to employees.(12) In addition to restricting the general processing of personal data, a distinction is drawn between general personal employee data and sensitive information, providing that:

> "Efficiency reports, personnel assessments as well as medical and psychological reports concerning employees shall not undergo automatic processing."(13)

Whilst the provision here may well be motivated by the

desire to free the individual from the sense that substantial aspects of his life are controlled by a machine, once again there is clear recognition that certain forms of activity may be inherently undesirable.

Whilst the context within which information is held and used will always be the major factor in determining the sensitivity of informational practices it is, it is submitted, possible to identify combinations of information and user which pose special threats and which should be subjected to more stringent controls, extending in some cases to a prohibition against processing, than those which are applicable to the bulk of data users. Decisions of this nature must be for the legislature taking account of the social traditions and political and historical developments in a particular state. In the case of the United Kingdom, it may be considered unfortunate that the opportunity was not taken to make such provision.

In broad terms, the data protection principles restrict a data user's freedom of action in a variety of areas. The first principle refers directly to the manner in which information might be obtained. Further provisions refer to the manner and circumstances in which the information may be stored and, in a somewhat indirect fashion, to the processing to which it might be subjected. Next, controls are placed upon the extent to

which information held by one user may be disseminated to a third party. Finally, in addition to imposing obligations upon data users the principles, in line with the notion of transparency underlying the concept of data protection, confer a right of access to personal data upon data subjects. Although, in comparison to the situation under the Lindop proposals, the point is not explicitly recognised, in their terms the principles can be seen as acknowledging the tension that exists between competing claims in the data processing field. In particular, a conflict may arise between the demand of the data user to seek information (a right guaranteed to natural persons by Article 10 of the European Convention on Human Rights) and the data subject's claim to at least a measure of control over practices which directly impinge upon his own interests.

In the main, the data protection principles constitute vague and somewhat elusive admonitions as to the standards of conduct which may be required of data users. This is not, per se, a cause for criticism. In introducing their proposed data protection principles, the Lindop Committee stated that:

> "..we regard them as means to an end, rather than as ends in themselves."(14)

The ultimate end of data protection must, of course, be

the satisfactory regulation of processing activities taking into account the needs and aspirations of both data users and data subjects. To attain this end the principles need to be interpreted and applied in the context of specific processing activities. In itself, this may be considered as another form of the transparency of processing. Both data users and data subjects must be able to calculate in advance the likely impact of the legislation upon particular processing activities. To this end, the principles clearly require to be supplemented by more precise formulations. Under the United Kingdom legislation detailed guidance as to the scope and meaning of the principles as applying to particular categories of user is likely to come about in three ways. In the case of some of the principles a measure of further guidance is to be found in the text of the Act itself. Secondly the Registrar and Tribunal have significant roles to play in interpreting and applying the principles in particular situations. Finally, the legislation envisages that codes of practice may be devised detailing the rights and obligations of parties within specific sectors of data processing.

2. The Data Protection Act

Attached to the data protection principles is an interpretation section. In the case of several of the principles this offers little precise guidance as to

their scope. For the first, third and seventh principles, however, reference is made to provisions within the body of the Act. These principles refer to the acquisition of personal data, its disclosure to third parties and the grant of subject access. The subject access provision will be considered in the following chapter.

In determining whether any breach of the first principle has occurred it is provided that account shall be taken of the fact:

> ".. whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed."(15)

Moving beyond this, the Act itself provides that, in respect of their designated functions, the police and taxation authorities will enjoy immunity from the threat of any action by the Registrar alleging a violation of the first principle.(16) In common with many aspects of the legislation, analysis of the motives behind and the scope of this provision is indicative of the government's general attitude towards the concept of data protection.

The first principle lays down two criteria for judging the acquisition of data; fairness and legality. In

justifying exempting the police and taxation authorities from the obligation to conform to these standards it was stated in Parliament that the value of information obtained by the police and taxation authorities might frequently depend on the data subject being unaware of its possession. This might well involve misleading or deceiving the data subject, factors specifically referred to in the interpretation section. Again information may be acquired as the result of a conversation being overheard, either by accident or design, and either by a police or revenue officer or by a member of the public. Such behaviour might well be considered unfair in terms of the first principle.

Whilst the public interest in efficient policing (and revenue gathering) may well call for an amelioration of the fairness component of the principle (although this has in any event to be interpreted in the context of a particular user's activities and it may be that the actions described above would not be considered unfair) there appears no case for the further provision preventing the Registrar from taking action in the event that data is obtained unlawfully. The Data Protection Act does not, of course, sanction illegal activities. In the event, for example, that a police authority engage in telephone tapping without obtaining the appropriate warrant there will be a breach of the Interception of Communications Act 1985. Such conduct

will constitute a criminal offence sanctions may be imposed under the terms of the Act and an order may be made by the Tribunal established thereunder for the destruction of any "copies of the intercepted material".(17) It would not appear that an order made under the provisions of the 1985 Act could extend to any information which had been culled from the intercepted material and subsequently incorporated in police computer records. Although such information must have been obtained unlawfully the Registrar is powerless to take action. Even accepting that there may be circumstances under which it is necessary that information, the acquisition of which is albeit tainted by illegality, should be retained, two criticisms can be made of the Act's approach. It may, first be noted that in responding to criticism of the scope of this provision the Government stated that:

> ".. we are not authorising the police to do anything in the Bill. We are merely saying that in certain circumstances it would not be right for the Registrar to have power to delete data"(18)

The key word in the above passage is "power". Although the statute charges the Registrar with the general duty of promoting the observance of the principles he retains near total discretion both as to whether to take action in any particular case and as to the form

which such action should take. The Registrar is nowhere required to order the destruction of material. Whilst it is not argued that the Registrar should turn a blind eye to infringing conduct, performance of his functions necessarily involves a degree of interpretation and the balancing of interests. It has been commented that:

> "The whole reason for having a Registrar is that there is someone of immaculate pedigree in whom the public as data subjects and society generally can place confidence so that we can give the Registrar the task of monitoring precisely how exemptions .. should be operated."(19)

Such a paragon must surely be considered capable of exercising discretionary powers in a reasonable manner. Public confidence in the efficacy of the Registrar cannot be enhanced when he is so clearly considered incapable of exercising discretion in such a significant area.

The second criticism of the legislation's approach accepts as a starting point the proposition that the Registrar should not be permitted to order the destruction of data which has been unlawfully obtained. Even with such a concession, however, there can be no satisfactory justification for denying the Registrar the right to take such behaviour into account in his

future dealings with the authority in question. The result is that even should a police or taxation authority openly proclaim their intention to institute record systems based on illegally obtained information, in a notorious phrase, "to bug their way around London" no sanctions would be available to the Registrar.

Whilst conflicts may, and do, arise in respect of any form of data processing they are highlighted in the areas currently under discussion. One the one hand are activities of the state which may directly and significantly affect the financial and physical situation of individuals. Their justification stems from the general public interest in crime prevention and detection and in the efficient collection of the public revenue. Against this has to be balanced the interests of the individual whose activities are the subject of official attention. It would be facile and disingeneous to suggest that the resulting conflicts of interests are susceptible of easy or precise resolution. Where the legislation can, it is submitted, justifiably be criticised, is in its failure to address the issue in any considered or meaningful fashion. In this - as in other areas - the Act appears more concerned with protecting data held by official agencies than on protecting those who constitute its subjects. The protection of data is substituted for data protection.

Moving from the acquisition of information to considerations as to its use, the third data protection principle enshrines the general rule that:

> "Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."

Control over the uses to which data may be put constitutes an essential component of data protection legislation being intended to promote public confidence in the fact that information supplied or obtained for one purpose will not be used for another without their knowledge. The third data protection principle proclaims that data transfers should be a matter of public record. In addition to the underlying concept described above a provision along the above lines was required if the Act were to comply with the requirements of the Convention that personal data should be:

> "stored for specified and legitimate purposes and not used in a manner incompatible with those purposes."(20)

Other than the requirement that the data be stored for a legitimate purpose neither the Convention not the Act set out to restrict the activities of data users. The

Act requires simply that a user give notice at registration of the extent of his processing activities and the range of dissemination of any personal data which he may hold, thereafter restricting his processing to these areas.

A user having specified the circumstances under which he may disclose data to a third party, it is, of course, possible that circumstances may change or a situation may arise which was not envisaged at registration. It is, of course, possible that the user's entry on the Register might be modified in the light of changing circumstances. Such a procedure cannot be immediately accomplished and the Act and the Convention recognise that there may be occasions where an unauthorised disclosure requires to be made in circumstances of urgency. The Convention provides, however, that national legislation may only waive the prohibition against unauthorised disclosure to the extent that this constitutes a:

> "..necessary measure in a democratic society in the interests of:
>
> a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
>
> b. protecting the data subject or the rights and freedoms of others."(21)

The use of the word "necessary" in this context reflects its appearance in several articles of the European Convention on Human Rights. The interpretation placed upon this word by the European Court of Human Rights has previously been discussed.(22) Although the treatment afforded to the information handling practices of the police and taxation authorities falls well short of total exemption from the Act, and can thus accurately be described as a "derogation" the question remains whether the scope of the derogation exceeds that which is "necessary". Although circumstances can be identified under which disclosures would be compatible with the values of the Convention, the Act's approach which creates the prospect of exemption in favour of the disclosure of data relating to the most trivial of offences, might be considered a measure disproportionate to the danger involved and, therefore, beyond the legitimate scope of the exemption. This aspect of the legislation has been the source of considerable controversy with the Chairman of the Data Protection Committee, Sir Norman Lindop, stigmatising the legislation's approach as "perpetrating a fraud on the public".(23) This criticism is based upon the argument that whilst the legislation purports to assure the public that no secretive disclosures of personal data may be made its provisions permit such practices to continue.

As has been indicated above, the most controversial

exemption from the non-disclosure principle has proved to be that applying to disclosures to the police or taxation authorities. Here, it is provided that the principle is not to apply(24) where the disclosure is in connection with:

> "(a) the prevention or detection of crime;
>
> (b) the apprehension or prosecution of offenders; or
>
> (c) the assessment or collection of any tax or duty."(25)

and where the application of the non-disclosure principle would be likely to prejudice any of these matters. It will be noted that this formulation does not expressly limit disclosures to the police or taxation authorities. It would appear that, for example, disclosure to a private detective might come within the ambit of the exemption.

The effect of this provision has been stated as giving the relevant authorities access to to any computerised data bank in the country. Against this it has been argued that by granting the exemption the Act does:

> "not give the police or any body any new powers. The police are given no powers to compel users to divulge information. This is a Data Protection Bill, not a data disclosure

> Bill. Clause 28(2) states only that whereas normally the user must not disclose personal data for a purpose not specified on the register, he may do so if he has reasonable grounds for believing that failure to disclose the information will be likely to prejudice, for example, the prevention or detection of crime. It is his decision and his decision alone."(26)

The statement that the Act does not take away any existing rights is one which is undeniably correct, although it appears a somewhat strange claim to be made in the context of a measure which, in the Government's own words, was introduced in order to "meet public concern". In addition, just as a justification advanced for restricting the scope of the Act to computerised data banks related to the increased threat perceived in the operation of these systems to individual freedoms, so it may similarly be argued that faced with the linkage potential of modern computers the retention of the status quo in respect of disclosures to the police or taxation authorities is not an acceptable option. It may further be argued that although the Data Protection Act does not place any new powers in the hands of the authorities or impose any duties upon those who hold information that the practical impact may be different. A distinction may be drawn between the previous situation where no legal provision existed to prevent

disclosure and the situation under the Act whereby disclosures are specifically legitimised. It has been commented that:

> ".. although this kind of disclosure is perfectly possible under existing law, what the Bill will mean in practice is that these disclosures - sanctified, as it were, by the permissive powers of the Bill - will become the norm."(27)

The exemption provided in the Act encompasses two possible forms of disclosure, those volunteered by the data user and those in response to a request from a relevant authority. Whilst circumstances no doubt exist under which both forms of disclosure may be justified and recognising the need for legislation to attempt to reconcile conflicting interests it is submitted that the approach contained in the Act provides inadequate safeguards for individual rights. In particular it may be argued that the criteria laid down in the legislation as justifying disclosure are excessively wide. The term "crime prevention" appears extremely broad and it is difficult to conceive of any item of information which could not be regarded as coming within its purview when the potential criminal in the United Kingdom is presented with a menu of some 7,000 offences.(28) Although it is further required that observance of the principles should be likely to

prejudice these functions it is, again, difficult to conceive of situations where denial of information could not be regarded as resulting in some degree of impairment.

The major criticism of the approach adopted in the Act relates to the breadth of the exception. The issue whether exemptions should be broadly or narrowly drawn is highlighted by an example put forward by the Government demonstrating how the exemption in favour of crime prevention might operate to the benefit of the individual. The situation was postulated where:

> ".. the police might have word that a man's life had been threatened and that an attack against him was planned. the police might go to the person's employer - possibly in the middle of the night - to find out the person's address so that they could get in touch with him, provide him with the necessary protection and thus deter the would be attackers."(29)

Whilst the benefit to the data subject of disclosure is clear in the above situation, it may be noted that the Act further provides that:

> "Personal data are exempt from the non-disclosure provisions in any case in which the disclosure is urgently required for preventing

injury or other damage to the health of any person or persons."(30)

This provision would appear perfectly adequate to cope with the situation described above. Although other situations may be envisaged along similar lines where the physical integrity of an individual may not be at issue, for example when an attack on property is involved the blanket immunity offered in the Act appears to pay inadequate regard to individual rights. Whilst accepting the need for the option of disclosure to be offered to a data user two alternative approaches would appear to offer a more equitable solution. First, the application of this provision could be restricted to the situation where investigations were being made into a serious criminal offence. For this purpose, it has been argued, the Data Protection Act should adopt the approach of the Police and Criminal Evidence Act 1984 which introduced the concept of a "serious arrestable offence", this being defined by reference to a variety of specified offences and, more subjectively by reference to specified criteria, viz whether the resultant consequences of the conduct in question are likely to include:

"(a) serious harm to the security of the State or to public order;

(b) serious interference with the administration of justice or with the

investigation of offences or of a particular offence;

(c) the death of any person;

(d) serious injury to any person;

(e) substantial financial gain to any person; and

(f) serious financial loss to any person."(31)

Such an approach would obviously impinge to some extent upon the effectiveness of criminal investigation or tax collection. Such a situation is by no means unprecedented with restrictions being placed upon the freedom of action of these authorities in the interests of individual liberties. Thus it was argued that:

"..we are dealing with the balance of the argument - the balance of public interest - and, therefore, the balance of the desirability of including with that one, possibly isolated case of value, many thousands of cases that would be of no value to public safety or security, but which could be most invidious to individual data subjects."(32)

On this occasion the issue of balance is specifically raised by the Government yet, once again, the legislation eschews any genuine attempt to confront the complex issues involved. In rejecting the case for a restriction upon the scope of these exemptions the

Government based their case upon the argument that it would place data users in a difficult position were they to have to decide when faced with a request for disclosure, whether the request related to a "serious arrestable offence". The Minister of State commented that:

> ".. the data user would have to say to himself, "I had better find out first of all whether the police are seeking a "serious arrestable offence". Perhaps they are after an offence, but it may not be a "serious arrestable offence".... I had better not give the police the help they are asking for because if I do I could be guilty of an offence.."(33)

Initially, it may be commented that it must be doubtful whether a user who passed on information under a misapprehension as to the purpose for which the disclosure is made will commit an offence. Under the terms of the Act it is provided that an offence will be committed only when a user discloses data outwith the scope of his registration where he does so "knowingly or recklessly".(34) Although there may be doubt as to the forms of conduct which will be characterised as "reckless" it may be doubted whether a user who responds to a request from a relevant authority will be exposed to any significant risk of prosecution even if the disclosure does not come within the scope of the

exemptions. The point should also be reiterated that the Registrar has considerable discretion in determining whether to take action against a data user who he considers has acted in violation of the data protection principles. It would not appear unreasonable for this discretion to be exercised in favour of a user who made a disclosure in the genuine belief that it was justified.

In the final resort, the Government's arguments against imposing a duty upon the data user to satisfy himself that a requested disclosure would conform with the requirements of the legislation are contradicted by the treatment afforded in the legislation to data relating to a data subject's:

> ".. physical or mental health or his sexual life.. "(35)

Such data is widely regarded as possessing a degree of intrinsic sensitivity. The Act, therefore, provides regulatory power enabling the data protection principles to be modified or supplemented in order to provide additional safeguards for the data subject. In respect of the non-disclosure principle the Act further provides that:

> "An order .. modifying the third data protection principle may, to such extent as the

> Secretary of State thinks appropriate, exclude or modify in relation to that principle any exemption from the non-disclosure provisions which is contained in part IV of this Act; and the exemptions from those provisions contained in that part shall accordingly have effect subject to any order made by virtue of this subsection."(36)

This provision was introduced into the legislation at the last possible stage. Its appearance may be considered due more to the lobbying power of the medical establishment than to any form of Pauline conversion persuading the Government of the value of affording special protection to sensitive data. Although the wording of the provision is general (and tortuous in the extreme) it was designed specifically to provide for the situation where access is sought to medical data.(37) Throughout the measure's parliamentary passage concern had been expressed by the medical profession at the possible impact upon the confidentiality of the physician patient relationship of the operation of the exemptions to the non-disclosure principle. Although accepting that the legislation did not compel disclosures, it was argued that the fact that these might take place would be sufficient to undermine a patient's faith that information passed to a medical practitioner would be treated in absolute confidence. The Government's

response to this concern was twofold. First, it was announced that a statutory code of conduct relating to the disclosure of personal health information would be issued under the authority of the National Health Service Act of 1977.(38) This code which would be binding upon health authorities and doctors and other employees of the national health service would specify the circumstances under which health data might be disclosed, other than with the consent of the patient, for purposes other than those concerned with his health care or treatment. In brief, the code requires that disclosures may be made only in specified situations. These include:

> "(a) Where the disclosure is required ... by or under a statute;
>
> (b) Where the disclosure is ordered by a court of law;
>
> (c) Where the disclosure is necessary for the proper investigation of a complaint."(39)

and that in any event the decision whether data should be disclosed should be made by a doctor. Second, the amendment quoted above was introduced to enable equivalent requirements to be imposed upon the private health sector.

Although the provision of additional safeguards must be welcomed from the individual's standpoint the provision

itself and the explanations as to its scope proferred in Parliament appear inconsistent with the views expressed by the Government concerning the general operation of the exemptions to the non-disclosure principle. The present exemption being intended to apply in respect of health data the question arises what items of data can be so regarded? This question will not pose problems within the national health service but may pose substantial difficulties where data is held by other organisations. The question then arises what information is to be regarded as health related and it would appear that the status of the person holding the data is irrelevant to this issue. In rejecting a proposal that data held for social work purposes should be accorded similar treatment to that afforded to health data on the basis that social work records frequently contain references to the subject's state of health, the Minister of State assured the House of Lords that the location of data was not relevant to considerations as to its status or categorisation, commenting that:

> "We must not be misled into thinking of health data as the data which doctors hold, and social work data as the data held by social workers as if the two were mutually exclusive ... The Bill operates not on the basis of files of data, but on individual items of data.

> Just because a file has my name on it, it does not mean that all the data contained on it are personal data to which I am entitled to have access. One has to look at the information contained in the file and identify that which is personal to me... Similarly, just because my name appears on the outside of a social work file, it does not mean that all the data in that file are exclusively social work data."(40)

Although we await the making of orders defining the scope of any restrictions upon the exemptions to the non-disclosure principles it is submitted that, at a stroke, the argument that the general exemption in favour of disclosures to the police or authorities cannot be restricted to the situation where disclosure is sought in connection with the prevention of or detection of the perpetrators of a serious arrestable offence has been destroyed. It will be recalled that the basis for the Government's decision in this respect was the argument that a more selective approach would place an unreasonable burden upon data users who might be uncertain whether a request satisfied this criteria. Users are now, however, expected to determine whether any portion of the data held by them falls to be regarded as health data in which case they will not be permitted to make disclosure unless they comply with the requirements of any order which may be made by the

Secretary of State. Such a task would appear no more straightforward than that of demanding assurance that the disclosure sought related to criminal conduct of sufficient gravity. Consistency would therefore appear to require that just as the disclosure of health data is considered to require special safeguards and procedures so these should be applied to, at least, those other forms of sensitive data identified in the Act and Convention. In this respect, the necessary powers are provided in the legislation; what is missing is any desire or intention to use them.

A further inequity may result from the application of the present exception to the non-disclosure principle. In the event that disclosure is sought by a police or taxation authority and where the user complies with this request; in the event that the Registrar subsequently determines that the disclosure was wrongful, the recipient authority will face no sanctions under the Data Protection Act. The user, on the other hand may face actions under the Data Protection Act both at the instance of the Registrar and of an affected data subject together with the possibility of a civil suit brought by the individual concerned under the law of breach of confidence. It may be considered, therefore, that a diligent user would wish to seek considerable assurances prior to making a disclosure that this will conform to the Act's requirements. If the user might have difficulty in

determining whether a request relates to a serious matter it may be expected that this task will not prove unduly burdensome for the police. Indeed in answering the question how police officers could be expected to decide whether he was entitled to exercise the powers conferred on him by the Police and Criminal Evidence Act the Minister of State commented that this would be possible

> "Because they are police officers exercising their powers."(41)

In view of the possibility that a user might face sanctions under the Data Protection Act if a disclosure were to be stigmatised as unauthorised it would not appear unreasonable that he should seek reassurance from the requesting agency as to the purpose for which the disclosure was sought and for the agency to be in a position to give such an assurance. In two further respects the provisions, or more accurately the lack of provisions, of the Data Protection Act regarding disclosures to the police or taxation authorities can be considered defective. First, the Act contains no requirements that a request for disclosure come from an officer of any degree of seniority or that it be considered at any particular level within the data user's hierarchy. Coupled with the fact that there is no requirement that a request for disclosure may be made in writing the result would appear to be that such

a request may be made verbally by any police officer acting of his own volition to the most junior member of the data user's staff who may, under the terms of the Act, legitimately make the disclosure. It may be, of course, that in the example given above that both parties would face sanctions from their respective employers but this may be of small consolation to the data subject concerned. Considerable disquiet undoubtedly exists concerning the ease with which access may be gained by police officers to sensitive information held, particularly on public sector computers such as those operated on behalf of the Department of Health and Social Security and it may be considered unfortunate that the Data Protection Act makes no attempt to provide a formal structure within which requests for access must be made.

A second cause for concern in this area concerns the absence of any requirement that records be maintained relating to the fact that disclosure of personal data has been sought and granted. Particular problems may arise in this situation because of the regionalised system of policing operated in the United Kingdom, each police force enjoying a considerable degree of autonomy. It may well be that one force's concept of circumstances which would justify disclosure would not be shared by another. It appears highly unsatisfactory that the Act should not provide that details of all such disclosures be recorded and made available for

inspection by the Registrar. Such a system would have to overcome the drawback that in making a request for information the police or taxation authority involved would not be acting as a data user and therefore will not be subject to the strictures of the Act. Even should the information thereby acquired subsequently be subjected to automated processing the Registrar will have no influence because of the Act's provision exempting the police from the requirement to comply with the first data protection principle. Control would, therefore have to operate at the level of the data user involved with the consequence that it might prove extremely difficult to obtain an accurate picture of the totality of requests made by a particular police or taxation authority. A proposal for recording of disclosures was made in parliament during the passage of the Act, it being suggested that:

> "... disclosures of personal data which are exempt from the non-disclosure provisions .. shall be recorded by the data user and such records shall be made available for inspection by the Registrar on request."(42)

This apparently innocuous suggestion did not find favour with the Government, the Minister of State arguing that this approach would:

> ".. bring little advantage to anybody, and

impose what are, therefore, unjustifiable burdens on users."(43)

It is difficult to identify any basis for the suggestion that the logging of disclosures would bring little benefit to anyone. The purpose of the non-disclosure principle can only be to assure the public that data obtained for one purpose will not be put to another without their having an opportunity to discover this fact. Accepting the need for some exemptions to be created in relation to this principle the need to protect the public interest remains. The only way in which this can be accomplished is for the Registrar to perform his role as ombudsman. If he is to do this he must be aware of the nature and scale of disclosures. It must be borne in mind that in the final analysis a decision may have to be made whether a disclosure is necessary in order to prevent the specified purposes laid down in the Act suffering prejudice. As the Act stands, no mechanism has been provided whereby the Registrar can obtain the information to perform this vital function. To a certain extent it may be argued that this situation arises on a more general basis when a data user makes a disclosure outwith the scope of his registration which does not purport to come within one of the exemptions discussed above. There is, however, an important distinction between these two scenarios. Under normal circumstances where a disclosure has taken place the data subject will have the right to obtain a

copy of any information referring to him held by the recipient of the data (assuming always that this data is held on computer). As will be discussed in the following chapter,(44) where data is held by the police or taxation authorities the individual's right of access is restricted and a major means by which an unauthorised disclosure might be identified will be lost. There appears, therefore, a need to provide an alternative safeguard for individuals against abuse of the exemption and a requirement of notification to the Registrar would appear to meet this goal. Against this, it may be argued that as sanctions may be imposed upon a data user in the event that the Registrar considers that a disclosure has been made without due cause, the imposition of a requirement of notification may have the effect of compelling a data user to incriminate himself. As has been stated,(45) however, the risk of prosecution would appear slight and it may be doubted whether intimation of the fact of a disclosure and even of the basic nature of the disclosure would furnish grounds for prosecution. A more substantial objection to imposing such an obligation upon users relates to the futility of such a practice. In the event that a wrongful disclosure occurs, liability rests upon the data user rather than on the person requesting the disclosure. Even if the information reaching the Registrar would appear to indicate that a particular police authority is making substantially and excessively greater use of the exemption than its

neighbouring forces there would appear nothing that the Registrar could do to put a stop to this practice.

In attempting to assess the adequacy of the general controls imposed upon data users in respect of their disclosures by the Data Protection Act it is important to draw comparison with the situation applying before the passage of the Act and, indeed, which still applies in relation to data stored in manual form. The point must also be emphasised that at this stage we are concerned only with the possible criminal consequences and administrative sanctions which may befall a data user. The previous position may be simply stated, information could be put to any use desired by its holder, including its disclosure to any person. Any criminal offences would be to some extent incidental to the transfer of data - thus if details as to a person's address were to be disclosed with a view to his being assassinated the person making the disclose would incur criminal liability. Short of such an extreme situation information could be disclosed at will. Immediately, the Data Protection Act limits this freedom by requiring prior disclosure of the situations under which information may be disclosed and of the range of persons who may receive the information. One of the major civil libertarian fears resulting from advances in computing technology is the possibility of linkage between computers being used to build up detailed profiles of an individual's movements, purchases and

actions. The non-disclosure principle should contribute significantly to preventing the secretive creation of such profiles.

The attainment of the objectives of the non-disclosure principle require that any exceptions be kept to a minimum and, where they are considered essential, alternative safeguards should be provided to preserve the data subject's position. In both these areas, it is submitted, the Act's approach is unsatisfactory. If the need for and value of the non-disclosure principle cannot be doubted, there must be cause for substantial concern on account of the exemptions permitting disclosure for the specified policing and tax gathering purposes. Most concern has centred on the exemption permitting disclosures for policing purposes. To some extent this may be considered surprising. The justification for the exemptions is that in performing the complicated balancing act between the individuals's claim for the restriction of the circulation of personal data, essentially that data should remain compartmentalised and, in some cases, for the maintenance of confidences and the wider interests of society that crime should where possible be prevented and, failing that, its perpetrators should be detected, apprehended and prosecuted, there will be occasions where the latter interests should prevail. The proposition that the State's revenue gathering activities should take precedence over individual

rights, in the absence of any suspicion that the individual concerned may have committed a criminal offence, is less axiomatic.

Even restricting consideration to the situation where personal data is disclosed by a data user to a police officer it is submitted that the provisions of the Act are excessively biased in favour of disclosure. The definition as to what constitutes a criminal offence is more broadly drawn in the United Kingdom than is the case with other European States. In particular, no distinction exists between the most minor misdemeanour, for example, overstaying one's welcome on a parking meter, and the most callous murder. It has been stated that almost every act is capable of breaking a criminal provision. By failing to place any restriction upon the severity of the crime which is being investigated by the police the Act must be seen as allowing potentially unlimited rights to seek access. The right is, of course, to seek access rather than to demand access. Nothing in the Act takes away a data user's existing right to refuse to cooperate with a request for assistance. By making, for the first time, a clear statement as to his entitlement to hand over data in violation of any obligation of confidence which may arise, the Act may be seen as placing a form of moral pressure upon the user to comply with a request for information. It might, however, prove salutory for users to consider that if they respond too readily to a

request which afterwards transpires to have no connection with the specified policing activities, they rather than the requesting authority will face criminal prosecution (and the possible service of an enforcement or de-registration notice) under the Act.

Perhaps the most substantial criticism of the new regime concerns the ease and informality with which requests for disclosure may be made and granted. Whilst it would be difficult for the legislation to impose any obligations or threaten any sanctions against those making the request but it might be reasonable to impose an obligation upon the data user concerned to ensure that, should he wish to benefit from the exemption, that the request be submitted in writing and be initiated by a senior police officer. It might additionally be provided that the decision whether to make the disclosure should be taken by by the user himself or by a nominated employee. Given the fact, however, that the essence of this situation is that it was not envisaged at registration that a particular type of disclosure might be made the establishment of a procedure to cope with unforseen eventualities might be difficult. A further safeguard for the individual might lie in a requirement that details of the disclosure be supplied to the Registrar by the data user concerned. The utility of such a course of action might be limited by the absence of any power on the part of the Registrar to impose sanctions against a police

authority which he considers is making excessive and unreasonable requests for access to data. A procedure of this nature might serve to promote public confidence and although he would have no direct power to prevent unreasonable requests the prospect of publicity, perhaps in the form of his annual report to Parliament, might exert a degree of influence.

The case for exemption is weaker in the situation where a data user wishes to volunteer information without having been directly requested so to do. Such a situation would appear to constitute a 'busy bodies charter' with users passing on to the police any item of gossip about an individual which may have found its way onto their computer. It is to be hoped, however, that the requirement in the legislation that it be shown not only that the disclosure be connected with policing purposes but also that a failure to disclose would be likely to prejudice those purposes may serve to limit the scope for such disclosures. Whilst it may be easy to establish that disclosure would be helpful to these purposes it may be more difficult to demonstrate that a failure to disclose will be prejudicial. Whilst, again, there may be an argument for restricting the scope of the exemption to the situation where a serious offence is involved it would appear that the requirements of the Act are better designed to safeguard the rights of the individual than

is the case where disclosure is sought by the police.

Ultimately, the question concerning this portion of the Act must concern the extent to which Sir Norman Lindop's strictures can be considered justified. In principle it may be argued that the allegation that the Act is fraudulent in pretending that disclosures of information can only take place in accordance with the provisions of an entry on the Register is inaccurate. The exemptions to the non-disclosure principle are contained in the text of the Act and this is, of course, available to anyone who wishes to read it. It is submitted, however, that fundamentally, Sir Norman's views have considerable merit. It is unreasonable to expect the average person to read the full text of the Act. The statute has been promoted as a measure to improve the lot of the individual. The application of the non-disclosure principle is, along with the requirement of registration and the provision of subject access, one of the corner stones of the legislation. Few would deny that it serves a major purpose in protecting the rights of the individual and yet in major areas the exceptions are such as to substantially restrict its value. It may certainly be said that in this area the Act delivers less than it promises.

3. Enforcement and De-Registration Notices

Under the Data Protection Act, the Registrar is charged with the duty:

> ".. so to perform his functions under this Act as to promote the observance of the data protection principles by data users and persons carrying on computer bureaux."(46)

Although in certain other jurisdictions the supervisory agency performs a purely advisory function (possessing only the sanction of publicity in the event that it considers a user to be in breach of the legislative provisions and the latter fails to modify his conduct), the Data Protection Act empowers the Registrar to apply a number of sanctions in the event that he considers a user to be in breach of the principles. One such power has already been discussed, that of refusing an application for registration or for the renewal of an existing registration on the basis of an anticipated violation of the data protection principles. Such a refusal would prohibit the user from commencing or continuing his processing activities. It has previously been argued, however, that the registration process appears ill fitted for the making of any judgments as to the acceptability of a user's actions. It may be more realistic to expect that the Registrar may take

action in the event that he receives complaints or discovers evidence pointing to a breach of the principles during the currency of a registration. In such an eventuality the Act provides two forms of sanction with the service upon the user involved of either an enforcement or a de-registration notice. In relation to an enforcement notice it is provided that:

> "If the Registrar is satisfied that a registered person has contravened or is contravening any of the data protection principles he may serve him with a notice .. requiring him to take within such time as is specified in the notice, such steps as are so specified for complying with the principle or principles in question."(47)

The introduction of the system of enforcement notices constitutes a relatively novel feature of the Data Protection Act and one which may serve to alleviate one of the major criticisms of previous licensing schemes in that their enforcement was limited by the lack of any intermediate sanction other than removal of a licence. As the effect of this might well be to terminate the business in question the sanction would frequently appear disproportionate to any offence which might have been committed. This in turn led to an understandable reluctance to impose it. In the consumer credit field, for example, the Director General of Fair

Trading has commented that:

> "If there is one serious weakness in the system, it is that the only ultimate sanction available to the licensing agency is revocation of a licence and, especially if consumer credit business is the sole or main activity of the trader, that sanction is equivalent to a death sentence... the sanction of revocation may in some instances seem too drastic, too draconian, to be a believable deterrent."(48)

It was further argued that where the malpractice is committed by a large company that the effect of withdrawing a licence could be to render considerable numbers of employees redundant, a situation which might be considered as socially undesirable as the original malpractice. One alternative which has been canvassed (and which has been applied abroad in the field of consumer credit) is to permit the licensing authority to impose fines in the event of malpractice by a licensee falling short of that which might justify termination of the licence.(49) Such an approach is subject to the objection that it creates a system of extra - judicial penalties. Enforcement notices, as provided for in the Data Protection Act, do not directly permit the Registrar to impose fines upon a user but constitute legally binding directions breach of which may constitute an offence punishable by fine.

An enforcement notice may be either positive or negative in its content, directing the user to take specified steps, for example to grant an individual's request for access to his personal data or to improve the level of security protecting data against the possibility of loss or unauthorised access. A negative form of enforcement notice will require that the user cease acting in a particular manner, for example, by disclosing personal data to persons other than those coming within a category specified at the time of registration. In both cases the notice must contain a statement of the principle or principles a breach of which is alleged together with a statement of the Registrar's reasons for reaching such a conclusion.

Upon receipt of an enforcement notice, a user is entitled to lodge an appeal with the Data Protection Tribunal. At the Tribunal hearing the onus is on the Registrar to satisfy the Tribunal that the disputed decision should be upheld.(50) Appeals to the Tribunal may be founded upon a question either of fact or of law.(51) The Tribunal may either uphold or reverse the Registrar's conclusions or in the event that it considers that:

> ".. the notice involved an exercise of discretion by the Registrar (and) that he ought to have exercised his discretion differently."(52)

may issue any other notice which it would have been competent for the Registrar to serve. In its proceedings, the Tribunal is not restricted to evidence submitted by the contesting parties, it being additionally provided that:

> ".. the Tribunal may, for the purpose of determining an appeal, make an order requiring the occupier of any premises ("the occupier") to permit the Tribunal, accompanied by the parties or their representatives and such number of the Tribunal's officers and servants as it considers necessary, to enter those premises at a specified time and, inspect, examine, operate or test any data equipment, or test any data material which is on those premises."(53)

Seven days notice must be given of such a proposed course of action.

A further appeal against the decision of the Tribunal lies, at the instance either of the Registrar or of the data user involved, to the courts. Such an appeal is only competent, however, where it concerns a point of law.(54)

The procedures and hearings resulting from the service of an enforcement notice can be considered analogous to

legal proceedings and it is to be expected that over the years the decisions of the Registrar and Tribunal in determining whether particular forms of conduct constitute a breach of the data protection principles will form a body of precedent providing steadily increasing guidance as to the scope and meaning of the principles. The Rules provide that:

> "The Tribunal may make arrangements for the publication of its decisions but in so doing shall have regard to the desirability of safeguarding the privacy of data subjects, and for that purpose may make any necessary amendments to the text of a decision to conceal the identity of a data subject."(55)

Publication of the Tribunal's decisions may provide a useful guide to all parties concerned with the operation of the Act as to its scope and extent. Because of the vast range of processing activities carried out by data users it must, however, be doubtful how far a decision addressed to one user can be considered to affect users operating outside that particular area.

In considering the role and potential effectiveness of the system of enforcement and de-registration notices the question must be asked how far they are likely to deter data users from acting in breach of the

principles? Upon this test, it is submitted, the system provides no real deterrent to an unscrupulous user. Generally, breach of the data protection principles does not, per se, expose the user to the risk of criminal proceedings. Given their nebulous nature such a stance may well be considered justified but the effect is that little deterrent is provided against deliberate or reckless violation. In certain cases a user may face civil action brought by an agrieved subject but the latter's rights of redress are circumscribed by the terms of the legislation and it must be doubted whether an individual could be considered to possess locus standi in order to enforce compliance with the principles. Attention must, therefore, be concentrated upon the role of the Registrar. Assuming that he discovers evidence suggesting a violation of the principles and serves an enforcement notice the Act provides that the user may normally continue his operations until the expiry of the appeal procedure. Even if the final decision goes against the user, an enforcement notice constitutes merely an instruction to him to modify his behaviour in specified ways. If the user complies with the notice at this stage he will incur no further liability. Given the scale of data processing, the limited resources available to the Registrar and the difficulties which he may encounter in obtaining sufficient evidence to justify service of an enforcement notice there would appear little incentive for a user to improve his

standards of behaviour. Such a consequence can only be avoided through the supply of more precise guidance directed at both users and the Registrar as to the interpretation of the principles. The legitimate interests of both must be best served when the likely legal consequences of any particular course of action can be calculated in advance.

In considering the possibility of an appeal being made to the Tribunal it should be noted that this action is available only to a data user who is aggrieved at being served with an enforcement notice. In the event that a data subject feels that a user is in breach of the principles but where the Registrar declines to serve a notice that individual has no right of appeal to the Tribunal in the event of the Registrar's refusal to act. It may be that an action may be brought in the courts seeking to compel the Registrar to consider a complaint, the Act providing that:

> "The Registrar may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected; and where the Registrar considers any such complaint he shall notify the complainant of the result of his

consideration and of any action which he proposes to take."(56)

It would appear, however, that the Registrar's only duty is to consider a complaint and that he retains near total discretion whether or not to take any action upon it. The absence of any right of appeal by individuals to the Tribunal has been justified on a number of grounds. First, it may be argued that the Act provides individuals with a variety of civil law rights in the event of malpractices by data users and that these may be pursued through the courts. Thus, for example, an individual who alleges that personal data is inaccurate may seek its rectification or erasure.(57) Against this, the rights given to individuals do not create locus standi in respect of breaches of all of the principles, there would not appear to be any action open to an individual alleging that excessive amounts of information were held concerning him. Again, it would appear that the individual rights granted under the Act can only, with the exception of the rectification of inaccurate information, be exercised after the individual has suffered financial loss, a requirement which, as will be discussed later,(58) severely restricts the prospects of a successful claim. The individual would thus appear relatively powerless until damage has been done.

A second line of argument suggests that a distinction should be drawn between the direct and serious consequences which may befall a user who is the recipient of an enforcement notice and the more nebulous impact which will be experienced by an individual whose request that the Registrar take this form of action against a user is ignored. Therefore it is argued:

> ".. it is necessary to provide an independent review body to which the data user may appeal."(59)

By contrast:

> "The data subject may not be granted the assistance he think he deserves if the Registrar declines to act; he may be left in precisely the same position he is now. But that is a different position from having positive action taken against him, which is the data user's potential fate."(60)

The argument that the Act does not place data subjects in a worse position than that which they enjoyed prior to its enactment is one which surfaces periodically throughout its parliamentary discussions. Such an argument seems rather inconsistent with the proclaimed view of the Act as a vehicle to improve individual

liberties. Whilst the individual may be able to pursue a complaint through the courts the effect of this restriction is to deny him access to what is intended to constitute a cheap and informal dispute resolution procedure.

Should an individual right of appeal be provided it would undoubtedly have the effect of increasing the number of appeals brought before the Tribunal. Such a situation could shift the balance of responsibility drawn up by the Act between the Registrar and the Tribunal. It has been argued that the provision of an individual right of appeal against the Registrar's failure to act would have the consequence that the Tribunal would come:

> ".. to dictate the way in which the Bill should be interpreted and the direction in which good data protection practices should evolve. That would change altogether the nature of the tribunal and would have obvious implications for the way in which it was appointed and the resources devoted to it, and it would have implications also for the way in which the registrar deployed his resources, making him less able to concentrate on those matters that appeared to him most serious and more concerned to ensure himself against an unfavourable finding from the tribunal that could confront

him."(61)

Whilst the consequence of the grant of an individual right of appeal might be to place the tribunal in the position of an appellate body vis a vis the actions of the Registrar it may be argued that it does already serve this function in respect of appeals by data users against the Registrar's actions. The criticism quoted above must surely apply, albeit perhaps to a lesser extent, to the current state of events. The debate as to the advisability of increasing the Registrar's exposure to the supervision of the tribunal does highlight a basic flaw in the Act resulting from the decision to reject the Lindop concept of a multi membered data protection authority in favour of a dual hierarchy of Registrar and Tribunal. Under the Lindop proposals the decisions of the authority would not be subject to any internal appeal, but would be susceptible of review in the courts. It is significant to note in this context that the Report recommended specifically that the right of appeal against decisions of the authority should extend to any individual who could demonstrate that he had been adversely affected by it.(62) By establishing a single registrar, the Data Protection Act renders almost inevitable the provision of some form of administrative appeal against his decisions. In the field of consumer credit, where decisions as to the grant, suspension or revocation of a licence are taken by the Director General of Fair

Trading, it is provided that where an application is rejected or a licence suspended or revoked an appeal may be made to the Secretary of State.(63) Such an approach would be incompatible with the decision taken in the Data Protection Act that the Registrar should be independent of government. If an appeal mechanism reaching to the government cannot be accepted the only option would appear to lie with the creation of a specific, non-governmental tribunal. The Data Protection Tribunal is the result. The consequences of this for the operation of the legislation are, it is submitted, unfortunate. The membership of the Tribunal is deliberately selected on account of their identification with the interests of either data users or of data subjects. Such a constitution appears to provide a recipe for a degree of polarisation. Whilst arguments can be advanced in favour of a multi membered data protection authority with members appointed from among the ranks of those likely to be affected by the legislation, the Data Protection Act adopts the alternative, but supportable, position with a single Registrar appointed to stand apart from sectoral interests and provide impartial and independent supervision over the operation of the legislation. As the decisions of the Tribunal must inevitably lay down policy guidelines which the Registrar will be obliged to follow the effect must be that the independent Registrar may be subordinated to the partial Tribunal. It may be considered inappropriate that the Registrar,

together with his considerable staff, who is appointed with the specific remit to ensure the compliance of data users with the principles should be subordinated to a body half of whose membership consists of representatives of those users. Whilst it may be considered equitable that some form of appeal should be provided against decisions of the Registrar, decisions which may have the most severe consequences for a data user's business activities it may be doubted whether this Tribunal is the most appropriate body to perform this task.

In the event that a user is served with an enforcement notice and complies with its requirements he will incur no further liability under the Act. Should he fail so to do, two further consequences may befall him. Firstly, it is provided that failure on the part of a user to exercise all due diligence in order to comply with the terms of an enforcement notice will constitute an offence.(64) Proceedings in respect of this may be brought either on a summary basis or on indictment. In the event of conviction the court may impose a fine and, additionally may order the erasure, forfeiture or destruction of any data which appears to the court to be connected with the commission of the offence.(65)

In addition to facing prosecution for failing to comply with the terms of an enforcement notice a recalcitrant

data user may also face further action from the Registrar in the form of a de-registration notice. This notice represents the ultimate sanction available to the Registrar. It may be served in the event that he considers that a user is in breach of the principles and that:

> ".. compliance with the principle or principles in question cannot be adequately secured by the service of an enforcement notice."(66)

It would appear that this would normally require that an enforcement notice should previously have been served and ignored although, in Parliament, the view was expressed by the Minister of State that a de - registration notice could be served where the user's attitude was such as to clearly indicate that he would not comply with an enforcement notice:

> "For example, the Registrar may come across a user who has refused subject access and whose attitude and behaviour make it quite clear that he will continue to refuse access, even if an enforcement notice were served on him."(67)

As the effect of a de-registration notice is to remove the user's entry from the register and, therefore, to render continuance of his processing activities illegal, it may be doubtful whether any user would be

so suicidally inclined as to make obvious his unwillingness to comply with a direction from the Registrar in the form of an enforcement notice and thereby risk immediate service of a de - registration notice. Even if the user should disagree with the Registrar's contention that he was in breach of the principles the possibility for an appeal to the Tribunal exists. Indeed it may be considered that a de-registration notice may only be served prior to an enforcement notice where the user has admitted his culpability but makes clear his refusal to contemplate mending his ways.

In the event that a de-registration notice is served appeals will lie to the Tribunal and the courts under the same conditions as described above in relation to the service of an enforcement notice.

The consequences of service of an enforcement or de registration notice can clearly be of the utmost significance for the recipient data user. It would appear to follow from this that the decision to serve such a notice is not one which should be taken lightly and that the Registrar should be possessed of satisfactory evidence prior to taking action. The obtaining of evidence of computer abuse threatens to constitute one of the major challenges to traditional concepts of law, so much so that it has been suggested that where allegations of computer fraud are made that

it may be necessary to reverse the fundamental principle of the common law that the onus of proving guilt rests with the prosecution. It would not appear that such drastic steps will be necessary in relation to data processing although the provisions of the Data Protection Act appear to place substantial restrictions upon the Registrar's freedom of action.(68) Initially, it may be noted that no duty is imposed upon data users to co-operate with the Registrar in any enquiries which he may wish to pursue. In itself this proposition may appear unobjectionable in that the criminal law has not hitherto obliged an accused person to incriminate himself (although the passage of the Criminal Justice (Scotland) Act of 1980 broke new ground in requiring individuals to cooperate with police enquiries(69)). Under the Data Protection Act, however, no such duty is imposed upon data users. Although in some circumstances the volume of evidence, perhaps in the form of complaints from data subjects, might be considered sufficient to justify service of an enforcement notice in other cases the inability to oblige users to cooperate may seriously inhibit the Registrar's performance of his functions. This position may be contrasted with that applying in several other jurisdictions. Under the Hessian Act of 1986, for example, it is provided that:

> "All data processing agencies and their contractors shall be obliged to support the

Hessian Data Protection Commissioner in the performance of his duties. In this respect, he shall, in particular -

> 1. be supplied with information in response to his enquiries and be allowed to inspect any documents relating to the processing of personal data;
>
> 2. be granted access to all official premises."(70)

To some extent the Hessian situation can be distinguished from that applying within the United Kingdom, the Data Protection Commissioner acting in an advisory as opposed to an executive capacity. In Sweden, however, the Data Inspection Board possesses such powers with the relevant legislation providing that:

> "For the purposes of its supervision the Data Inspection Board shall be granted admission to premises where ADP is carried out or where computers or equipment or recordings for ADP are kept. Moreover, the Data Inspection Board shall have access to documents relating to ADP and may make arrangements for operating the computers."(71)

In the case of Sweden it would appear that data users may, additionally, be subject to inspection as a matter of routine, it having been stated that:

> "The supervising division every week inspects two responsible keepers of registers or service centres. Recently both the Secret Service and the Defence Forces have been investigated. No activity in society is excluded from the legislation."(72)

Although the Registrar cannot compel cooperation, it is provided that application may be made to the courts for a search warrant empowering him to enter and search the user's premises and, most significantly, his computer. A search warrant may be issued if the registrar can satisfy the Sheriff that he has reasonable grounds for suggesting either that one of the criminal provisions of the Act is being breached or that any of the data protection principles are not being observed and that evidence of the conduct in question is likely to be found on specified premises.(73) Once again, however, the issue may arise whether the evidence available to the Registrar will found such a conclusion.

Under normal circumstances it is provided that a search warrant will only be issued after the Registrar has previously requested and been refused access to the

premises and that the user has been given seven days notice of the registrar's intention to apply for a search warrant. Under these circumstances, the user will have the right to be represented at the hearing in connection with the Registrar's application.

Such requirements would appear likely to place impossible burdens upon the Registrar and, in particular, it may be considered that the requirement that seven days notice of the intention to take further action would provide ample opportunity for a user to remove or to destroy any incriminating data. Fortunately, it is provided in the Act that the above mentioned requirements need not be complied with:

> "..if the judge is satisfied that the case is one of urgency or that compliance with those provisions would defeat the object of the entry."(74)

On the assumption that most applications for search warrants will seek to take advantage of the ex parte procedure it may be considered somewhat unsatisfactory that this procedure should be provided as an exception to the general rules.

Whilst there is a valid objection to the imposition of a duty to cooperate in circumstances where this may expose the user to the risk of criminal proceedings, it

must be noted that violation of the data protection principles is not, per se, an offence. The option made available to the Data Protection Tribunal to inspect a user's facilities may, at first glance, appear a valid precedent for the grant of a similar power to the Registrar but, given the quasi judicial nature of its proceedings, may be more closely analogous to the grant of a search warrant.

A basic tenet of data protection and a justification for the imposition of legislative controls lies in the belief that the consequences of informational abuse must be prevented rather than cured. Such a belief must call for an active as opposed to a reactive Registrar. The Swedish model, described above, demonstrates a better appreciation of this point than is to be found in the United Kingdom legislation. Even were the Registrar's powers to be extended in the situation where he possessed some evidence of abuse this would, it is submitted, still fall short of the ideal. This would require not only that the Registrar respond to complaints but that he should take positive steps to satisfy himself that the requirements of the legislation are being met.

4. Codes of Practice

Whilst service of an enforcement or de-registration notice will be binding upon its recipient and may,

assuming details are published, serve to give a measure of guidance to other data users, an element of chance must exist as to whether and when a particular aspect of processing will form the basis of such an order. Additionally, it is inherent in the nature of the process that a user can only be informed ex post facto that his conduct is unsatisfactory. The interests of all parties concerned in data processing would appear to suggest that more extensive guidance be given as to the interpretation of the principles, such guidance being tailored to the needs and circumstances of particular forms of processing. This guidance could be provided in a number of ways. One obvious candidate must be the Act itself. Whilst this approach would have the advantage of locating principles and rules in the same document it is subject to the objection that the detailed application of the principles is dependent to a considerable extent upon developments in technology. Given the rapid pace of this, detailed statutory provision might be considered a somewhat unwieldy and inflexible regulatory tool. Against this it may be argued that data users would be aware from the outset of legislative requirements and that the task of regular amendment of the legislation is one which may well have to be undertaken by Parliament. It may be noted that in Hesse, scene of the world's first data protection statute, the 1986 Act represents the third statute on this topic. Amendments to the initial statutes have either been introduced or are under

active consideration in several other jurisdictions. In common with other statutes operating in areas characterised by rapid technological change it would appear that data protection statutes may have a limited life span. More specifically it has been stated that the optimum life span of a statute in this area in in the region of 5-6 years. After this time, it is suggested, obsolescence sets in.(75)

In other areas of activity it has been considered that the task of providing for the detailed application of a statute or for the updating of its provisions is one which may be delegated to the executive. The Consumer Credit Act provides an excellent example of such a framework statute whilst a variety of statutes imposing criminal penalties provide for the regular updating of these penalties to take account of changes in earnings and inflation. Two objections can, however, be made against delegating power to interpret the principles to the executive. First, it may be argued that the principles are so vague and generalised that the distinction between detailed interpretation and fundamental change will be blurred. To this extent, delegation may well be considered to place an excessive measure of discretion in the hands of the executive. Second, on the basis that many of the most sensitive computer applications occur within the public sector, it may be considered inappropriate to provide for detailed rules concerning these activities to be

devised by the executive. Even accepting that secondary legislation will be subjected to Parliamentary scrutiny it is submitted that it would be inappropriate to provide for the detailed application and interpretation of the principles to be made a matter of governmental regulation.

Given that the parliamentary process may not be considered well fitted for the enactment of detailed provisions which may require frequent modification, but that this is not a task which may satisfactorily be left to secondary legislation, the attempt must be made to discover an alternative mechanism capable of providing both data users and data subjects with detailed and authoritative guidance as to the scope and extent of the principles in relation to their area of activity. In the United Kingdom, such consideration has centred on the role of the supervisory agency and the production of codes of practice.

The concept of a code of practice providing guidance as to the scope of legislative provisions is a well established one. Undoubtedly the best known example of the species is the Highway Code. The legal basis for this dates back to the Road Traffic Act of 1930 which provided that:

> "The Minister shall as soon as may be after the commencement of this Act prepare a code (in

this section referred to as the "highway code") comprising such directions as appear to him to be proper for the guidance of persons using roads..."(76)

The value of the Highway Code as a precedent for action in the field of data protection is restricted by the fact that responsibility for its production is vested in a government minister. An alternative approach was essayed under the provisions of the Employment Protection Act of 1975. This measure extended certain rights to employees including, inter alia, the right to a reasonable amount of time off in order to fulfil trade union duties. It further provided for a code of practice to be devised to give practical guidance both as to the amount of free time which might be considered reasonable and as to the activities which might be considered to justify such treatment. Creation of the code was to be the responsibility of the Advisory, Conciliation and Arbitration Service. In order for the code to enter into effect, parliamentary approval was required. As the Service is constituted as a body corporate, independent of direct government control, it was considered desirable to minimise any impression of governmental control over its actions. It was accordingly provided that the draft code should be transmitted to the relevant Minister who would:

"(a) if he approves of it, lay it before both

Houses of Parliament; and

(b) if he does not approve of it, publish details of his reasons for withholding approval."(77)

In this manner, the Minister retains a power of veto but is not entitled to modify the proposals.

Having received statutory approval, the question arises as to the legal status of a code of practice. The Employment Protection Act contains what has become the typical format in this respect:

"A failure on the part of any person to observe any provision of a code of practice shall not of itself render him liable to any proceedings; but in any proceedings .. any Code of practice .. shall be admissible in evidence, and if any provision of such a Code appears .. to be relevant to any question arising in the proceedings it shall be taken into account in determining that question."(78)

Given the above formulation it would be difficult for a party to argue that a failure to comply with the requirements of the code should not be equated with breach of a related statutory provision.

Similar codes of practice have been introduced under a number of statutes including the Race Relations Act 1976 and the Sex Discrimination Act 1975. In all these cases, however, it must be noted that whilst several codes of practice might be issued covering various aspects of a topic, each code would apply to all those operating within its area of application, for example, all motorists or all employers. In addition, in some cases, the codes could be seen as building upon a substantial corpus of statutory provision with the aim of providing practical guidance as to the scope of complex provisions. Neither of these factors is present in the field of data protection. The data protection principles are themselves vague and imprecise. More significantly, the principles are not susceptible of universal interpretation having to be applied in the context of particular forms of processing and a multitude of spheres of business, commercial, educational and other activities. Assuming that detailed interpretation of the principles through the medium of codes of practice should be considered desirable, a considerable number of such codes will be necessary in order to adequately regulate the entire spectrum of data processing.

In their report, the Lindop committee identified the need to provide definitive guidance to data users as to the ramifications of the data protection principles for their particular activities. Having determined that the

significant scale of public sector data processing argued against reliance upon the traditional forms of secondary legislation, the committee considered the extent to which law making powers should be vested in their proposed Data Protection Authority. It concluded that the Authority should be empowered to devise as many codes of practice as were considered necessary to regulate all relevant aspects of data processing. In view of the high priority afforded to the need to demonstrate the independence of the Authority from government it was considered that the latter should have no involvement in the procedures for creating and granting legal force to the codes. Even the limited degree of governmental intervention provided for under the Employment Protection Act 1975 was considered unacceptable, it being argued that this would be:

> ".. inappropriate, given that the purpose of the legislation will be to establish, and be seen to establish, a means of subjecting government and other users to control by an independent body.."(79)

Instead it was proposed that draft codes of practice should be transmitted directly from the Authority to Parliament. Such a system would have been constitutionally unprecedented, a fact which may demonstrate the importance attached by the committee to the need to have a patently independent supervisory

authority possessing significant regulatory powers. The novelty of the Lindop proposals did not rest solely in the manner of their creation. It was additionally proposed that a code should be legally binding upon affected data users. Breach of a code would not merely be considered as evidence suggesting a breach of some substantive legal provision but would become a offence or the basis for civil liability per se. This development was advocated on the basis that:

> ".. in matters of this kind, both users and data subjects should clearly know their rights and obligations (and) that those rights and obligations should have the force of law ... "(80)

It was envisaged that codes would be devised in order to be appropriate either for a particular category of user, for example, police authorities, or for particular data processing functions, for example, personnel records. In total it was estimated that some 50 separate codes of practice might be required.(81) One of the consequences of this approach would be to render redundant the possibility of the service of enforcement notices as the level of detail to be contained in the codes would be sufficient to render any user who failed to comply with the requirements liable to criminal prosecution.

In common with many of the aspects of the Lindop committee's report, their suggestions regarding codes of practice found little governmental favour. Whilst the novel nature of their proposals may in part have prompted their rejection objection was also taken to the perceived cost of this system. Although the committee recognised that there would be a need for the Authority to consult with affected data users (and with data subjects) as to the form of particular codes, ultimate responsibility for their compilation would rest with the Authority. As the Lindop proposals envisaging an extensive multi-membered authority were rejected in the Data Protection Bill in favour of a single Registrar and small staff (initially it was stated that a staff of 20 would be employed by the Registrar(82)), largely on economic grounds, it was argued that insufficient resources would be available for this exercise. In this respect it may be noted, however, that by May 1987 the Registrar employed 45 permanent staff (and a further 25 temporary staff(83)). The Lindop Committee, albeit reporting at an earlier stage of computer development, considered that the Data Protection Authority would require a permanent staff of 40.(84) Allowing for the vagaries of such estimates, the question may be posed whether the result of the legislation's introduction of a system of near universal registration has resulted in an obsessive regard for procedure with inadequate attention paid to the fundamentals of data protection. The point may also

be made that the committee did not envisage all the codes of practice being produced coincidentally. Instead it argued in favour of a system of phased registration with users being required to register only when a code had been devised for their particular area of activity.

Although the notion of legally enforceable codes of practice was rejected the government were willing to concede a role for voluntary codes of practice, it being stated that:

> "The Government sees some value in codes of practice in this field and expects that some professional bodies may wish to prepare such codes as a guide to their members."(85)

The role of codes of practice in the general field of consumer protection is a well established one, with the most significant developments in this field occurring under the aegis of the Fair Trading Act 1973. This Act created the office of Director General of Fair Trading and charges him with the duty to:

> " .. encourage relevant associations to prepare, and to disseminate to their members, codes of practice for guidance in safeguarding and promoting the interests of consumers in the United Kingdom."(86)

The apparently passive role of the Director is to some extent misleading. Under the terms of the Restrictive Trade Practices Act of 1976 any agreement made by a trade association as to the terms or conditions under which its members will do business will be regarded as a restrictive agreement which must be notified to the Director.(87) Upon receiving such notification the Director is, prima facie, obliged to refer it to the Restrictive Trade Practices Court. It is, however, further provided that in the event that the Director considers that the restrictions contained in an agreement are not significant be may seek the consent of the Secretary of State to a decision not to refer the agreement to the Court.(88) The Director can thus be seen as possessing a power akin to that of a veto over the proposals put to him, although, of course, the final say as to the acceptability of any code which the Director is unwilling to accept will lie with the Court.

The utility and value of voluntary codes in the field of consumer protection has been widely recognised. The Director has commented that:

> "codes of practice refresh those areas of business activity that the general law cannot reach."(89)

More generally, it has been argued that business self-

regulation offers a number of benefits over legislation:

> "Firstly, it is said that it conserves the public resources which would go into law making and law enforcement. By encouraging businesses to police themselves, the costs to society are minimized. Secondly, it is said that self-regulation can be quicker and more flexible than introducing and enforcing legislation .. Thirdly - and this is related to the previous point - voluntary standards are said to be well in advance of legal standards .. A fourth advantage is said to be that the standards evolved for self-regulation can be applied in a practical and common sense manner and not in the legalistic or rigid way of the courts. Finally, businesses are said to comply with voluntary standards in the spirit as well as the letter, whereas they might push the law to its limit and find loopholes. This more positive attitude to voluntary standards derives from businesses' interest in the proper implementation of something they have established and from their greater willingness to comply with peer group pressure than when confronted with force."(90)

Notwithstanding this acknowledgement of the utility of

such codes, the Data Protection Bill originally contained no mention of such instruments. This omission was explained on the basis that nowhere did the Bill prevent or prohibit users from devising a code of practice. Given this fact the insertion of any specific empowering provision would be an act of tautology. This approach, however, begs the important question whether users should be encouraged to formulate codes of practice. Ultimately, the point was accepted by the Government that the legislation should provide some positive encouragement for the compilation of codes of practice and a provision was inserted providing for:

> "It shall be the duty of the Registrar, where he considers it appropriate to do so, to encourage trade associations or other bodies representing data users to prepare and to disseminate to their members, codes of practice for guidance in complying with the data protection principles."(91)

This provision is closely analogous to that found in the Fair Trading Act. Whilst the apparent success of initiatives introduced under this legislation may appear to furnish a hopeful precedent for the introduction of codes of practice in the data protection field it may be doubted how far the underlying situations are comparable. Codes of practice devised under the Fair Trading Act invariably build

upon a sizeable corpus of law, whether statutory or common law in origin, specifying the rights and obligations of the parties who may be involved in particular transactions. In certain respects the codes may attempt to particularise general legal provisions so as to increase their relevance to a particular trade or profession. It may also be the case that a code will indicate acceptance of a higher degree of liability than that required under statute or common law provisions. To a considerable extent, however, the codes stand apart from the legal system, offering alternative remedies and alternative forms of dispute resolution. The role of codes of practice under the Data Protection Act would appear more contentious. As has been repeatedly stated, the data protection principles are composed of vague and generalised statements. In attempting to define these in the context of a particular application and given the absence of substantial statutory or common law guidance, a code must be seen as exercising a creative function. An example may be supplied from the first code of practice produced in the field of data protection, that sponsored by the Advertising Association relating to:

> ".. the use of Personal Data for Advertising and Direct Marketing Purposes."(92)

Referring to the first data protection principle

requiring that information be obtained fairly and lawfully, the code provides that:

> "If in the course of acquiring personal data from data subjects, data users materially misrepresent to these data subjects the purposes for which the data are to be held, used or disclosed, those data will be regarded as having been unfairly obtained."(93)

In interpreting this principle the Act provides that, in determining whether information had been obtained unfairly, account should be taken whether any person from whom it was obtained was:

> "deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed."(94)

Although the distinction between these two passages may be trivial the word "materially" as found in the code has no direct equivalent in the Act. A more blatant example of the abuse of the role of a code of practice can be seen in that devised by the Committee of Vice-Chancellors and Principals in respect of data processing within universities.(95) Dealing with the question of subject access to examination marks, the code advises universities that:

> "Examination marks processed on a computer, but not permanently stored thereon, may not necessarily have to be disclosed to students. If a university decides that it does wish to process examination marks on a computer and retain their confidentiality, it can only do so by use of the provisions in the Act which permit responses to data subject access requests to be delayed for up to 40 days from the date a valid request is received .. If, within 40 days of a request for access being received, all examination marks relating to an enquiring student had been deleted from the computer **as a matter of standard university routine**, it would be in order to delay responding until the end of that period of forty days, and to inform the student that no examination marks were held at the time of response."(96)

Such an approach prompted the response from the Registrar:

> "I note the comments made .. about examination marks. Whilst the procedure envisaged in this section is not wrong in law, it is likely to give rise to difficulties and I find it disappointing that it should appear in an otherwise positive document."(97)

The legal aspects of such a policy will be considered at a later stage. In this context, however, it may be commented that the provisions of the code appear to give the lie to the assertion that codes encourage a generous spirit of compliance with the spirit of legislative provisions rather than minimalist observance of the letter of the law.

Although the question whether any code attempts to interpret, apply or offer alternative rights and remedies to those provided at law may often be a narrow one it is submitted that the general nature of the data protection principles serves to render them an unsatisfactory basis for codes of practice drawn up on behalf of data users.

Criticism of the role allocated to codes of practice under the legislation takes account of the interests of both data users and subjects. Each have a legitimate and substantial interest in being able to assess the impact of the legislation upon particular data practices. Because of their voluntary nature, codes will not possess any legal force. In welcoming the initiative of the Advertising Association in producing their code, the Registrar was forced to issue the warning that:

> "Observance of this code does not constitute an assurance that I will accept in all cases and

> without qualification that data users have complied with the Act. However, in considering relevant complaints it is my intention to give careful regard to whether the data user concerned has been complying with his code of practice and will take such compliance as a positive factor in his favour."(98)

Under the Data Protection Act, beyond the existence of the duty to encourage the creation of codes, there is no provision for any direct input from the Registrar into the drafting process. It might be argued that the interests of data users and subjects would be best served were provision to be made for the Registrar to formally approve a code and to certify that compliance with its requirements would satisfy the requirements of the data protection principles. In both Houses of Parliament amendments to this effect were tabled to the Bill. This proposal was regarded with disfavour by the Government, it being pointed out that it was also the role of the Data Protection Tribunal to consider whether the data protection principles had been observed. To this end the views of the Registrar who may have certified that a particular code was in conformity with the principles would be irrelevant. Lord Elton, the Parliamentary Under Secretary of State at the Home Office, hypothesised a situation where a user had been served with an enforcement notice alleging and appealed to the Tribunal on the basis that

his conduct conformed with a code of practice. The user would:

> ".. remind the tribunal that the registrar has certified this as meaning that he was likely to have avoided a breach of the principles and will sink back in the expectation of commendation. But what a disappointment! - for the tribunal is not there to consider whether there has been a breach of the code. It is there to consider whether there has been a breach of the principle, and the code is an interesting irrelevance."(99)

Once again the split in functions and authority between the registrar and the tribunal appears to be a stumbling block to limit the utility of the Act. There would, however, appear to be no reason of principle why the Tribunal should not have been instructed to take the terms of a code of practice into account in considering any case before it.

4. Conclusion

Analysis of the current state of the data protection principles gives cause for a degree of pessimism concerning their likely impact. Whilst few could challenge their underlying motives the machinery for their application and elaboration appears to be

deficient. An illustration of the pitfalls which lie in wait for a statute which attempts to lay down general standards can be found in the Unfair Contract Terms Act 1977. Eleven years after this entered the statute book the critical question whether a particular exclusion clause satisfies the statutory requirement that it be fair and reasonable continues to defy precise resolution. With the data protection principles the urgent need is for these to be transformed from general statements of principle into specific and detailed guidance directed at particular data users and subjects. Unfortunately, it must be doubted whether the mechanisms provided in the statute are capable of performing this task.

Although service of an enforcement or a de-registration notice will have an obvious impact upon its recipient the enormous range of processing activities coming within the ambit of the legislation must diminish the precedental value of these notices. Whilst codes of practice provide a means whereby the general principles can be interpreted within particular context, the Act's provisions must be seen as minimising the attractiveness and value of these to all concerned. Whilst the Registrar may encourage their creation he can give no guarantee that compliance with the code will ensure immunity from service of an enforcement or de-registration notice. Equally, from the data subjects' standpoint, there can be no implication that

a user who fails to comply with the requirements of a relevant code will be regarded as being in breach of the principles. Whilst voluntary codes of practice may provide useful guidance on a de facto basis they must be considered a poor substitute for precise legal guidance. The point may also be made in connection with voluntary codes that, beyond the Registrar's function of providing encouragement, responsibility for their creation lies with data users. Inevitably, this must mean that their coverage will be patchy. Support for this assertion can be taken from the fact that in 1978 the Lindop committee identified a need for some 50 codes of practice. Given the subsequent expansion of computer applications today's comparable figure may well be considerably higher. By May 1988, almost four years after the Act received the Royal Assent and two years after the date by which existing users were required to apply for registration, fewer than 10 codes were either in force or in the course of preparation.(100) Although the Lindop notion of codes being in situ prior to registration may have been expensive in terms of public resources it is submitted that this approach would have served to ease the burdens of the legislation upon data users and would also have served to promote an increased awareness among data subjects as to the extent of their rights under the legislation. If data protection legislation is to have a significant impact upon the behaviour and attitudes of both data users and data subjects it would

appear that changes must be brought about at the time of the measure's introduction. Procrastination can only serve to give the impression that data protection is a matter of trifling concern and it may be more difficult to enforce the Act's strictures at a later stage once the momentum for change has been lost.

Footnotes

1. Supra pp.62-4.

2. Supra pp69-71.

3. Supra Chap.2.

4. Sch.1. Only the eighth principle is applicable to the operator of a computer bureau.

5. S.2(3).

6. See Simitis Sensitive Data - The Quest for a Legal Regime op cit in which he identifies the categories of sensitive data with the privacy interests which have been protected in certain jurisdictions.

7. Art.6.

8. Art.1.

9. Art.2.

10. S.6.

11. S.34(5).

12. See, however, Personnel Council at the Municipal Regional Computer Centre Kassel v Director of the Municipal Regional Computer Centre Kassel [1980] ECC 199 in which it was held that the provisions of the Hessian Data Protection Act should prevail over those of the Hessian Personnel Representation Act.

13. S.34(6).

14. Supra para 21.10.

15. Sch.1.

16. S.28(4).

17. S.7((5)(b).

18. Official Report (Standing Committee H) 10 April 1984 Col 762.

19. Ibid col 764.

20. Art.5(b).

21. Art.9(2).

22. Supra pp.211-16.

23. Letter to the 'Times' 26 March 1984.

24. S.28(3).

25. S.28(1).

26. 40 Official Report (House of Commons) 11 April 1983 Cols 626-7.

27. Official Report (Standing Committee H) 5 April 1984 Col 710.

28. Justice. Breaking the Rules, 1980.

29. Official Report (Standing Committee H) 5 April 1984 Cols 620-1.

30. S.34(8).

31. S.116(6).

32. Official Report (Standing Committee H) 5 April 1984 Col 627.

33. Ibid Col 650.

34. S.5(5).

35. S.2(3)(c).

36. S.2(5).

37. The amendment was introduced at the Report stage in the House of Commons.

38. 61 Official Report (House of Commons) 5 June 1984 Cols 217-8.

39. Internal DHSS Memorandum.

40. 53 Official Report (House of Lords) 29 June 1984 Cols 1165-6.

41. Official Report (Standing Committee H) 5 April 1984 Col 651.

42. Official Report (Standing Committee H) 10 April 1984 Col 735.

43. Ibid Col 738.

44. Infra p.387 et seq.

45. Supra pp.184-5.

46. S.36(1).

47. S.10(1).

48. Borrie. The Development of Consumer Law and Policy. Op cit. pp.89-90.

49. Cranston. Consumer Law. Weidenfeld and Nicolson (2nd Ed.) 1984 p.367.

50. Data Protection Tribunal Rules, Rule 19.

51. S.14.

52. S.14(1)(c).

53. Data Protection Tribunal Rules, Rule 9.

54. S.14(5).

55. S.30.

56. S.36(4).

57. S.24.

58. Infra pp.442-3.

59. Official Report (Standing Committee H) 15 April 1984 Col 391.

60. Ibid Col 392.

61. Ibid.

62. Supra para 20.59.

63. S.41.

64. S.10(8).

65. S.19(2) and (4).

66. S.11(3).

67. Official Report (Standing Committee H) 13 April 1984 Col 389.

68. 'Guardian' 1 May 1986.

69. S.1.

70. S.29.

71. S.16.

72. Freese. Six Years of Swedish Data Legislation - An Analysis of its Impact and Future Trends; in Information, Computer and Communications Policies for the 80's.

Gassman (Ed). North Holland, 1981.

73. Sch.4.

74. Para 1(2)(b).

75. Simitis in verbal presentation at Council of Europe Conference. Op cit.

76. S.45.

77. S.6.

78. S.6(11).

79. Supra para 20.74.

80. Ibid para 19.87.

81. Ibid para 20.50.

82. Explanatory and Financial Memorandum.

83. Third Report of the Data Protection Registrar p.49.

84. Supra para 22.23.

85. Cmnd 8539 para 8.

86. S.124(3).

87. S.1.

88. S.21(2).

89. Borrie. The Development of Consumer law and Policy. Op cit p.74.

90. Cranston. Op cit p59.

91. S.36(4).

92. Entering into force in March 1987.

93. Para 3.1.3.

94. Sch.1.

95. Entering into force April 1987.

96. Para 14.2.

97. Foreword.

98. Foreword.

99. 443 Official Report (House of Lords) 19

July 1983 Col 1122.

100. Third Report of the Data Protection Registrar, p.9. Encyclopedia of Data Protection Law. Sweet and Maxwell, 1987, part 5.

Chapter Five

Individual Rights and Remedies

Individual Rights and Remedies

1. The Role of the Individual

To date, in considering the application of the data protection principles it has been apparent that responsibility for defining and applying these rests primarily with the Registrar. Whilst, despite the United States' quibbles, there can be little doubt but that a public supervisory agency can play a useful role in protecting the general interests of data subjects, there must be doubt how far any public agency can be held responsible for the preservation of the rights of a particular individual. In addition, therefore, to establishing such an agency, and regardless whether data protection is regarded as a device to promote individual's rights of privacy or as an attempt to minimise inequalities of power resulting from the information society, a central consideration of legislation must revolve around the need to involve the individual in, and extend a measure of control over, informational practices which may directly affect his welfare. One aspect of this requires that any actions which may affect the individual should be based upon accurate information. To this end the fifth data protection principle requires that:

"Personal data shall be accurate.."

In many cases it will be the data subject who is in the best position to be cognisant of the accuracy or inaccuracy of any data. In order to ensure accuracy, therefore, it is necessary for the subject to be aware what information is held. Whilst the establishment of the Data Protection Register serves to advance the cause of data transparency there is also a need for the subject to have access to the detail as well as to the generalities of any records. To this end, the notion of subject access has come to be regarded as a key component in data protection legislation.

2. Subject Access

A starting point for investigation of the practice of subject access can be found in the provisions of the Convention. This requires that national laws ensure that:

"Any person shall be enabled:

> to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in

an intelligible form."(1)

This provision is mirrored by the Data Protection Act which provides that:

> "An individual shall be entitled-
>
> (a) at reasonable intervals and without undue delay or expense
>
> (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
> (ii) to access to any such data held by a data user."(2)

Beyond the assertion that subject access is necessary to promote public confidence in data processing it is not easy to identify the legal basis for such a right. Where information is held within the public sector it may be argued that this is held by the public authorities on behalf of the individual and, therefore that he has a right of access to such data. Such a situation has historically prevailed in a number of states - notably Sweden.(3) In this context the claim to subject access under data protection legislation becomes intermingled with the demand for freedom of information. Although these two concepts may sometimes

conflict with data protection legislation attempting to minimise the range of disclosure of personal data whilst freedom of information statutes maximise its dissemination. On a privacy based analysis, one man's claim to data protection may be incompatible with another's demand for access to information. Approached from an alternative standpoint, however, that of the allocation of informational power, the two concepts appear complementary. In 1982, a recommendation of the Committee of Ministers of the Council of Europe, whilst recognising that genuine considerations of privacy might compel restraints upon the extent of access to information stated that the:

> ".. pursuit of an open information policy in the public sector, including access to information, is among the objectives of member states."(4)

The all embracing nature of the Official Secrets Acts coupled with the recent invocation of the civil law of breach of confidence by the Government in the case of Attorney General v. Guardian Newspapers,(5) might suggest that open access to official information does not currently constitute a prime Governmental objective.

The justification for permitting individual access to personal data held within the private sector is equally

elusive. One argument which may be put forward is to the effect that personal data belongs to the individual concerned and, therefore that he should have the right to control its use and dissemination. Thus, for example, an individual faced with a request for information concerning some detail of his personal life may well respond in the negative with the statement; "Its none of your business." Whilst such a scenario may well accord with practical realities the legal point at issue is whether a negative action in refusing to volunteer information to a particular enquirer can be elevated to the status of a right of property or ownership in that information capable of being invoked against the world at large.

Although the Data Protection Act is silent on this matter the question of the legal status attaching to information is one of the key issues in the field of computerised information. Discussion and legal debate in this area has tended to centre in the realm of criminal law. In most Western legal systems the criminal law is based on the twin concept of offences against persons and property. The question has arisen in several contexts and several jurisdictions whether information, divorced from any connection with a physical object may be regarded as property.(6)

The question of the legal status of information assumes most significance in the situation where it is alleged

that this commodity has been stolen. In both Scotland and England the law of theft is based on the notion of an infringement with the owner's rights in property.(7) In order to sustain such a charge information would have to be regarded as property. Such a conclusion is subject to two objections, one conceptual and the other practical. First, unlike the situation where physical property is removed, it is difficult to identify precisely what the "owner" of information has lost. In the situation where unauthorised access is obtained to information and the perpetrator carries the information away, whether in his memory or in the form of a printed copy, the "owner" will retain the information. At the strongest it may be argued that the quality of his possession has been diminished; that whereas he may previously have had exclusive knowledge of the contents of the data, that knowledge is now shared with at least one other person. As it appears established, however, that the unauthorised use of a person's property, for example, an employee's use of an office typewriter to type a personal letter, does not, per se, constitute a criminal offence,(8) this may not constitute a significant factor.

A more fundamental objection to the application of the law of theft in this area relates to the legal status of information. Under the law of theft, both in Scotland and in England, only property can be the subject of this crime and it would not appear that

information can properly be so regarded. The traditional view relating to the status of information was expressed by Lord Upjohn in the case of Phipps v. Boardman(9) to the effect that:

> "In general, information is not property at all. It is open to all who have eyes to read and ears to hear."(10)

The notion that information could form the subject matter of theft received short shrift in the case of Oxford v. Moss.(11) This centred on an abortive scheme by a university student to cheat in his examinations. Discovering a proof copy of an examination paper which he was shortly due to sit, the student removed this intending to copy the questions and return the paper. His plot was discovered and criminal proceedings were instituted. Under the then provisions of the Theft Act a charge of theft could not be brought in respect of the paper itself in the absence of any intention on the part of the defendant to permanently deprive the owner of it - indeed his scheme depended on the fact that the paper's temporary absence was not discovered. As an alternative, the defendant was charged with the theft of the confidential information contained in the paper. This charge was dismissed by the Magistrate who ruled that:

> ".. confidential information was not a form of

> intangible property as opposed to the property in the proof examination paper and the words printed thereon."(12)

This conclusion was unanimously upheld by the Divisional Court. A similar view was taken by Megarry V-C in the case of Malone v. Commissioner of Police for the Metropolis (No.2).(13) Here the plaintiff, whose telephone had been tapped by the Metropolitan Police in the course of a criminal investigation, asked the court to declare such activities unlawful. Inter alia, he alleged that his rights of property in the words spoken over the telephone had been infringed. Rejecting this argument the Vice-Chancellor stated that:

> "Counsel's first proposition for the plaintiff rested in the first place on a right of property. To tap a person's telephone conversation without his consent, he said, was unlawful because the person had rights of property in his words as transmitted by the electrical impulses of the telephone system, and so the tapping constituted an interference with his property rights. An analogy that he suggested was that the important part of a letter was the words that it contained rather than the paper that it was written on .. I do not see how words being transmitted by electrical impulses could themselves (as

> distinct from any copyright in them) fairly be said to be the subject matter of property."(14)

In Scotland a similar decision as to the legal status of information has recently been reached in the case of Grant v. Allan.(15) Here, it was alleged that an employee had taken copies of computer printouts containing details of his employer's customers and had offered to sell these to rival companies. Dismissing the charge the High Court held, first, that the conduct complained of, viz the dishonest exploitation of the confidential information of another person, did not refer to any offence recognised under the law of Scotland and, second, that this was not a situation in which the use of the Court's declaratory power would be justified. The Lord Justice Clerk (Ross) stated that:

> "I recognise that there may be reasons for thinking that conduct of this kind ought to be regarded as criminal. However, if that is so, I am of opinion that it is for Parliament and not the courts, to create any new crime in that regard....'Where Parliament fears to tread, it is not for the courts to rush in'."(16)

A contrary view both as to the status to be afforded to information and as to the role of the judiciary in applying the provisions of the law to new forms of conduct accompanying new forms of technology can be

seen in the Canadian case of R v. Stewart.(17) Here, faced with a factual situation similar to that applying in Grant the majority of the Ontario Court of Appeals held a charge of "counselling the theft of information" competent. Under the Canadian Criminal Code, the offence of theft may be committed when a person:

> "... fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or the use of another person, anything whether animate or inanimate."(18)

Although this definition might appear wider than those applying in the United Kingdom the provision appears in that part of the Code entitled, "Offences against property" and it was accepted by all the judges involved in the case that is should be interpreted restrictively so as to encompass only those things capable of being considered property. Accepting this limitation, and also that information should not generally be considered a form of property, the majority held that confidential information should be so regarded. This conclusion was justified by reference to the importance of information to the business community. Thus, Houlden J.A. explained that:

> "Compilations of information are often of such importance to the business community that they

> are securely kept to ensure their confidentiality. The collated, confidential information may be found in many forms covering a wide variety of topics .. The importance of confidential information will increase with the growth of high technology industry. Its protection will be of paramount concern to members of industry and the public as a whole."(19)

In similar vein, Cory LJ pointed out that:

> "While clearly not all information is property, I see no reason why confidential information which has been gathered through the expenditure of time, effort and money by a commercial enterprise for the purpose of its business should not be regarded as property and hence entitled to the protection of the criminal law."(20)

Whilst the value of information today cannot be denied the approach adopted in the Canadian courts is open to criticism. Although the whole may on occasion be greater than the sum of its parts the argument that property rights may exist in a lot of information but not in a little is an unattractive one. To take the example of a mailing list, it appears illogical to argue that an individual name and address cannot be

owned by its holder but that a collection of names and addresses can be owned by a third party. The decision in R v. Stewart would also appear to offer little assistance in attempting to provide a justification for granting a right of access to personal data held within the private sector. In most cases factual information relating to an individual will be intermingled with assessments and statements of opinion made and held by the data user. It is impossible to identify any basis upon which ownership of these might be ascribed to the individual concerned. Further, it may be argued that much personal data is within the public domain, eg names and addresses on the electoral roll and, finally, that the raw information upon which a record is based may frequently be volunteered by the individual concerned in return for obtaining, or being considered for, some service or facility. Even were the Scottish courts, therefore, to accept that information could, in certain circumstances, be considered as property it may be doubted whether this would provide much assistance for a data subject.

If the justification for subject access cannot be found in property rights a relevant precedent may be found in the statutory restrictions upon the doctrine of freedom of contract found in such statutes as the Unfair Contract Terms Act of 1977. In restricting the theoretical freedom of parties to negotiate the terms and conditions of their contracts, the statute

recognised that a distinction exists between the legal concept of equality between contracting parties and practical realities. Similarly, the relationship between data user and data subject can be considered an unequal one with the concept of subject access being seen as a corrective or equalising device. It must be recognised, however, that the approach of the Data Protection Act is more intrusive than that of the Unfair Contract Terms Act. Whilst the latter restricts the ability of a contracting party to act in certain ways, the Data Protection Act requires that the user act in a particular way; that he grant subject access.

To a considerable extent, therefore, there appears little basis within the British legal tradition for the grant of subject access either within the public or the private sector. In both areas, it is submitted, the prime justification for this lies with the development of the information society. Although, as distinct from other commodities, information is an infinite resource the interests of society require that positive steps be taken to allocate informational power and to control those who seek to wield such power.

The practical application of this principle is extensively defined within the text of the Act. Consideration of this aspect of data protection raises three main issues. First, the extent of the right of access and, in particular, the restrictions which may

apply in this area, second, the procedures by and the circumstances under which an individual may challenge the inclusion of particular items of data and, finally, the remedies which may be available to the individual if he suffers loss because of errors in the record.

Although it is the development of the computer which has served to transform the impact of informational practices, the first statute providing for the grant of subject access was the Consumer Credit Act of 1974. Recognising that the decision whether to extend credit facilities to a particular applicant would often be based upon information relating to that person's credit record and financial standing held by a credit reference agency and aware of the consequences for the individual should that information be inaccurate the Act requires the operator of such an agency to supply, upon request, a copy of any information held relating to an individual or a non-corporate body.(21) Although applying only to a specialised area of data processing, the provisions of the Consumer Credit Act can be seen as a precedent to those of the Data Protection Act. Prior, therefore, to considering the detailed operation of subject access under the Data Protection Act, an examination will be made of the nature and extent of these earlier provisions.

The right of access under the Consumer Credit Act arises because of the status of the record holder as

operating a credit reference agency. The Act defines a credit reference agency as a:

> ".. person carrying on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose."(22)

The question whether information is maintained on computer is of no significance for the purposes of the 1974 legislation.

In relation to subject access the Consumer Credit Act provides that any non-corporate body should be entitled to request a copy of any relevant file held by a credit reference agency. The word "file" is defined as:

> "..all the information about him kept by a credit reference agency, regardless of how the information is stored, and "copy of the file", as respects information not in plain English means a transcript reduced into plain English."(23)

To date, 5419 credit reference agencies have been licensed under the Act.(24) As with the Data Protection Register the register of those licensed to conduct

credit businesses is a public document. The Act establishes an entitlement on the part of an individual to make a written request to any licensed agency as to whether they hold information and, in the event of an affirmative answer, to be supplied with a copy.(25) Although the number of licensed agencies is much smaller than that of registered data users the legislation recognises that the task of attempting to identify those agencies which may hold information about a particular individual is likely to prove a time consuming, inefficient and, as a fee will have to accompany every application, expensive process. One solution to this problem would be to but the onus upon credit reference agencies to notify individuals that they hold information concerning them. This approach has been adopted in the Federal Republic of Germany(26) but is one which did not commend itself to the United Kingdom's legislature. The Act does, however, recognise that the situation which will cause individuals most concern as to the contents of their credit files is when they make application for and are refused or have difficulty in obtaining, credit facilities. It is accordingly provided that when an individual has made application for credit he should be entitled to request details as to any credit reference agency which has been consulted in determining his application. In order to be effective such a request has to be made within specified time limits, it being provided that the name and address of the credit reference agency must be

supplied if a request is received within 28 days from the termination of any antecedent negotiations between the consumer and the creditor or any broker or negotiator acting on his behalf.(27)

The phrase "antecedent negotiations" is broadly defined in the legislation as including any communications between the parties and any representations which may be made to the individual with a view to the making of a credit agreement.(28) In most cases, these negotiations will terminate when the individual makes formal application for credit facilities. This approach leaves open the possibility for a creditor who, as a result of consulting a credit reference agency, determines not to accept an application for credit facilities, but who does not wish to encourage the individual to pursue the matter with the credit reference agency, to delay notifying the individual of his decision until the 28 day period has expired. At this point the creditor would be able to refuse to comply with a request that he supply details of the credit reference agency consulted.

It might be argued that the period within which an individual should be able to request details should expire only after the creditor's decision has been communicated to him. An alternative approach has been adopted within the United States where the Fair Credit Reporting Act requires that where an adverse report

from a credit reference agency constitutes the reason for refusal of a credit application the creditor is obliged to inform the applicant of the identity of the agency involved.(29) To this extent the American provision might be considered more favourable for the individual than the United Kingdom equivalent although is is significant that having been informed of the reason for rejection the applicant is entitled only to be informed by the agency of the tenor of the information held by them.(30) There exists no right to a copy of all of the information held.

Assuming that an individual discovers the identity of a credit reference agency, either by utilising the procedure described above or otherwise, and submits a written request seeking access, a copy of any file must be supplied within 7 working days.(31) A fee of £1 may be charged by the agency for this service.(32) In addition to enclosing a copy of the file the agency must supply a statement of the rights afforded to the individual under the Consumer Credit Act in the event that he objects to any of the contents of his file. The terms of this statement are prescribed by regulation.(33)

The Consumer Credit Act regulates agreements not only where the debtor is an individual but also business transactions where the debtor is a non-corporate body, for example, a sole trader or a partnership. The rights

described above will normally apply regardless of the status of the debtor but a credit reference agency faced with a request for access by a business applicant may, if it considers that to supply the applicant with a copy of the information held would:

> " .. adversely affect the service provided to its customers by the agency.."(34)

may make request to the Director General of Fair Trading to follow an alternative course of procedure. If the Director General is satisfied that:

> " ..having regard to the methods employed by the agency and to any other relevant factors, it is probable that consumers carrying on a business would not be prejudiced by the making of this direction."(35)

he may direct that the agency supply to the subject such information as he thinks fit.(36) Comparatively few requests have been made seeking to take advantage of this provision. In the event that partial details are supplied to the applicant he must be informed of this fact. If he is is dissatisfied either as to the accuracy or the extent of the information supplied he may appeal to the Director. At this stage the Director may require that the agency supply him with a copy of the file and has discretion to release more information

to the subject or to order the deletion or amendment of any information contained in the record.(37)

This provision recognises that much information may be supplied to credit reference agencies in confidence. Disclosure of the information might inevitably result in identification of the source with the consequence that informants may be wary of so acting in the future. Once again a balance has to be struck between competing interests. It is significant to note that in respect of private individuals their interests unequivocally prevail. Where business applicants are involved the balancing act is more complex but, in contrast to the position which frequently applies under the Data Protection Act, the solution adopted does not involve total exemption but, rather, places the Director in a pivotal position.

In considering the precedental value of the provisions of the Consumer Credit Act the limited sphere of operation of this measure must be constantly born in mind. It may also be relevant to note that the nature of their operations requires that credit reference agency files should be arranged in such a way as to facilitate the withdrawl of information by reference to a particular individual. To this extent, responding to a request for subject access should pose few operational or logistical problems. This may not always be the case with the more general files coming within

the ambit of the Data Protection Act. In addition, the underlying intention of the earlier legislation was limited and in assessing the value to the individual of the controls contained in the 1974 legislation it must be noted that although it adopts the notion of subject access it contains no requirements, other than that of accuracy, relating to the quality or relevance of data. Further, it does not seek to control the means by which data is acquired or the uses to which it is put. The Consumer Credit Act contains no equivalent to the data protection principles. Within the field of subject access, however, the 10 years experience obtained under the Consumer Credit Act may offer some prognosis for the effectiveness of the rights contained in the Data Protection Act.

Moving from consideration of the requirements of the Consumer Credit Act to the detailed requirements contained within the Data Protection Act the basic provisions of the latter statute can be briefly stated. Building upon the requirements of the seventh data protection principle it is provided that:

> "... an individual shall be entitled-
>
> (a) to be informed by any data user whether the data held by him include personal data of which that individual is the data subject; and

(b) to be supplied by any data user with a copy of the information constituting any such personal data held by him.."(38)

In the event that any portion of the data is expressed in terms which may not be intelligible to the data subject, for example, should value judgments be expressed in terms of a numerical scale, the enquiring user is to be supplied with an explanation of the information in question.(39)

The operation of the subject access provisions may pose certain problems for data users. Although they are required to comply with requests from a data subject, the right of access normally extends only to the particular subject. If information is disclosed to any other person the user may be found to have violated the third data protection principle and may face actions both from the Registrar and the data subject. It must, therefore, be reasonable for a data user to take steps to ensure that a request for access actually emanates from the subject in question. Although the Act does not directly require than a data subject make written request for subject access it does provide that a data user will only be obliged to comply with a request when this is received in writing. It is further provided that a user may require, prior to meeting a request for access, that he be:

> "... supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which he seeks.."(40)

The initial requirement of this section raises no substantial issues. In view of the sanctions which may await a user who makes an unauthorised disclosure of personal data it is only reasonable that he should be entitled to require evidence as to the identity of the enquirer.(41) The second element, however, raises more substantial issues. Depending upon the structure of the user's data base personal information may be stored by reference to criteria other than name, and a trawl for information relating to an individual may be considerably assisted if the user is informed of any alternative identifiers. It is uncertain, however, to what extent the Act will permit him to require such additional indicators as a prerequisite to granting subject access. It is submitted that this provision should be restrictively interpreted so as to apply only in respect of information which the data subject may reasonably be expected to possess. Such a view would appear in conformity with the normal meaning of the word 'require' as something which is necessary to attain a purpose. Initially the Registrar appeared to take a wider view of the interpretation of this requirement, advising users that:

> "As far as locating information is concerned, you may ask the Data Subject for example, for his national insurance number if that is the "key" you need to find his record. Or you might, for example, ask if he has been an employee or customer of yours, if that information will assist you in locating his personal data."(42)

Subsequently, this view was modified with users being informed that:

> "The fact that further information would assist the Data User in locating the personal data does not necessarily mean that he is entitled to refuse to comply with a subject access request until he receives the information."(43)

In giving examples of the situations in which it would be reasonable for the user to require further information the Registrar appears, however, to retain the notion of additional information facilitating rather than permitting response to a request. Thus, it is stated that if a data user:

> "... reasonably believes that part of his collection of personal data relates only to his current and past customers (it) would be reasonable to ask the individual to say whether

> or not he has ever been a customer. If he says that he has not, then the Data User need not search that part of the collection."(44)

It is submitted that in the above example, the user's request is intended to facilitate or simplify his search and cannot be regarded as essential to its success. The point may seldom be of more than academic interest but it may be considered that the complicating of the subject access procedures, for whatever motives, might have the effect of inhibiting data subjects from pursuing a request for access.

Although the right to request access is normally restricted to the particular data subject, the law has always recognised that children and those suffering from mental disorder may not be capable of fully exercising their rights and, therefore, that action may be taken on their behalf by a third party. The question to be discussed in this context is the extent to which, when personal data relating to a child or to a person suffering mental disorder is processed, the rights of subject access may be exercised by those legally charged with the welfare of the subject.

Provision is made in the Act for the situation where the subject suffers mental disorder, it being provided that:

"The Secretary of State may by order provide for enabling a request .. (for subject access).. to be made on behalf of any individual who is incapable by reason of mental disorder of managing his own affairs."(45)

To date, no regulations have been made prescribing the procedures to be followed in the above situation. As definite legal procedures exist, however, leading to such a declaration of incapacity comparatively few problems may be anticipated. The position is less clear cut where children are involved. The Act making no specific mention of the extent of access rights in this situation, the provisions of the general law must remain operative in this area. This may create difficulties for data users, not only in ascertaining the extent of legal rights and obligations under this aspect of the law, but also by reason of the fact that the substantive law differs between Scotland and England. Under English law it would appear that the right of a parent to act on behalf of a child applies only insofar as the child is considered, whether by reason of age or lack of maturity, to be incapable of acting on its own behalf. This proposition is illustrated in the recent case of Gillick v. West Norfolk AHA(46) where the majority of the House of Lords held that a child under 16 could, albeit in exceptional circumstances, have the right to consent to medical treatment irrespective of parental wishes. In

line with this decision the Registrar has advised data users that when they are faced with a request for access by or on behalf of a child they will have to determine whether the child is capable of understanding the nature of the request. If the child is considered capable a response should be made only at their request, in other cases the parent or guardian's request may be met where this is in the interests of the child subject. Such a state of affairs appears to impose an almost impossible task upon the data user and may constitute one of the few situations where he might reasonably require further information prior to complying with a request for access.

Comment regarding the position under Scottish law is handicapped by the lack of any recent relevant case law. In Gillick, the Law Lords emphasised that the extent of parental rights was not static but varied with the changing social climate. In this respect, it was considered that parental rights are less absolute today than had been the case in the previous century. In referring to the earlier authority of In re Agar-Ellis(47) Lord Fraser commented that:

> "in my opinion, the view of absolute parental authority continuing until a child attains majority which was applied in Agar-Ellis is so out of line with present day views that it should no longer be treated as having any

authority. I regard it as a historical curiosity."(48)

whilst Lord Scarman referred approvingly to dicta of Lord Brandon in the case of Reg. v. D(49) to the effect that:

"The Common Law, however, while generally immutable in its principles..is not immutable in the way in which it adapts, develops and applies those principles in a radically changing world and against the background of radically changed social conditions and conditions."(50)

In the absence of any modern authority, and assuming that a similar view of the role of the Common law would be taken by a Scottish court, comment regarding the state of Scots law must involve a degree of speculation. The Registrar has advised users that:

"In Scotland individuals under the age of 18 are, for legal purposes, either 'pupils' or 'minors'. Until the age of minority is reached (12 years for a girl and 14 years for a boy) the child is a pupil. From that age until he or she reaches 18 the child is a minor.

For a pupil the subject access right

> will be exercised by the person entitled under Scots law to act as the 'tutor' of the child - this will usually be the parent.
>
> Minors will be entitled to exercise the right for themselves. The Data User is not required to obtain the consent of the parent or other 'curator' of the minor. A request by a minor's parent or curator should only be complied with if there is evidence that the minor has authorised the request."(51)

To the extent that this advice refers to pupil children it is clearly correct. It is less certain, however, that it accurately reflects the legal position in so far as minors are concerned. It has been argued that the basis of parental rights in Scots law is founded not on questions of the child's capabilities but:

> "..from a regard to the inexperience and maturity of judgment on the part of the child which requires friendly and affectionate counsel and aid."(52)

On this basis parental rights will continue beyond the stage where a minor is capable of understanding his

actions and, it has been argued, may be exercised "unless it is clearly against the child's interest to do so."(53) In order for this right to have any meaning it is necessary that parents should be informed of matters affecting the child, a practice that must include access to personal data held on computer. Should this argument be accepted by the courts, and it must be conceded that a counter argument exists to the effect that parental right terminate upon the child's reaching the age of maturity, it would appear that, where personal data is held concerning a minor child, a dual right of access may exist and the life of the data user be further complicated. Even assuming that the Registrar's advice to users is correct, they will be required to make decisions as to the maturity and understanding of a child, decisions which have tested, and indeed divided, the highest courts of the land.

3. The Cost of Access

Prior to considering any request for subject access the user is entitled to demand a fee. The question of the amount of this fee has proved one of the most controversial aspects of the subject access provisions. The Act empowers the Secretary of State to fix, by order, a maximum fee which may be charged by data users.(54) Significantly, although the Secretary of State is obliged to consult with the Registrar before fixing the level of any fees which may be paid to the

Registrar, for example those due at registration, there is no similar obligation in relation to the subject access fee. Despite the lack of a statutory consultation procedure the Registrar arranged for a survey of public attitudes towards fees to be conducted the results of which were transmitted to the Government. This survey revealed that the majority of individuals surveyed considered that a fee of between £3 and £5 would be reasonable.(55) Equally significantly, the Registrar's survey indicated that, although estimates of the cost of responding to requests for subject access ranged from £1 to £75, only 3% of data users expressed a desire to levy a fee in excess of £5. Although the Registrar did not formally recommend any level of fee he commented that:

> "During debates in Parliament, the Minister suggested a maximum subject access fee of between £3 and £8. In the light of the research results, this seems an appropriate sort of range. A fee towards the bottom end of this range would meet the public's requirements, be comparable with the fees in other European countries and be not too dissimilar from the charge of £1 made for access to credit reference files under the Consumer Credit Act."(56)

The tenor of the Registrar's remarks would would appear

broadly compatible with the expressed views of the Lindop Committee. Arguing in favour of a low level of fee for subject access the Committee were willing to accept that this would involve some users in financial loss whenever they responded to a request for subject access; a proposition which they justified by arguing that:

> ".. the guiding principle to be applied in fee negotiations should be that reasonableness for the data subject should override operational inconvenience for the user."(57)

This recommendation must be taken, however, in the context of the Lindop recommendations for the establishment of statutory codes of practice for the various forms of data processing. Thus the level of fee could vary depending upon the particular application. This approach proved anathema to the Government in sponsoring the Data Protection Act but, it is submitted, the ability of codes to provide detailed regulations for specific areas of activity would have been of considerable benefit in relation to all of the aspects of subject access discussed above.

In the event the fee for subject access has been fixed at £10.(58) Initially, this level of charge may be contrasted with the position regarding subject access under the Consumer Credit Act where applicants may be

obliged to pay a fee of £1. It must be accepted that the two situations are not precisely comparable; whilst credit reference agencies may be assumed to be organised on the basis that individual records will be drawn out of the data bank this may not be the case with all data processing activities. Personal data may frequently be held for a variety of purposes with the complete details relating to a data subject seldom being withdrawn as an entity. In such a case the cost to the user of satisfying a request for access may be considerable. Even on this basis, however, the level of fee appears excessive. Bearing in mind the Registrar's finding that only 3% of users would seek a fee greater than £5 it appears that the demands of a tiny minority of data users have been allowed to prevail. Whilst the statutory fee represents a maximum figure the suspicion must be that it will become a de facto standard. Support for the proposition that the legislation's approach is susceptible of misinterpretation or abuse can be found in the case of the University of Strathclyde which has indicated that it will levy a fee of £10 in the case of requests for subject access this being:

> ".. the level recently recommended by the Home Secretary.."(59)

Not only is no such recommendation made in the enabling regulations; but this level of fee represents, in the

case of access to examination results, a five fold increase over the charge previously levied for this facility. Early, and very limited, research has identified major differences in approach between users. Whilst Glasgow District Council have decided against levying any fee in respect of subject access to files held by them, Edinburgh District Council levy the maximum fee of £10. In explaining his authority's approach the Data Protection Officer for Glasgow District Council has commented that the council recognised that it was in their own interests to ensure that the information they kept was accurate and that the participation of data subjects in the record keeping process provided a valuable means of attaining this objective.(60)

Even assuming that all data users do not levy the maximum charge, it may be suggested that the less scrupulous data users, who should be subjected to the most stringent scrutiny, may find the level of fee permitted an excellent weapon in any attempt to minimise the invocation of the subject access provisions. At the theoretical level the debate as to the amount of the fee charged for access to data can be related to differing philosophies as to the purpose of subject access. A high fee must signal a belief that a subject should only seek access in exceptional circumstances; that access is to be a rare event, undertaken, perhaps, after the subject's suspicions

have been raised concerning the activities of a particular user. In this respect subject access can be seen as a surgical procedure. On the other hand, were access to be either free or subject to a small or nominal charge, the message might be transmitted that access is an essentially preventative step, to be invoked not upon actual suspicion but from a general desire on the part of the subject to increase the level of control enjoyed over his own affairs. Placing the most friendly construction upon the level of fee provided for, it may be concluded that it represents an increase upon the Government's own estimates, that it is significantly higher than that sought by the vast majority of data users, at a level considered unreasonable by a large majority of data subjects, appears out of line with the views of the Registrar and, finally, will do little to promote the exercise by data subjects of their right of access. The Government's attitude in this respect must cast considerable doubt upon their committment to the philosophy and values of data protection.

Concern about the wisdom of the Government's approach cannot be limited to internal considerations. A £10 fee may give rise to challenge on the basis that it violates the Convention's requirement that subject access be granted "without excessive .. expense".(61) Although this must envisage the levying of some fee in respect of subject access, the level of fee applying in

the United Kingdom appears significantly greater than that of other signatory states. Although the determination what may be considered an excessive fee is largely a subjective one, any form of charge must inhibit subject access to some extent and it may prove particularly difficult for the United Kingdom authorities to justify the disparity between the fees charged under the Consumer Credit and Data Protection Acts. Whilst the variety of applications regulated under the Data Protection Act may include some which are not designed with a view to the information being withdrawn in the manner required to comply with a demand for subject access and, therefore, the costs to the user of compliance may be higher it is doubted whether these difficulties are widespread or severe enough to justify a general disparity in cost. Even where the constraints of his system may make it difficult and expensive for a user to withdraw all the information held concerning a particular subject, the possibility exists for that user to split his registration and require that the subject specify that portion of his records to which he requires access.

A further recommendation of the Lindop Committee which was not acted upon was the suggestion that where an individual obtains access to personal data and discovers an error in the data he should be entitled to a refund of any fee which he has paid.(62) Such a situation applies, for example, in France.(63) It is

difficult to conceive of any justifiable reason why such a system should not operate within the United Kingdom. Whilst a refund may not be appropriate in the situation where errors are minor in nature and do not affect the substance of a record, its provision might encourage subject access and provide recognition of the fact that any improvement in the accuracy of records must be to the benefit of both users and subjects. The impression is instead given that access is a privilege bestowed upon data subjects in respect of which they must expect to make payment. A second consequence which may result from the high cost of access may be that the subject access provisions are separated in the subject's mind from the remainder of the data protection principles, in particular, that relating to the accuracy of data, instead of demonstrating the totality of data protection.

4. Frequency of Access

In the event that responding to access requests causes loss to a data user, he may be particularly concerned in the event that a particular subject makes numerous requests for access. The Convention and the principles require that a user be entitled to access "at reasonable intervals."(64) Once again, neither the Convention not the Act elaborate upon this provision. Under the Consumer Credit Act no restriction is placed upon the number of requests for access that may be made

to a particular agency by a particular individual, the only requirement being that each application be accompanied by a fee. In many cases the same approach would no doubt be appropriate under the Data Protection Act. In cases where a data user feels that the access system is being abused he is entitled to refuse access. In this event two options are available to the data subject. First, a complaint may be made to the Registrar. In this event the Act provides that the Registrar:

> ".. may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected; and where the Registrar considers any such complaint he shall notify the complainant of the result of his consideration and of any action which he proposes to take."(65)

In this event the appropriate course of action for the Registrar, should he uphold the subject's complaint, would be to serve an enforcement notice upon the user.

In the event that the data subject does not wish to rely upon the Registrar a complaint may be brought before the courts. Here if the court:

> "... is satisfied on the application of any person who has made a request (for access)... that the data user in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request; but a court shall not make an order under this subsection if it considers that it would in all the circumstances be unreasonable to do so, whether because of the frequency with which the applicant has made requests to the data user under those provisions or for any other reason."(66)

It may be that the fact whether responding to requests for subject access involves the user in financial loss would be a relevant factor in determining the frequency of requests which would render a subsequent refusal reasonable. The abstruse concept of reasonableness must promote uncertainties which may serve to deter data subjects from exercising their rights and it must be doubted whether many would have either the resources or the determination to pursue a claim through the courts. Whilst recognising that data users are entitled to be protected against the actions of data subjects when these are prompted by malice, it is submitted that a preferable approach to this problem would be to lay down a minimum access entitlement; perhaps one application to a particular user per year and provide

that whilst more frequent applications may be made these may be rejected if they are considered excessive. This approach has been adopted under the Swedish Data Act of 1978 which provides that:

> "At the request of an individual registered the responsible keeper of the register shall as soon as possible inform him of the personal information concerning him in the register. When an individual registered has been thus informed, new information need not be given to him until twelve months later."(67)

In similar vein, the Danish Public Registers Act of 1978 provides for a twelve month moratorium upon the right of subject access except in the situation where the data subject:

> "can prove any special interest in such renewed application."(68)

Although other legislative approaches eschew any attempt to restrict the frequency of requests for access the closest parallel with the United Kingdom approach may be found in France where the law permits a user to request permission from the National Data Protection and Liberties Commission to deny requests:

> ".. which manifestly are unreasonably numerous,

repetitious or systematic."(69)

Two comments may be made concerning this provision. First, the contrast with the United Kingdom approach must be noted in that the onus is placed upon the data user to seek permission to refuse to comply with a request for access whereas, under the Data Protection Act, the onus is placed upon the data subject to pursue a complaint. In a second respect, however, the French criteria for refusing a request are broader than their British equivalents in that they permit a request to be made for permission to refuse applications which are made on a "systematic" basis. This word possesses connotations of organisation or coordination. In the context of subject access it must be recognised that a coordinated campaign on the part of data subjects to demand access to their data may pose substantial problems for the data user. A trade union engaged in an industrial dispute, for example, might encourage its members to simultaneously make demand for subject access. Especially where a large undertaking is involved such tactics could effectively bring the employer's computer operations to a halt with capacity being utilised in order to satisfy these demands. Other large data users may be equally vulnerable to such tactics. In the field of local government, it has been commented that:

"If there were a concerted campaign by some

> group and we suddenly had 5,000 applications arriving on the same day, we would obviously have a problem in providing the information to each individual within the 40 day period permitted by law."(70)

It may be, of course, that the comparatively high access fee sanctioned under the Data Protection Act would serve to inhibit the use of such tactics. It would not, however, appear that the Act provides any protection to the user in such a situation. Although the defences made available to the user in any proceedings alleging a failure to comply timeously with a request for access conclude with the nebulous phrase that this was due to:

> ".. any other reason."(71)

it would appear that this must make reference to the actions of the particular data subject, for example in failing to supply adequate identifying information. It would appear an extreme step for a court to hold that where an individual is given a precise legal entitlement that this should be denied him in the event that his motive in using it might be malicious. Although the French approach may be criticised on this basis (and it may be argued that it fails to comply with the requirements of the Convention in this respect) a user who wishes to obtain a dispensation

from the obligation to respond to systematic requests for access must make specific request to the data protection authorities. Such a procedure may be considered more acceptable than that which would apply in the United Kingdom where the onus would lie on the data subject to challenge any denial of access.

Considering the implementation of subject access in the Data Protection Act, and taking account of the procedures adopted within other states, an unhappy picture emerges. The Act's provisions may comply with the Convention's requirements (subject to a caveat concerning the cost of access) but this is attained in a niggardly fashion with vague criteria being chosen in preference to precise formulations and with the onus of challenging a refusal placed squarely upon the user. Such a grudging approach towards data protection cannot serve to promote public confidence in the efficacy of the legislation.

5. Access Procedures

Having received an application for subject access the user is normally required to supply any relevant personal data within 40 days.(72) This period begins with the date upon which the user receives the request and ends with the day upon which the details are transmitted to the subject. There appears no particular reason for the selection of a 40 day response period.

Under the provisions of the Consumer Credit Act, requests for access to credit reference agencies files must be satisfied within 7 days.(73) Such a short period of time might pose problems for particular data users whose systems were not designed with a view to regular interrogation of the kind required to comply with a request. In these, and in other cases, the least operational inconvenience might be caused should requests for access be gathered together and processed as a batch at, perhaps, monthly intervals. As originally introduced, the Data Protection Bill provided for a 28 day response period.(74) Subsequently this was extended to 40 days.

The Act's provision of a specific time limit must be contrasted with the approach of the Convention which requires that details be supplied "without excessive delay".(75) Where, under continental data protection statutes, a specific period is specified this tends to be somewhat shorter in duration than that applying under the Act(76) but in the remaining systems the terms of the Convention are repeated vertabim with no specific time limits provided.(77) The United Kingdom approach is not conspicuously generous to data subjects but there appears no reason to believe that it will not comply with the Convention.

The general requirement of a 40 day response is subject to two exceptions. First, in the situation where a

user, having received an application for access reasonably requires the subject to supply further identifying information.(78) In this event the 40 day period will not begin to run until the user has received the further particulars. Second, and more significantly, special provision is made for the situation where the personal data to which access is sought includes exam marks obtained by the data subject.(79) When the Data Protection Bill was published it was pointed out that requiring a response to be made within 40 days of receipt of a request could pose substantial difficulties for many examining authorities. Problems might arise in two respects, first with large scale exams such as the GCE or SCE examinations, several months would elapse between the date of the exam and the date when the candidates would be notified of their performance. Much of this time would be required to modify and refine raw marks which may have been awarded to candidates and stored on computer shortly after the date of the exam. Requiring a response within 40 days could result in candidates seeking access to these initial marks in order to obtain an indication as to their likely final performance. The need to employ staff resources to satisfy such requests could serve to delay the date of formal publication of the final results. Problems were also envisaged with the 40 day period where student performance was assessed on a continuous assessment basis. Although in most cases students would be

informed on their performance as the course progressed it was argued that circumstances existed under which some portion of the assessment should be kept secret until the completion of the course.

In order to alleviate these difficulties, special provisions were introduced into the Act offering examination authorities a choice as to the method of compliance with requests for subject access. The first alternative would be to operate the general rules for access. If this should involve logistical difficulties the maximum period for complying with requests may be extended to the earlier of five months from the date upon which the request is received or forty days subsequent to the date upon which the results are announced.(80) The somewhat unusual period of five months is designed to take account of the specific timetabling needs of the English GCE examinations. An examining authority wishing to take advantage of this extension will, however, discover that it contains a sting in its tail. Where more than 40 days elapse between receipt of the request and the user's response it is provided that:

> ".. the information to be supplied pursuant to the request shall be supplied both by reference to the data in question at the time when the request is received and (if different) by reference to the data as from time to time held

> in the period beginning when the request is received and ending when it is complied with."(81)

The effect of this is that the data subject is entitled to be supplied not only with details of his final mark but also with those of any preliminary marks or comments which appeared on the computer at any time subsequent to his request for access being submitted. The complexity of this procedure should not be underestimated. In arguing that a similar provision should not apply to all data users, the Minister of State commented that:

> "In order to furnish the history of all transactions processed during the month he would need to make substantial changes to its processing. That would involve reprogramming the system, redesigning and enlarging the files to hold the extra data and, possibly, completely replacing his present hardware and software at considerable expense."(82)

In addition to the administrative burdens, the effect of such a procedure upon examining processes and student response thereto could be significant. A major objection to the supply of definitive marks to students has rested on the assumption that an increase in appeals will follow if students become aware that they

have narrowly failed either to pass an exam or to be awarded a higher grade. The effect may be even more significant were a student to become aware that he had originally been awarded a pass mark but that this had subsequently been reduced to a fail.

The provisions relating to access to examination marks provides an excellent illustration of the conflicts which may result when established practices of secrecy come into conflict with the principles of openness and accessibility espoused by the Data Protection Act. It may certainly be argued that the effect of subject access will be to require examiners to adopt more objective criteria in their assessments than has hitherto been the case. There may be debate as to whether this marks a positive or a retrograde step but there can be no doubt that changes in procedure will be required.

It is only in the situation where access to examination marks is delayed beyond the 40 day period that the requirement to supply a full historical record will apply. Under normal circumstances the requirement on the user is to supply a copy of the record as it existed at the date when the access request was received This is, however, subject to the proviso that the copy supplied:

"..may take account of any amendment or

> deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request."(83)

This provision recognises that records held by many users will be subject to continuous amendment and that, as has been described above, the cost of modifying procedures to provide a historical record could be considerable. The requirement that the amendment should be of a routine nature is intended to prevent a user censoring or altering data so as to present a more acceptable record to an enquiring data subject. The suggestion of the Committee of Vice-Chancellors and Principals as to the manner in which this provision could be utilised in order to legally frustrate attempts to obtain access has previously been noted.(84) Whilst comparatively few users may be expected to find themselves in the situation where all data is entered onto computers within a very short space of time and where their administrative requirements for such detailed information is equally short lived, the conduct proposed appears inimicable to the underlying concepts of the legislation. The proposal raises two issues, whether the course of action canvassed would be permitted under the Data Protection Act and, whether such a state of affairs would comply with the requirements of the Convention.

The second element of the problem would appear to have a straightforward answer. The Convention requires that as soon as personal data is processed, which in the example at issue would occur as soon as details were entered onto the computer, the data subject is to be given a right of access to that data. The effect of tactics such as those described above would have the effect of denying access to the data. Were the Data Protection Act to sanction such behaviour there would appear little doubt that it would fail to comply with the Convention's requirements.

Turning to the provisions of the Data Protection Act it would initially appear that the routine deletion of data might effectively defeat the subject access provisions. The first data protection principle requires however, that personal data be processed "fairly and lawfully". The definition of processing contained in the Act includes the deletion of data. On this basis, it is submitted, the Registrar would be entitled to conclude that a data user who routinely deleted data so as to prevent data subjects from exercising their access rights was engaging in unfair processing.

Even assuming that the above proposition is correct the tactics suggested illustrate the problems which may follow from the well intentioned attempts to ease the burdens which subject access may impose upon data

users. The technical problems which may face users were they to be required to record amendments to data have been referred to. The Government's attitude to these was demonstrated by the Minister of State who, when presented with a claim that only a minority of data users might be adversely affected by a requirement to supply historical data, replied that:

> "It is generally easier to treat all data alike to cater for the few exceptions and to treat every record as the worst case."(85)

It may be that the exception goes to prove the rule, but in this situation the approach adopted gives primacy to the economic interests of data users over the rights of data subjects and, rightly or wrongly, one group of users has obtained the impression that the subject access provisions might be evaded. The situation would appear to be one where either a transitional period might be appropriate to allow users to phase in the necessary technical changes to their systems so as to enable them to comply with the Act's requirements, or where the prior approval of the Registrar should be required, perhaps at registration, to the form of processing proposed by the user.

6. Exceptions

In common with all existing data protection statutes,

the Data Protection Act provides that the right of access is not to apply in a number of situations. In these, it is considered, the advantages of access are outweighed by other considerations pertaining to general societal interests, the legitimate needs of the user, the interests of other individuals or even the best interests of the applicant subject. The case for exemptions is recognised in the Convention which provides for these to the extent that they can be considered necessary in a democratic society in the interests of:

> "..protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences.
>
> (b) protecting the data subject or the rights and freedoms of others."(86)

At first glance the scope of these exemptions appears extremely broad. A major limiting factor must, however, be the initial requirement that the measures be necessary and compatible with the ideals of a democratic society. As has previously been discussed in the context of exemptions justified by reference to the needs of national security, this has been interpreted in a restrictive and minimalist fashion. On this basis, it is submitted, several of the Data Protection Act's provisions appear to have been drafted in an

unacceptably broad fashion.

a Identification of Third Parties

Under the Act, the right of access is subjected to one general and a number of sectoral exceptions. In the former situation it is provided that a data user is not obliged to comply with a request for access:

> ".. if he cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request."(87)

Since one of the basic tenets of data protection is the imposition of controls regarding the dissemination of personal data, it is clear that, once again, legislative provisions will have to arbitrate between competing claims. Information may not always be susceptible of neat compartmentalisation with its connection to a particular individual marking an immutable boundary. Society requires considerable interaction between its members and the grant of subject access to one subject may, either expressly or impliedly, disclose information relating to another.

Recognising the existence of conflict, there can be no complaint where data protection legislation attempts to resolve this. Such a solution must inevitably involve a degree of compromise. Where the approach of the Data Protection Act can be criticised is in its failure to attempt any sophisticated and principled analysis of the issues involved. Instead, the Act's provisions impose substantial and often, it is submitted, unjustified restrictions upon the right of access yet, contemporaneously, may face the data user with problems of fact and law which he may have difficulty in solving.

Where the data in question relates to the affairs of the third party, there can be little substantial objection to the exemption provided for above. Any more general right of access to information should be introduced under a freedom of information rather than a data protection statute. The exemption is not, however, limited to this situation, it being further provided that:

> "... the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request.."(88)

Thus where personal data relating to the data subject,

consisting either of alleged statements of fact or statements of opinion, has been supplied by a third party the Act provides for at least a limited denial of access. This is, however, constrained by two further provisions of the exemption. First, it is provided that the exemption cannot be utilised where the third party has consented to the disclosure. Clearly, if the source of data is willing for this fact to be disclosed to the subject, the data user can have no legitimate objection to this. The enquiring subject is, however, placed in an impossible position here. The user need not supply third party data unless he is satisfied that that party has consented to the disclosure. No duty is imposed upon the user to seek this consent. In such an eventuality, the only way in which this might reasonably be acquired would be for the subject to contact the third party. The subject, however, will not be informed of his identity. Second, it is provided that the user must disclose so much of the data as is possible without divulging information relating to the third party. Again, where the information relates to the informant's own affairs, such a task may be relatively simple and non-controversial. The major difficulties will arise where the third party has supplied data relating to the enquiring subject. It may be difficult, if not impossible, for the data user to determine whether simple deletion of the name or other identifying particulars of the source will suffice to conceal his identity from the data subject in the event

that the substantive information or statements of opinion supplied are revealed. Much will depend here upon the extent of the data subject's knowledge, a fact of which the user cannot reasonably be expected to have cognisance.

Analysis of the potential problems resulting from the Act's approach may be assisted by reference to the decision of the House of Lords in the case of D v. National Society for the Prevention of Cruelty for Children.(89) Here, an allegation had been made to the Society concerning the treatment of a young child. Acting on this information, an officer of the society had visited the child's mother. Upon investigation the allegation proved to be unfounded but as a result of the experience the mother suffered severe shock, depression and insomnia. She subsequently brought proceedings against the society alleging that their negligence had caused these injuries. In the course of her action she sought to discover the identity of the informant. This request was opposed by the society who argued that the information had been received under an express undertaking of confidence and that the effect of disclosure would be to inhibit others from reporting suspicions of child abuse to the society. The majority of the Court of Appeal (Lord Denning dissenting) held that the society should be required to disclose the information. Lord Scarman, rejecting the argument that the public interest lay in favour of the confidence

being maintained, posed the question of the nature of society which is to be reflected in the law and concluded:

> "If it be a society in which as a general rule informers may invoke the public interest to protect their anonymity, the law may be found to encourage a Star Chamber world wholly alien to English tradition."(90)

Although the House of Lords reversed this finding on the basis that the work of the society should be regarded as analogous to the work of a policeman and should be afforded the same protection against disclosure as that afforded to the latter in respect of the identity of their informants, the judgments clearly indicate that the extent of the public interest is to be narrowly defined and the mere fact that information has been supplied in confidence would not, per se, suffice to protect it from disclosure.

The parallel between the situation arising in the N.S.P.C.C. case and that applying under the Data Protection Act is far from exact. In the former the issue was whether information should be disclosed in the course of legal proceedings, under the Data Protection Act the issue is whether information should be disclosed upon request and it may be argued that the justification for disclosure is less. It is submitted,

however, that the fundamental issue remains the same, whether the public interest favours disclosure or secrecy. In the N.S.P.C.C. case the House of Lords, although denying disclosure in the particular case, appeared to accept a presumption in favour of disclosure. In this particular area, the Data Protection Act adopts a very different approach.

As the N.S.P.C.C. case demonstrates, the most important question in debate concerning the access to data relates to the extent to which the fact that it has been supplied by a particular party should be concealed from the enquiring subject. In making any assessment on this point an attempt must initially be made to identify the dangers that might follow for a data user and for his sources should the data subject be granted unrestricted access to the information held relating to him. Three possible dangers exist. First, that if the donor of the information acts in the belief that his identity will be kept secret breach of this expectation might result in his being unwilling to supply further information. That this should constitute cause for regret is far from certain. It has been written that:

> "Few situations in life are more calculated to cause resentment in a person than to be told that he has been traduced, but cannot be confronted with his traducer. It is submitted that, ideally, nothing but the very pressing

> demands of public security, where the vital interests of the community are unquestionably involved, can require that private individuals should be expected to acquiesce in their vulnerability by an invisible foe."(91)

It is submitted that those who pass on information concerning another have no legitimate expectation of anonymity simply by virtue of their actions. It may also be argued that as much personal data is transmitted on a commercial basis, the financial interests of those supplying the information will ensure its continued supply.

A second objection to the disclosure of sources lies in the possibility that, assuming the information is inaccurate, the source might face an action for defamation at the instance of the data subject. The possibility of such liability being incurred appears remote. If the source is acting out of a sense of public duty in passing on the information the defence of qualified privilege will be available, rendering him immune to liability in the absence of evidence of malice. In the event that information is passed other than in pursuance of a duty there appears no compelling reason why the source should not face action. In any event, should matters go as far as the institution of legal proceedings it must be considered likely that disclosure would be ordered by the court. It is

significant to note that under the requirements of the Consumer Credit Act a credit reference agency is obliged to supply a consumer with all of the information held including any references to its source. Such a state of affairs does not appear to have caused great problems either for the agencies or for their sources. The argument in favour of divulging the identity of the source to the data subject is undoubtedly strongest in this situation. Whilst the subject will have no cause for complaint in the event that information is accurate should the contrary be the case, there must be a likelihood that the same information has been, or will be, further disseminated. The subject's protection would require that the error be traced to, and corrected at, its source. Even given the cooperation of all concerned this will often be a difficult task. The provisions of the Data Protection Act may serve to place an insurmountable barrier in the path of a subject attempting to cure an error.

The final ground purporting to justify the concealment of the identity of an informant is perhaps the most substantial. That were the informants identity to be revealed to the data subject he might face the risk of physical or mental harassment. The possibility of such a consequence was referred to in the N.S.P.C.C. case and although not explicitly recognised in the judgments may well have influenced the final decision.

Assuming that disclosure would not be justified when this might reasonably be expected to expose the informant to the risk of harm, the first question must be how far the general exception is likely to prevent such a risk? It is submitted that the criteria adopted are too vague to offer substantial reassurance to an informant. The user is required to supply as much information as may be possible without identifying the source. The Act lays down no criteria, however, for determining what will constitute identification. A record maintained by an agency such as the N.S.P.C.C. may state that:

> "X has reported that Smith's child has been left alone and crying in the house on 5 evenings in the last month. Y confirms this information."

Assuming that the information can be assumed to relate to Smith, thereby triggering the subject access provisions, in the event that Smith lives in a large housing estate where many people may reasonably have been the source of the data such censorship may be considered to adequately conceal the identity of the particular source. Even here should Smith suspect, rightly or wrongly, that he knows the identity of the informant the dangers of harassment described above may follow even though disclosure along the lines required might be required under the Act. In an alternative

scenario, assuming the same record, Smith may live in the country with only two neighbours and clearly the substitution of letters for names would be unlikely to conceal the precise identity of the informants. Various other permutations could easily be devised but the above examples perhaps serve to illustrate the difficulties of the situation that the Act's approach may produce for a data user. Censorship of data may cloak in anonymity those who have no legitimate expectation to such privacy yet may prove inadequate in situations where it is justified.

Having criticised the approach adopted in the Data Protection Act it is less easy to suggest viable alternatives. It is submitted, however, that in line with the new regime of openness in record keeping inherent in the concept of data protection the presumption should be in favour of total disclosure. A preferable formulation might be to the effect that the data user must disclose all the data held relating to a particular subject unless he has good reason for believing that a third party source would object to this. In the event that there is a genuine conflict between the claims of disclosure and those of secrecy a much more sophisticated resolution procedure is required. An argument exists for permitting the withholding of data only where this is covered by a specific exemption. As will be discussed, the sectoral exemptions contained in the Data Protection Act would

appear to encompass most situations where the public interest might be considered to justify concealment. The N.S.P.C.C. case demonstrates, however, that information may be held by bodies whose legal status and functions does not admit of easy categorisation - the functions of the N.S.P.C.C. appearing to constitute an amalgam of social work, law enforcement and charitable purposes with a private organisation performing certain public functions. A general provision may be necessary to cope with such circumstances but its scope should be closely circumscribed. It might be reasonable to permit a user to refuse a request for access in circumstances where a similar claim would be accepted were it to be made in the course of legal proceedings. An alternative formulation might make specific reference to the public interest. Thus the Danish Public Registers Act provides that subject access is not to apply:

> ".. if it is found that the registered party's interest in knowing the data in question ought to be overridden by public or private interests."(92)

In the event of any dispute, it is further provided that the determination is to be made by the Data Surveillance Authority, a body performing functions comparable to those exercised by the Registrar. In similar vein, the Austrian Data Protection Act, also

enacted in 1978, provides that where personal data are held by a user in the private sector that the subject shall normally be entitled to access to the data and of its origin. Access may be denied where this:

> "would endanger overriding legitimate interests of the person responsible or of a third party and where this refusal can be justified vis a vis the person affected."(93)

Although the invocation of such criteria would introduce a measure of uncertainty into the United Kingdom legislation, it is submitted that this would be no more substantial than that which already exists under the legislation, whilst the application of alternative criteria would create a more equitable balance between the interests of those supplying data and the subjects of the data.

b. Data Held for Policing or Revenue Gathering Purposes

In addition to the general exemption discussed above which may be utilised by any data user, the Data Protection Act provides for a number of sectoral exemptions applying in respect of particular categories of data user or processing activities. Undoubtedly the most controversial of these exceptions has been that applying in the situation where data is held in connection with:

"(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders; or

(c) the collection or assessment of any tax or duty."(94)

Although it was argued in Parliament that total exemption would be permitted under the Convention it must be recalled that this permits exemption for policing and tax gathering purposes only to the extent that this is necessary in a democratic society. Once again, the jurisprudence of the European Court of Human Rights will be relevant here and in view of the restrictive interpretation previously afforded to this phrase it may be considered that a total exemption would not have been justified.(95) In the event the scope of the exemption is limited by the Act's providing that it is to apply only to the extent that the operation of the subject access provisions would prejudice the attainment of one or more of the specified purposes. As such, there is a considerable degree of similarity between this provision and the exemption to the non-disclosure principle discussed in the previous chapter. The background to the two provisions is, however, substantially different. In relation to non-disclosure the point must be made that, prior to the Act's introduction, data users could make

whatever use of data that they pleased without facing the risk of any criminal or administrative sanctions. The exemptions to the non-disclosure principle retained the status quo, albeit in a limited area, and could be criticised on the basis that they, at best, made only marginal improvement to the individuals data privacy and, at worst, might lead to a de facto erosion of his position. By contrast, the subject access provisions have to be contrasted with the previous situation in which the individual possessed no right of access whatsoever to personal data. Although the right of access may be restricted, and the extent of these restrictions will be criticised in this thesis, there appears no question that the individual's position, vis a vis the data user has been improved as a result of the passage of the Data Protection Act.(96) In general terms, the provisions relating to access to police and tax records offer some promise of a significant extension in the level of accountability required of those who compile and maintain such records.(97)

Whilst few would deny the need for the police and taxation authorities to maintain records it must be accepted that this information, when acted upon, can have the most serious and detrimental consequences for the individual. In the event that the information is inaccurate such consequences cannot be justified whilst, even if the information should be accurate the infringements of rights involved in its acquisition or

the consequences which may follow from its storage and utilisation, may be considered disproportionate to any offence which may have been committed.

Although, as has been stated previously, police information gathering and processing practices are exempt from the application of the first data protection principle requiring that data be obtained and processed fairly and lawfully,(98) the remainder of the data protection principles are applicable. Thus, for example, data held must be adequate, relevant and not excessive, it must be accurate and timeous. In these circumstances, subject access provides the optimum, and perhaps the only, method by which compliance with the principles' requirements can be verified. Against this, it must be recognised that circumstances may arise in which the public interest in efficient and effective policing may require that an individual should be denied the opportunity to ascertain the nature and extent of information held concerning him.

In recent years concern over police record keeping practices has centred both on the scale of such activities and also at the degree of secrecy with which they are surrounded. The Lindop Committee attempted to gather evidence on these matters but its experiences with the Metropolitan Police prompted the observation that:

"We visited the Police National Computer (PNC) at Hendon and we received evidence from the Home Office, from police representatives and from other individual witnesses. Most of the evidence that we received from the police was helpful and willingly given, but the Metropolitan Police seemed to assume that a wide exemption would be granted for police applications and that it was therefore not necessary for us to receive detailed information on some of them about which we made pressing enquiries. The observations we make on any applications are of value only to the extent that the information on which they are based is adequate; in the case of the Metropolitan Police we have not been able to satisfy ourselves that this is so."(99)

From this the conclusion followed that:

"While we have no reason to believe that the public need be unduly alarmed by the general use of computers for police purposes, in relation to the Metropolitan Police we do not have enough evidence to give a firm assurance to that effect for all aspects of such use by them."(100)

One encounter between the Committee and representatives

of the Metropolitan Police was subsequently recounted by a member of the Committee. After objecting to a request from the chairman that their evidence be recorded on tape, on the basis that:

> "..there are members of your committee whose loyalty we cannot take for granted."(101)

the performance was characterised as one:

> ".. of truly magnificent stonewalling. Any old lag who is accustomed to being pulled in by the and who wants a lesson on how to dodge difficult questions could have learned a lot from the senior chief officers of the Met. They were not prepared to be drawn on any matter of substance as far as the computerisation of police records or the computerisation of police information was concerned."(102)

Upon the Committee's facing its witnesses with media reports concerning the scale of investment in computer facilities it proved:

> "..impossible to draw from our visitors either confirmation or denial, even of the most tight lipped variety."(103)

To some extent the position regarding secrecy of police

practices may have been improved by the registration requirements imposed upon the police under the Act although the information required here is of the most general variety.

In discussing the extent of the access which may be permitted to police records, the point must be made that the Act establishes a presumption in favour of access. In order for such a request to be legitimately denied the purpose for which it is held must first be established, the exemption applying where data is held in connection with crime prevention or detection or with the apprehension or prosecution of offenders. The inclusion of crime prevention in this list of categories constitutes one of the most controversial features of the exemption and a proposal that it should be deleted from the failed by a single vote during the Bill's Committee stage.(104) Although few would dispute the argument that the prevention of crime constitutes as important a component of policing as its subsequent detection this may, by its very nature, involve the maintenance of records on persons who have not been convicted of any criminal offence. Considerable publicity has been given to allegations that the processing powers of computers have been seized upon by several police forces in order to launch fishing expiditions with officers required to report any item of information which may have been passed on to them or which may have come to their notice. To a considerable

extent, the operational effectiveness of officers will be gauged by the volume of information supplied by them.(105)

The storage capabilities of computers coupled with the development of free text retrieval systems allowing information to be stored in an unstructured form make it feasible for more extensive information files to be maintained than was the case in the pre computer era. An example of such practices and of the consequences which may befall an individual was reported in 1985:

> "One piece of malicious gossip - to the effect that a certain man was a paedophile - was overheard in a village shop by a policeman's wife and subsequently found its way onto a police computer. When the man in question came to apply for promotion his employers engaged a professional organisation that dealt with personnel intelligence to check his background. The computer record came to light and, needless to say, his advancement was halted."(106)

The above example serves to demonstrate some of the problems which the operations of the data protection principles may cause both for data users and data subjects. The fact that the information was received by a third party might suggest a breach of the eighth data protection principle requiring that adequate security

precautions be built into a computer system. It has, however, been announced that several local authorities are proposing to check with the police authorities on the backgrounds of those who are applying for positions which will bring them into contact with children. Analysis of the legal position regarding these issues discloses a situation of considerable complexity and uncertainty.

Where information, such as that described above, is held by the police themselves it is difficult to argue that it is held for crime prevention purposes. Unless the information relates to a specific offence, e.g. a planned bank robbery, and its subject is to be kept under continuous scrutiny the information will not prevent him committing an offence. To this extent, it is submitted, a request for subject access could not be denied on the basis that it would be detrimental to the purpose of crime prevention.

If the holding of data in the above circumstances cannot be justified by reference to the prevention of crime, consideration must be given to the remaining exceptions relating to the detection of crime or the apprehension or prosecution of offenders. Here, publicity has recently been given to the involvement of computers in the course of major police investigations with the equipment being used to collate and process vast amounts of data. Although there appears little

evidence that the involvement of computers has improved the proportion of serious crimes solved by the police this can be seen as a classic example of personal data being processed for crime detection purposes. In the above example should it be the case that the subject was suspected of having committed an offence there could be little doubt but that the information would be regarded as held for the purposes either of the detection of crime or the apprehension or prosecution of offenders. In more general terms, it may be argued that almost any item of information may be of assistance in the detection of crime. The list of car owners maintained by the DVLCC and transferred on a daily basis to the Police National Computer has proved a useful tool in aiding the detection of stolen vehicles and in the detection of other offences in which a motor vehicle was involved. To this extent it may be argued that the information is held in connection with the detection of offenders even though particular offences may not have occurred.

Subject to the above argument, it may be doubted whether the information, as held by the police authority, would benefit from any of the Act's exceptions. Should the information be disclosed to a third party such as an education authority, however, it could be strongly argued that this was for the purpose of crime prevention. As such the disclosure would be sanctioned under the exceptions to the non-disclosure

principle even though the authority might not have been registered as a potential disclosee by the police authority. The end result is that information which is arguably held for a non-exempt purpose can be transferred for an exempt purpose. In the event that the information is disclosed and is recorded by the recipient authority the question of the purpose for which it is held will, of course, arise again. The conclusion must be that the status of particular items of information will vary from time to time depending upon the use to which it is put.

The question whether data is held for the prevention or detection of crime constitutes, of course, only one aspect of the equation concerning the application of the subject access provisions. More significant than arguments about whether data can be regarded as held for preventional or detectional purposes (or indeed for the purposes of the other exemptions specified in the Act) is the fact that access may be denied only to the extent that it can be demonstrated that this would be prejudicial to that purpose. The extent to which access will be so regarded constitutes one of the most significant issues under the legislation. As has been indicated, virtually all information can be regarded as being held for an exempted purpose and it may be argued that a portion of the value attaching to any such data is dependent upon the fact of its possession by the police should not become known to the subject. Even at

this level, however, a distinction should be drawn between intelligence information which may be speculative and factual information, such as records of criminal convictions. There can be no case for refusing subject access in respect of the last mentioned form of information. It must be assumed that the subject is aware of the fact that he has been convicted and of the fact that details of convictions will be recorded by the police. Allowing access to such records cannot be seen as in any way prejudicial to their purposes and, whether a request comes from an individual who has a criminal record but who wishes to check that this is accurate or whether it comes from one with no criminal history who wishes to ensure that he has not been confused with another person, it is submitted that access must be granted (in the case of the second enquirer discussed above the response will, hopefully, be a negative one). More difficult issues arise with respect to access to intelligence data. In one respect the claim for access is greater here, this data is, by its very nature, speculative and the possibility of its being erronious or misleading must be considerable. The argument against disclosure is equally clear. This data may comprise a valuable policing asset but much of its value will be dissipated should the subject become aware of its existence and extent. It may of course be argued that much of this information must be regarded as held for crime prevention purposes. Thus the police may receive information indicating that a particular

individual is planning to commit a criminal offence. The individual may be placed under surveillance and further information garnered as a result of this activity. In most cases, the act of planning a criminal offence is not, per se, illegal. In these circumstances the information can only be regarded as being held for for the purposes of crime prevention. There appears a degree of logic in the assertion that if information exists indicating that an individual is planning to commit an offence, that the interests of crime prevention would be best served were the individual to be told of the information held about him. Knowledge that his plot had been discovered might be considered likely to prevent at least that particular crime. In the event that access were to be requested and denied in such circumstances might lead to the conclusion might be to the effect that this form of crime prevention does not mean preventing the crime being accomplished but does involve catching the perpetrator red handed.

In performing the delicate balancing act required between these two demands it has to be accepted that whatever criteria for access may be devised there will be situations where an individual will be denied access to data which is erronious and which, if acted upon could prove detrimental to his interests; alternatively, the granting of access may be to the benefit of a criminal data subject. The question for

the Registrar and the courts must be which evil is to be preferred? It is submitted that the criteria which would be most in accord with the aims of data protection would be to the effect that access may be denied where this would be likely to prejudice the prevention or detection of a specific and serious offence. Whilst there is clearly a difficulty in determining what is a serious offence, the argument against incorporating such a definition in relation to the exemption to the non-disclosure principle cannot apply to this situation which is very closely analogous to that predicated in the Police and Criminal Evidence Act relating to a police officer's powers of arrest. It is relevant here to note than under the German federal Data Protection Act which applies similar criteria to the British in respect of subject access to police records that some 70% of requests for access to such data have been complied with.(107) Although national circumstances may vary, such a figure may serve as a benchmark as experience of the operation of the United Kingdom system develops.

The extent to which the subject access provisions will apply in this area is dependent upon the decisions of the Registrar and of the courts. Unfortunately, the extent to which instances of denial of access may be brought to their attention is limited by the nature of the response which may legitimately be given by a user to a request for access. In the event that the user

determines that information constituting the subject matter of a request for access is held for one of the excepted purposes and that the grant of access would prejudice that purpose, he is entitled to inform the data subject that he does not hold any personal data to which he is required to grant access. In strict legal terms such a response is accurate but may be highly misleading. Whilst the justification for such a policy vis a vis the data subject is readily apparent - a statement to the effect that data is held but which is covered by an exception to the subject access provision may prove almost as illuminating as the supply of a copy - the nature of the proceeding appears unsatisfactory. It may be argued that the user should be obliged to inform the Registrar of the fact of, and the circumstances surrounding, the refusal.

In the event that an applicant is faced with the above response two further courses of action are available. First, a complaint may be lodged with the Registrar requesting that he investigate the situation. Following such enquiries, one option available to him will involve service of an enforcement notice requiring the user to supply a copy of the contested information. As an alternative to involving the Registrar the data subject is entitled to bring proceedings before the courts with a view to obtaining an order compelling disclosure. In the event that the latter option is exercised it is additionally provided that, for the

purpose of making its determination the court:

> ".. may require the information constituting any data held by the data user to be made available for its own inspection .."(108)

Perhaps surprisingly, no similar power is vested in the Registrar who, save in the event that he makes application to the courts for a search warrant, will be required to make a determination on the basis of the complaint and on any information which may be volunteered by the data user. It is submitted, however, that as the Act contains a presumption in favour of access save in specified circumstances, in the event of the Registrar acting upon a data subject's complaint the onus of establishing that data is held for one of the specified purposes and that access would be prejudicial to that purpose must rest with the data user. If this argument is correct, the consequence would be that silence would not benefit the data user. In the event that the user responds to the Registrar's enquiries, the latter will have to determine whether the refusal of access is justified. Although the legislation does not specify the criteria that are to be applied in such circumstances it would appear to be the Registrar's view that each refusal of access must be justified by reference to its particular circumstances.

Despite uncertainty as to the extent of the new right of access to police and tax data provided under the Data Protection Act it is undoubtedly true that these provisions mark an extension of the rights of the individual. Hitherto, no right existed to obtain access to data held by these organisations. However the Act's provisions may be interpreted, any degree of access marks an extension to the status quo. The enshrinement of individual rights is not the only significant development in the Act. The procedures whereby a refusal of access may be challenged before the Registrar or the courts, with both empowered to order access and with the former able, by means of service of an enforcement notice, to prescribe the approach which must be adopted to any future requests for access. This marks, it is submitted, the first occasion upon which the record keeping practices of police forces and tax authorities have been subjected to independent scrutiny. In respect of both these factors the Registrar is given considerable discretion and it is to be hoped that it will be exercised, wherever reasonably possible, in favour of the individual.

c. Financial Services

Although much criminal detection will be conducted by police forces, a variety of criminal or quasi-criminal functions are exercised by other regulatory authorities. Where investigations are in train it may

be as undesirable to permit subject access as is the case with police data. Accordingly, the Data Protection Act provides that the Secretary of State may provide that the access provisions are not to apply in respect of statutory functions where these are designed to protect the public:

> ".. against financial loss due to dishonesty, incompetence or malpractice by persons concerned in the provision of banking, insurance, investment or other financial services or in the management of companies or to the conduct of discharged or undischarged bankrupts."(109)

The scope of this provision was extended by the Financial Services Act 1986 to include the activities of recognised self-regulatory authorities concerned with the maintenance of standards within the financial sector.(110)

In applying this principle the Data Protection (Regulation of Financial Services etc.) (Subject Access Exemption) Order was made in 1987(111) and contains an exhaustive list of the functions and the agencies whose activities are to be exempted from the subject access provisions. Such treatment would appear to be justified under the Convention either on the basis that the conduct in question may be criminal or that it may

operate against the interests of investors or other members of the public. It may be noted, however, that the exemption cannot apply in respect of any internal arrangements which may be made by a financial institution to monitor the compliance of its own members of staff with legal requirements.

d. Medical Data

Moving on from the areas of police and tax records, the Act provides for restrictions to the right of access in several other significant fields. Particular problems have been identified where medical records are involved. The Convention recognises that medical data possesses an exceptional degree of sensitivity which may call for especially stringent controls to be imposed upon those data users active in this field.(112) It might appear to follow from this that the case for the operation of the subject access procedures is also exceptionally strong in this field. The reality is, however, less clear cut. Such records often include technical terms which are not, and may not realistically be rendered, intelligible to a non-professional. Again it may be argued that these records may contain clinical assessments of a patient and prognosis as to their future health prospects. Such data is frequently provisional or speculative and the grant of subject access may have the effect of causing unnecessary distress to the data subject.

Taking the above factors into consideration, the Convention, nonetheless, maintains a presumption in favour of access, providing that a request to this effect may only be denied where this is necessary in the interests of:

> ".. protecting the data subject or the rights and freedoms of others."(113)

Save in the situation where information on a medical record relates to a third party, any exemption in this area must be justified by reference to the interests of the applicant data subject. In view of the underlying premise of data protection legislation that openness in record keeping is required in order to promote public confidence, the proposition that secrecy may be beneficial to the individual's interests appears a contrary one. Although to justify any interference with the individual's right to know by reference to perceptions of his own best interest may appear a paternalistic approach, the Convention must be seen as recognising the possibility of a conflict between the patient's "right" to subject access and the physician's obligation to act in the best interests of a patient. Circumstances may arise in which it is perceived that this will be best accomplished by keeping information from the patient.

In applying the Convention's provisions, the Data

Protection Act provides that the Secretary of State may:

> "..by order exempt from the subject access provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health of the data subject."(114)

This power was exercised prior to the subject access provisions becoming operative with the making of the Data Protection (Subject Access Modification) (Health) Order 1987.(115) This applies in relation to data held or compiled by, or on behalf of, a health professional and establishes as the criteria for refusing an application for access the belief that this:

> ".. would be likely to cause serious harm to the physical or mental health of the data subject .."(116)

Where only a portion of the record is considered likely to have this effect, and this can be severed from the remainder of the record, access must be supplied to the latter portion. With reference to the impact of access upon the interests of others it is provided that a request may be denied where this:

> ".. would be likely to disclose to the data

> subject the identity of another individual (who has not consented to the disclosure of the information) either as a person to whom the information or part of it relates or as the source of the information or enable that identity to be deduced by the data subject either from the information itself or from a combination of that information and other information which the data subject has or is likely to have."(117)

This latter provision will not apply to the extent that the other individual referred to is a health professional involved in the care of the data subject.

In respect of all requests for access to data coming within the scope of the Order, it is provided that the decision to grant or to refuse the application must be made by the "appropriate health professional"; defined as the medical or dental practitioner best qualified to advise on the patient's case or, in the absence of such a person:

> ".. a health professional who has the necessary experience or qualifications to advise on the matters to which the information which is the subject of the request relates."(118)

By providing that access may be denied only to the

extent that this would cause "serious harm" to the health of the data subject, the Order must be seen as establishing a strong presumption in favour of access. As is the case where police or tax data is withheld under the terms of an exemption, such a decision may have to be justified before the Registrar or the courts. Concern must, however, exist both as to the manner in which the access procedures will be operated and as to the exceptions provided under the legislation.

Whilst recognising that circumstances, particularly those connected with psychiatric illness, may exist in which the supply of a copy of a medical record may not be in the best interests of the patient, it may be doubted whether the procedures adopted under the Order are, in themselves, likely to prove any less harmful. In common with the situations arising under other exemptions, a health professional may respond to a request for access with the statement that no relevant personal data is held. To a perhaps greater extent than with the other exceptions, the data subject is likely to be aware of the fact that data is held. The failure to supply data may well be a source of distress in itself whilst discovery of the fact that the data has been withheld for fear that access would cause serious harm to the patient's health would, in itself, appear inimicable to his or her health interests. Whilst it may be expected that the above factors will be taken

into account in deciding whether the grant or the refusal of access would best serve the patient's interests, it is submitted that the mechanism provided under the Act is intrinsically unsatisfactory. The prime purpose of the subject access provision is to benefit the individual. This must take precedence over the procedures through which it is obtained. Whilst in most cases the administrative convenience of the data user and the interests of the subject can best be served through the supply of a copy of the information held, situations, epitomised by those currently under discussion, exist in which a different procedure would be preferable. A model for such an alternative can be found in the French data protection statute which provides that:

> "When exercise of a right of access applies to medical data, these may be disclosed to the person concerned only through a doctor designated by him for this purpose."(119)

Whilst it must be accepted that such an approach may fail to overcome the suspicions or even paranoias of a minority of patients, the general regime established under this legislation would appear to provide a more suitable and sympathetic environment for this form of subject access than that pertaining under the Data Protection Act.

e. Social Work

As is the case with medical records, the Data Protection Act adopts the view that, in certain situations, access to a social work record may be inimicable to the data subject's interests. Once again, the legislation lays down general criteria and delegates regulatory power to provide for the detailed application of any exception. The Act here provides that:

> "The Secretary of State may by order exempt from the subject access provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the order, being information -
>
> > (a) held by government departments or local authorities or by voluntary organisations or other bodies designated by or under the order; and
> >
> > (b) appearing to him to be held for, or acquired in the course of carrying out social work in relation to the data subject or other individuals;
>
> but the Secretary of State shall not under this subsection confer any exemption or make any

> modification except so far as he considers that the application of those provisions (or of those provisions without modification) would be likely to prejudice the carrying out of social work."(120)

Although this provision appears similar to that regulating the extent of access to health data, the empowering provisions differ in that whilst in respect of health data the Secretary of State's discretion is unfettered; in the area of social work derogation is permitted only in situations where access would prejudice the carrying out of social work functions. In Parliament, several examples were supplied as to circumstances under which this power might be legitimately invoked. It was, for example, stated by the Minister of State that:

> "We have in mind the subject who might be too unstable or immature to accept the truth about himself or perhaps an elderly person who might be unnecessarily upset by disclosure that he was not as welcome a guest in the family as he thought he was. Usually social workers will counsel a client until he is able to accept the information in question, but there may be circumstances where this is not possible. In such a case we should not rule out the possibility that the data should be

withheld."(121)

It was further indicated that exemptions might be required in respect of social worker's assessments of their clients, it being asserted that:

> "It is important that social workers should maintain full and frank records about their clients, and in many cases there will be no reason why there should not be full disclosure of those records. But there might be a danger that social workers would become less frank in the observations which they recorded if they thought that they would be revealed in full to their clients. Moreover, the relationship between the social worker and the client might itself suffer if these observations were all revealed to the subject."(122)

Whilst derogation in the first situation described above could be justified by reference to the Convention's provision empowering derogation in the "interests of the data subject" the legitimacy of exemption in the second scenario is open to question. This would appear to be based upon the premise that subject access should be limited where this would be in the best interests of the data user. Whilst it may be argued that the interests of data subjects generally would be best served by ensuring that social workers

compiled full and frank records of their views, any refusal of access must be justified by reference to the particular subject. Apart from the question of compatibility with the Convention, the above view must be contrasted with that of the Lindop Committee which, after considering the issues involved in this field, concluded in favour of an unqualified right of access to social work data except where this would prejudice the confidentiality of those third parties who had supplied information to social work authorities. Noting criticisms that social work records were often compiled by unqualified staff, that they contain information which was "inaccurate subjective and irrelevant" and that the data was often used for a variety of purposes so that the effect of a single entry could impinge upon many aspects of the subject's life, the committee concluded that:

> "We think, therefore, that where information about a social work client is handled by automated means, the client should normally be able to see that information and check it. In our view the granting of this right would have several advantages. The first, and most important, is that it would lead to an improvement in the accuracy and quality of the information recorded. If, as the BASW suggests, it causes a social worker to think twice before placing information on computer so much the

better. It should also lead to a more standardised recording practice. Finally, it would serve to dispel the kind of suspicion and unease expressed by the National Association for Mental Health (MIND), which is perhaps also shared by some social work clients."(123)

In the event, the provisions of the Data Protection (Subject Access Modification)(Social Work) Order 1987(124) define the extent of subject access to social work data. Data will be regarded as held for this purpose if is maintained in the course of specified statutory or voluntary functions. Thus it is provided, for example, that data maintained by the N.S.P.C.C. will, assuming it relates to a welfare function, be regarded as coming within the scope of the exemption. In these circumstances, access may be denied where it:

"..would be likely to prejudice the carrying out of social work by reason of the fact that -

(a) serious harm to the physical or mental health or emotional condition of the data subject would be likely to be caused; or

(b) the identity of another individual (who has not consented to the disclosure of the information)

> either as a person to whom the information or part of it relates or as the source of the information would be likely to be disclosed to or deduced by the data subject or any other person who is likely to obtain access to it either from the information itself or from a combination of that information and any other information which the data subject or such other person has or is likely to have."(125)

As is the case with health data, it is provided that this latter provision cannot be utilised in order to conceal the identity of the person responsible for the compilation of the record or a part thereof. Again, where data would lead to the identification of a third party, where possible, these details must be severed from the remainder of the record.

Although the provisions relating to social work data appear similar to those applicable in the health field sufficient differences exist to give rise to concern. Initially, it may be noted that the reference to access affecting the physical or mental health of the data subject cannot take account of any data held or supplied by a health professional, access to these being regulated under the Subject Access Modification

(Health) Order. The effect of this is that a determination will have to be made whether access to data other than medical data might be seriously detrimental to health. The order does not require that such decisions be made by a health professional, and, indeed, contains no provision relating to the level at, or procedures under, which a decision whether to grant or refuse a request for access is to be made. Although the procedures followed might subsequently be reviewed by the Registrar or the courts in the event that a data subject complains following an unsuccessful application for access, such a situation appears to place an unreasonable burden upon data subjects who may well be incapable of adequately asserting their rights. In addition to considerations of the impact of access upon the subject's health the social work exemption introduces the subject's "emotional condition" as a factor justifying a refusal of access. This appears an extremely nebulous concept and, although it is qualified by the use of the adjective "serious", would appear to confer extensive discretion upon the data user.

As is the case with access to health data, the provisions regarding access to social work data can be criticised on two grounds. First, it is submitted, the general principle that subject access is beneficial is too easily cast aside. Although every rule may have its exceptions, in these areas it appears at least possible

that the exceptions will become the rule. Again, the approach of the Data Protection Act demonstrates a blinkered view of the purpose and rationale of subject access. The Act assumes that if a copy of information cannot satisfactorily be transmitted to the subject in an impersonal manner, the only alternative is to remove the right of access. The procedure, it is submitted, through which access is obtained is a vital feature of access. The interests of the data subject, which are afforded priority in the Convention, would be best served by providing a virtually unqualified right to be informed what information is held but by prescribing access procedures designed to ensure that the subject is best able to come to terms with the content of the record. Save in cases where the individual is incapable by reason of mental illness or incapacity of managing his own affairs, a possibility previously discussed and provided for in the Act, the final decision whether to know the content of a record and to accept any risk involved must be one for the data subject. An example of such a procedure can be seen with the solution adopted with respect to the question of an adopted data subjects right of access to data which might indicate the identity of his natural parents. Here, the relevant provision of the Act states that:

> "The Secretary of State may by order exempt from the subject access provisions personal data consisting of information the disclosure

> of which is prohibited or restricted by or under any enactment if he considers that the prohibition or restriction ought to prevail over those provisions in the interest of the data subject or of any other individual."(126)

Although this provision is open to the criticism that it affords excessive discretion to the Secretary of State, it being noted in particular that the provisions of the Official Secrets Acts prohibit the unauthorised disclosure of any item of Government held information, the addition of the final phrase referring to the "interest of the data subject or of any other individual" would appear to ensure that consideration of governmental interests could not be a relevant factor. It was stated in Parliament that this power might be invoked in respect of the Adoption (Scotland) Act 1978.(127) This Act prescribes a procedure whereby adopted children can obtain details of their original birth certificate which would identify their natural parents.(128) Prior to receiving this information, however, the enquirer would be obliged to seek counselling. In the event, this result was attained with the making of the Data Protection (Miscellaneous Subject Access Exemptions) Order 1987 which provides that the access procedures under the Adoption (Scotland) Act 1978 are to prevail over those of the Data Protection Act.(129) Such an argument does not appear unreasonable although it does, perhaps

unconsciously, make a significant point concerning the role of the computer. The provisions of the Adoption (Scotland) Act apply regardless of the format in which the information is held. One of the major justifications put forward for the concept of data protection and, more negatively, for the restriction of the Act's ambit to the field of computerised information, is that special dangers and problems arise form the use of the computer. The above provision, envisaging the general law enjoying primacy over the specialised computer law, indicates that the involvement of the computer may sometimes be of peripheral significance with the data itself being the critical component.

f. Judicial Appointments

In England, it has been reported that the Lord Chancellor's Office maintains a computerised data base containing information on those members of the legal profession who might be candidates for appointment to judicial office.(130) Such data subjects will not be permitted access to the information, the Act providing that:

> "Personal data held by a government department are exempt from the subject access provisions if the data consist of information which has been received from a third party and is held as

information relevant to the making of judicial appointments."(131)

Thus, whilst a degree of access will be permitted to this under the general provisions of the legislation no access will be permitted to reports or references supplied by a third party. This exemption is wider than that applicable under the general restriction of access to information supplied by a third party, here access will be denied even if the third party is willing for access to be granted or if the information could be censored so as to conceal the identity of the source. There must be doubt as to whether such an exemption conforms with the provisions of the Convention, denial of access not being justifiable by reference to any of the relevant interests there specified.

g. Legal Privilege

Information divulged in the course of the lawyer - client relationship has always been afforded the highest degree of privilege by the courts. This protection could clearly be negated were another party, perhaps engaged in litigation with the client, to be allowed to exercise his access rights and obtain a copy of any information about himself which may have been passed on the the solicitor by the client or obtained on the client's behalf. The Act attempts to avoid such a result by providing that the access provisions are

not to apply where:

> "..the data consist of information in respect of which a claim to legal professional privilege (or, in Scotland, to confidentiality as between client and legal professional adviser) could be maintained in legal proceedings."(132)

The exemption under the Data Protection Act extends beyond the situation where legal proceedings are in train or even, it would appear, contemplated. In this eventuality the criteria adopted would appear to call for a degree of speculation, with the parties called upon to decide whether a claim to confidentiality would be upheld in the event that legal proceedings were to be instituted. It may further be queried whether this provision might be invoked by the lawyer against his own client. The situation might be envisaged where a lawyer had recorded comments concerning his client which he would not wish to reveal to the client. Assuming that confidentiality might be maintained in respect of this information vis a vis third parties the section appears to leave open the question whether a similar approach might be adopted against the client. Against this it might be argued that the notion of confidentiality exists for the benefit of the client and could not be extended to the situation where it was invoked for his lawyer's benefit. This view has been

adopted by the Registrar who has advised users to the effect that:

> "This exception is likely to apply where a lawyer has received information from a client about a third party and the lawyer later receives a subject access request from the third party. The privilege belongs to the client and not the lawyer. So, for example, a lawyer could not refuse to give subject access to his own client on the grounds that the information to be revealed is covered by legal professional privilege."(133)

Such a result would also be in conformity with the provisions of the Convention. In this situation, the lawyer will be regarded as the data user and, of course, the Convention does not admit of a denial of access where this is in the interests of the user. The wording of the statute may, however, be considered unfortunate in that it attempts to transplant the notion of confidentiality from its traditional role as an element within particular legal proceedings into a wider arena. This may, of course, be regarded as an inevitable consequence of the Data Protection Act granting unprecedented rights of access to personal data. A second point may also be raised resulting from the Registrar's comments. These would appear to indicate that the exception will apply only in favour

of information supplied by a client. Information relating to the client may also be supplied to the lawyer by a third party, for example, a medical report. Such information would appear to be covered under the heading of privileged information, particularly as the Act defines this in relation to Scotland.

h. Miscellaneous Exceptions

The subject access provisions will not apply in the situation where the data user is statutorily obliged to otherwise make the information available for public inspection, whether free of charge or upon payment of a fee.(134) This would be the situation, for example, with the electoral roll or with a public company's statutory accounts or, indeed, with the Data Protection Register. As such this provision does not appear to raise any significant issues. Similarly the provision that the subject access provisions are not to apply in relation to data which is stored merely as a back up to other data to which the subject access provisions will apply.(135)

Finally, in considering the exemptions from the subject access provisions, consideration must be given to the position of those credit reference agencies who maintain their records upon computer. The Data Protection Act provides that such agencies will be exempted from its access provisions being required to

comply with those operating under the Consumer Credit Act.(136) There can be little quibble with such an approach which offers considerable advantage to the individual as access under the latter statute is quicker and cheaper than that applying under the Data Protection Act. It does, however, appear somewhat anomalous that two different regimes should apply in relation to data banks and it might be considered that an argument exists for considering whether the substantive provisions of the two statutes could be merged with all data banks placed under the same supervisory authority regardless of their purpose. In practice this would appear to require that responsibility for at least the day to day running of credit reference agencies should be transferred from the Director General to the Registrar.

7. The Value of Subject Access

Subject access has come to be regarded as one of the corner stones of data protection legislation. It may be doubted, however, whether its role in protecting individuals vis a vis the possibly adverse consequences of data processing activities justifies such a position of prominence. Although the holding of excessive or irrelevant items of data by a data user may justify the Registrar in serving an enforcement notice the data subject possesses no direct measure of control over the inclusion of accurate data. Whilst, in individual

cases, harm may be caused through reliance upon inaccurate data the critical danger identified as resulting from computerisation is that accurate data obtained or supplied for one purpose will be used for another. The dangers are of linkage and the accumulation of vast amounts of data, each item being perhaps innocuous in itself but combining to produce a detailed profile of the individual's personality. Subject access can do little to mitigate against these dangers. In these terms subject access may be considered a placebo, of little relevance to the main issues. The grant of subject access will give an indication as to the current state of a record but affords no guidance as to previous records or assurance as to future practices. Subject access provides, essentially, a snap shot view of data practices with little guidance as to the context in which this should be considered. To some extent this may be provided by the terms of the user's entry on the Data Protection Register but these tend to be phrased in general terms. For the continuing and long term protection of the interests of all data users, it is submitted, the active involvement of a public supervisory agency. Compared to this subject access is of secondary importance.

Although the importance of subject access should not be overstated, neither should its value be dismissed. This value lies in the belief that in order to play a full

role in an "information society", the individual's ability to access and to control information must be maximised. Whilst it will be argued that this should not be restricted to the situation where personal data is held, the Data Protection Act creates a valuable breach in the walls of informational secrecy. Less happy, however, is the manner in which this advance is accomplished. Whilst few would dispute the need for some exemptions from subject access, the provisions of the Data Protection Act, taken together with those relating to the procedures under which access may be sought, demonstrate a grudging attitude towards the concept which does much to dilute the welcome which would otherwise be given to the legislation. Time alone will reveal the extent to which the grant of access to police and tax records will constitute the exception or the rule. Equally significant, in the case of access to health or social work data the approach adopted would appear to indicate either an excessive degree of paternalism on the part of the Government or a desire to inhibit, so far as possible without falling foul of the Convention, the demand for access. Where recourse is had to the notion of protecting the data subject, whilst it may be a user's wish, or even duty, to counsel and warn as to the consequences of access the final decision, it is submitted, whether to pursue such a request must be, save in the most exceptional circumstances, one for the individual.

One final point may be mentioned in connection with the exercise of the subject's right of access. Whilst this is intended to benefit the individual, the suspicion has been voiced that the existence of the facility may operate to his detriment with a third party requiring that the subject exercise his right of access, obtain a copy - perhaps a list of criminal convictions - and supply this to him as a pre-requisite to being considered for some benefit. A similar scenario could be devised in relation to the exemption to the non-disclosure principle permitting disclosures to be made to a third party with the data subject's consent. As there would appear nothing in the Act to prevent these situations arising and as it would appear difficult to formulate any effective prohibition there may be the danger that subject access may serve to imprison rather than to benefit individuals.

8. Remedies

a. Rectification

The act of obtaining access to information may constitute only the first step for an individual in attempting to fully exercise his rights in respect of the data held or of the uses to which it is put. These rights and remedies may exist either under the Data Protection Act or the provisions of the general law. Initially, consideration will be given to the situation

in which the individual has become aware of the content of data held but disputes its veracity. In this respect the Convention requires that national legislative provisions enable the data subject:

> ".. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention
>
> .. to have a remedy if a request for .. rectification or erasure .. is not complied with."(137)

The nature and extent of these rights and remedies is a matter for national legislatures. Under the Data Protection Act, in the event that an amicable solution cannot be reached between the data subject and the data user two procedures are made available to the data subject. These involve recourse either to the Registrar or to the courts. Prior, however, to considering the procedures established under the Data Protection Act it may be valuable to consider the extent and operation of the corrective procedures applying under the Consumer Credit Act in respect of information held by credit reference agencies, the provision of this Act once again serving both as a precedent and as a basis for

comparison with the provisions of the Data Protection Act.

Under the terms of the Consumer Credit Act, an individual is entitled to challenge the inclusion of any information on the basis that it is "incorrect". The interpretation of the word "incorrect" is obviously critical in this context. Although the Act essays no direct definition it would appear that this must be determined both by reference to the factual accuracy of particular items of data and to the overall tenor of the record. The omission of relevant information may serve to render the record incorrect even though those items recorded may be correct. The fact that information, although accurate, has no direct connection with the individual's credit worthiness, for example, details of criminal convictions for assault, would not appear sufficient to found direct action by the individual concerned. It would be open to him, however, to make a complaint to the Director alleging that the form of record keeping maintained by the agency indicated that it should not be considered fit to hold a licence under the Act.(138)

In the event that the subject wishes to challenge the record he must serve written notice upon the agency requiring them either to remove the entry from the file or to amend the record. They must respond within 28 days, informing the consumer either that they have

complied with his wishes, that they are willing to amend the record in some other way or that they consider that no case has been made for any alteration of the record. If the agency offers to amend the record a copy of the amended information must be supplied.(139)

If the contested information is removed this will be the end of the matter. If any other response is received the subject is entitled, within 28 days, to serve a "notice of correction" on the agency. This notice will consist of a statement, not exceeding 200 words, drawn up by the subject and which is to be inserted in his record. A copy of the notice of correction will thereafter have to be supplied whenever information included in or based on the contested entry is supplied to a third party.(140) Once again, the agency has 28 days within which to consider their position. If they do not respond within this period the subject may refer the matter to the Director. If the agency do not wish to include the notice of correction to the record they may only refuse so to do on the grounds that it is:

> "..incorrect, or unjustly defames any person, or is frivolous or scandalous, or is for any other reason unsuitable."(141)

Up to this stage questions as the the accuracy or

otherwise of information or as to the acceptability of any notice of correction submitted fall to be decided by the parties themselves. In the event that the agency are unwilling to accept the subject's notice of correction, either party may refer the matter to the Director who will act as an arbiter.(142) No fee is charged for this service and the Director is empowered to make any order concerning the record that he may think fit. It would appear that in making such a determination the Director is acting in an administrative rather than in a quasi-judicial capacity. His decision is, therefore, not susceptible of judicial review.

Two comments appear apposite concerning the provisions for the correction of inaccurate information. It would appear that, even if the subject should consider that information has no basis whatsoever in fact, he has no direct right to insist on its removal. His only entitlement under the Act is to serve a notice of correction. In the event that this totally contradicts the stored information - as opposed to placing it in its proper context - it may be felt that the subject's credit worthiness may still be damaged in that a potential creditor who receives the consumer's notice of correction together with the agency's conflicting information, may consider it financially prudent to accept the latter's version. It will only be if the agency refuse to accept the proferred notice of

correction that the subject will be appeal to require the Director to make a determination, although a failure on the agency's part to remove information that is clearly demonstrated to be untrue might again allow the individual to complain to the Director on the issue whether the agency is fit to hold a licence under the legislation.(143) Secondly, the Consumer Credit Act does not confer any legal rights upon consumers. A contention that a record is incorrect can only be pursued through the above procedures described and cannot directly be invoked in the course of legal proceedings before the courts.

The amendment of, or removal of information from, a credit record does not extinguish the agency's responsibilities under the Act. If any change has been made to the record details of this must be transmitted to every person who has received information from the record within the 6 month period subsequent to the date on which the agency received a request from the subject to be supplied with a copy of his record and where the details supplied have either included or been based upon the amended information.(144) Such a provision may go some way towards repairing any harm suffered by an individual where the incorrect information has been supplied to and acted upon by a third party. Although the practical utility of this provision may be limited - in the event that the information is passed to a creditor who thereupon refuses to extend credit

facilities to the subject the passage of time may have obviated the need for credit or this may have been obtained from another source - the principle that data users who supply inaccurate information should be obliged to take steps to minimise the damage that may be caused through their actions is one which must be commended.

Consideration of the extent of the Consumer Credit Act's corrective procedures serves to define the parameters of this topic. Four issues arise, first, the extent of the right to challenge information, second, the procedures under which this may be accomplished, third, the role of the supervisory agency and, finally, the extent of any remedies which may be available.

The corrective procedures established under the Data Protection Act become operative in the event that data is considered to be "inaccurate". Data will be so considered if it is:

> " incorrect or misleading as to any matter of fact."(145)

This definition is somewhat wider than that found in the Consumer Credit Act. The inclusion of the word "misleading" extends the range of situations in which data may be challenged and would be applicable in the situation where a record contains a selective

presentation of the facts of a case. Also, the subject will be permitted to challenge the inclusion of any statements of opinion which appear to be based upon inaccurate data.

Faced with a record which is considered inaccurate and with a data user who refuses to make any amendments to it, a data subject has two options. The holding of inaccurate data is a violation of the fifth data protection principle and may form the basis for action by the Registrar. It is, therefore, open to an agrieved data subject to make a complaint to the Registrar who, assuming that he considers that the complaint satisfies the statutory criteria, is obliged to investigate.(146) In the event that this confirms the subject's allegations, the Registrar may serve an enforcement notice. Insofar as the inaccurate data was generated by the user himself or contains no indication as to its source, the notice will require that the contested data be rectified or erased. The position is more complex in the situation where the contested data was supplied by a third party and where:

> "the data indicate that the information was received or obtained as aforesaid or the information has not been extracted from the data except in a form which includes an indication to that effect."(147)

In such a case it is provided that as an alternative to serving an enforcement notice requiring rectification or erasure the Registrar may require that the data be supplemented:

> ".. with such statement of the true facts relating to the matters dealt with by the data as the Registrar may approve."(148)

This power appears somewhat analogous to the procedures under the Consumer Credit Act where a dissatisfied consumer is entitled to compose and submit a notice of correction to the credit reference agency. A significant distinction would appear to lie in the fact that here the Registrar will be responsible for the form of the corrective notice. It would appear open to him to approve an unequivocal statement that the content of a report in the record is false; although in such a case it would appear preferable to order the rectification or erasure of the data in question.

If comparison is made with the provisions of the Consumer Credit Act it is apparent that under the earlier statute a formalised structure is established under which the Director General of Fair Trading is given sole responsibility for arbitrating in the event a dispute between a credit reference agency and a consumer cannot be amicably resolved between the parties. Such procedures create an informal and

inexpensive means for a data subject to obtain an independent resolution of a dispute. Although the Registrar has the power to provide a similar facility the lack of procedures and the extent of his discretion whether to pursue a complaint may inhibit the utility of such an approach.

In cases where an individual seeks rectification or erasure of data there may well be dispute between him and the user concerning the accuracy of the contested information. Here the act is silent as to where the onus of proof will lie. This situation is to be contrasted with that arising under the French legislation where it is explicitly provided that:

> "In the event of dispute, the onus of proof shall be on the department in relation to which the right of access is exercised, unless it appears that the disputed data were disclosed by or with the consent of the person concerned."(149)

In the United Kingdom it would appear that, in line with the normal rules applicable to civil proceedings, the onus of proof would lie with the data subject whilst, should the Registrar serve an enforcement notice, he will require to justify his action in the event that the data user brings an appeal before the Tribunal.(150) Although it would be anomalous for the

normal burden of proof imposed upon the Registrar to be reversed in this particular situation a different conclusion might be reached in the case where the individual brings proceedings before the courts. As the user is, presumably, intending to obtain some benefit from the possession of personal data it would not appear unreasonable that he be required to justify his actions.

The act of correcting or removing inaccuracies from a record may serve to protect the individual from future detrimental action initiated by the particular data user but will provide no protection in the event that the data has been passed on to a third party. A requirement that the data user maintain an audit trail detailing the identities of those third parties to whom the data in question may have been disclosed constitutes a major feature of several continental systems. Thus, in France it is provided that:

> "If an item of data has been sent to a third party, its correction or deletion must be notified to such party unless the Commission waives such a proceeding."(151)

In theory, the requirement to inform appears open ended here. in other jurisdictions the requirement to supply notification of corrections only subsists for a specified period of time. Thus, in Denmark, notice of

correction may be required to be transmitted to any third party who has received the data in question within the previous six months.(152)

Several attempts were made in Parliament to introduce an audit requirement into the Act's provisions, it being suggested, for example, that where the Registrar had ordered amendment of data:

> ".. the data user shall furnish the Registrar, upon his request and within a reasonable time, with any information about the source of that personal data and the persons to whom the data has been disclosed."(153)

Similar provisions were proposed for the situation where data were amended in compliance with a court order. In rejecting this argument stress was placed by the Government on the potentially unlimited extent of such a requirement, the Minister of State commenting that:

> "Every single data user would have to develop some sort of logging system, because no user could be certain that he could never come to the Registrar's attention and be ordered to rectify or erase data. Every user would therefore have to record the source of every item of data that he possessed, as well as

> maintaining a record of every disclosure. Both records would need to be maintained indefinitely because he would never know when the registrar might come knocking on his door."(154)

Although the amendments would have left the decision whether to require details of sources and disclosures to the Registrar it was argued that:

> "The user would have no choice but to operate on a worst case basis and to put himself in a position to provide the information against the possibility that he would be required to do so."(155)

Whilst this argument is not without merit in the context of the particular amendments proposed, it may be doubted whether the difficulties referred to are insurmountable. As has been stated, it has proved possible to introduce a logging requirement in several continental countries and it may be doubted whether the technology used by British data users is inherently incapable of performing such a function. In debate in Parliament it was suggested that:

> "Anyone with even a modest knowledge of computer programming knows that nothing more than a Mickey Mouse programme would be required

to index sources and recipients."(156)

Some support for this view would appear to come from the report of the Lindop Committee. This recounted conflicting views as to the extra cost of a logging system and drew a distinction between the various forms that this might take.(157) Whilst accepting that imposing a requirement to log all occasions when access might be obtained to a record would constitute a substantial burden, a requirement to record disclosures to third parties would not be unduly onerous. Inevitably, however, this recommendation has to be considered in relation to the basic thesis that;

> ".. if high costs look likely, there is either a serious deficiency in the current practices of the organisation in question, or the specification of privacy regulations to which it is to conform is inappropriate and could be improved."(158)

Put simply, no single regime can be appropriate to regulate all data users.

It may further be recalled that under the terms of the Consumer Credit (Credit Reference Agency) Regulations,(159) where a record is amended following representations from the consumer, details of the correction have to be transmitted to all third parties

who have received the relevant details within the previous six month period. Whilst recognising the distinction between the sectoral coverage of the consumer credit legislation and the broad spectrum of activities regulated under the Data Protection Act it is submitted that it would normally be reasonable to impose a similar fixed term logging requirement upon data users coupled with an obligation to notify third parties of any change which may have been made to the record. Although situations might be identified in which such an obligation would impose unreasonable burdens, for example, in the case of a computerised legal retrieval service where the operators may not be aware of the exact data accessed by a customer, such exceptions should be narrowly and precisely defined.

b. Compensation

As an alternative to bringing a complaint before the Registrar, the data subject may institute legal proceedings against the user seeking rectification or erasure of any inaccurate data. The grounds upon which a court may make such an order are similar to those available to the Registrar and it may be considered that, save in the event that the Registrar refuses to take action against a data user, few data subjects will institute legal proceedings purely with a view to seeking rectification or erasure of inaccurate data. It must be more likely that any challenge before the court

will be linked to a demand from the individual for compensation caused as a result of the user's holding inaccurate data. At this stage two actions would appear to be open to the data subject, first he may base his claim upon the provisions of the Data Protection Act and, second, he may pursue his action under the law of defamation. Under the Act it is provided that:

> "An individual who is the subject of personal data held by a data user and who suffers damage by reason of the inaccuracy of the data shall be entitled to compensation from the data user for that damage and for any distress which the individual has suffered by reason of the inaccuracy."(160)

Liability under this heading is not strict; it being further provided that:

> "In proceedings brought against any person by virtue of this section it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time."(161)

Additionally, it is provided that no liability will arise where inaccurate data has been received from a third party and is marked as having been so received.

In justifying this provision, the Minister of State commented that:

> "Where a data user records inaccurate information supplied by someone else, the data are accurate. They are an accurate record of what someone else said."(162)

Such a statement appears tinged with unreality. The consequences of inaccuracy for the data subject would appear to be unconnected with the fact whether the data was internally generated or was supplied by a third party. As defined in the Act, a data user is the person who controls data. The approach adopted ensures, albeit to a limited extent, that the user enjoys power without responsibility.

A further consequence of the Act's definitions is the requirement that the data subject demonstrate some degree of financial loss as a prerequisite to any claim. If this can be demonstrated then an additional element may be included in any award of damages made by the court in respect of the distress which the presence of inaccuracy has caused, but no claim will lie in respect of distress unaccompanied by financial loss. By way of contrast it may be noted that the Registrar is instructed, when contemplating serving an enforcement or a de-registration notice, to consider whether the alleged contravention:

> ".. has caused or is likely to cause any person damage or distress."(163)

Under the Act the entitlement to compensation is not dependent upon whether the data in question have been passed on to a third party but even without such a restriction it is difficult to conceive of circumstances under which financial loss might be demonstrated. It may be, for example, that an employee could claim that he was passed over for promotion because of inaccurate information held on his personnel record. Unless he could demonstrate, however, that he would have been promoted but for the inaccuracy his claim will relate merely to a lost opportunity, a circumstance which the law does not recognise as constituting a basis for compensation. By contrast, it may be noted that under the provisions of the United States Privacy Act of 1974 an action will lie at the suit of any Federal employee in the event that his employer:

> ".. fails to maintain any record concerning any individual with such accuracy, relevance, timeliness and completeness as is necessary to ensure fairness in any determination relating to the qualifications, character, rights or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which

is adverse to the individual.."(164)

Such an approach would appear to be eminently justified in an era where decisions concerning an individual are increasingly made on the basis of written records. In these circumstances the fact that an individual has been denied a benefit or an opportunity coupled with the presence of inaccurate data, should suffice to establish at least a prima facie claim for compensation.

Similar considerations must apply in the situation where inaccurate data is passed to a third party. In this case it is easy to envisage circumstances under which the data subject will be distressed by the transfer but, again, occasions where he suffers recognised financial loss will be far fewer.

The requirement that quantifiable loss be suffered as a pre-requisite to a claim for damages constitutes a major tenet of English and, albeit to a lesser extent, Scots law. This rule is subject in both jurisdictions to a major exception under the provisions of the law of defamation. In the event of a successful action being brought under this heading an aggrieved pursuer will be entitled to compensation for the injury to his feelings resulting from the defender's conduct. The provisions of the Data Protection Act in no way affect the existing rights and remedies under this heading of the

law.

The effects of the non-availability of compensation under the Act in respect of distress resulting from the holding or dissemination of inaccurate information may be mitigated by the possibility that an aggrieved subject might institute proceedings for defamation against the data user or, in the event that the contested information was supplied by a third party, against its source. Detailed consideration of the action for defamation is outside the scope of this thesis. A data subject, however, who contemplates such a course of action may encounter several obstacles. In order for an action to lie in defamation several conditions have to be satisfied. Initially, the remarks complained of must be defamatory. Not every false statement will be so regarded. A statement will only be considered defamatory if it is likely to lower the pursuers standing in the minds of right thinking members of society. An inaccurate statement on a medical record to the effect that the data subject suffers from cancer may cause him distress and may lead, if communicated to a prospective employer, to the loss of a job opportunity but could not be considered defamatory. In contrast, a false statement as to the subject's qualifications - assuming that he was portrayed in an unfavourable light - would appear to be defamatory.

A second prerequisite to an action in defamation is that the statement be communicated. This raises the possibility that two parties may be liable in respect of defamatory statements. If the information is supplied to the data user by a third party and not further disseminated until disclosed to the subject then the third party will be liable. The aggrieved subject may, of course, experience considerable difficulty in discovering the identity of the source of the data, although this information may, on occasion be obtained in the course of legal proceedings. In other cases where the data is generated by the user himself, the liability will be his. In this situation it may be that the data is held by the user for his own purposes with no intention of communicating it to a third party. At this stage, the element of communication necessary for liability to arise will not be present. Should the data subject make a request for access to the data, however, the user will normally be obliged to comply and to communicate the data to the subject. In this respect it would appear that, for the data user, one of the costs of complying with the statutory requirements of access may be that he will incriminate himself in the event that the subject institutes proceedings for defamation. In such an event, however, it would appear that only a minimal amount of compensation would be appropriate.

Even if data is considered to be defamatory and the

necessary element of communication can be identified an action for defamation may be met with the defence of qualified privilege. If established, the effect of this is to confer immunity upon the defender in respect of defamatory statements except where his actions are motivated by malice. In order to establish the applicability of this defence the defender will be required to establish that the statement was made in the course of some public duty. Thus it has been commented that qualified privilege applies where a communication is:

> ".. fairly made by a person in the discharge of some public or private duty, whether legal or moral, or in the conduct of his own affairs, in matters where his interest is concerned .. If fairly warranted by any reasonable occasion or exigency, and honestly made, such communications are protected for the common convenience and welfare of society .. "(165)

The range of duties covered by this defence is not susceptible of precise definition. In the case of MacIntosh v. Dun(166) the Privy Council held that the activities of a commercial credit reference agency should not qualify for the protection of the defence of qualified privilege. After accepting the primacy of considerations as to the public interest the Privy Council drew a partial distinction between statements

which are volunteered and statements which are made in response to an enquiry, commenting that:

> ".. in cases which are near the line and in cases which may give rise to a difference of opinion, the circumstance that the information is to be volunteered is an element for consideration certainly not without some importance."(167)

In the present case, although the communication at issue was made in response to an enquiry from a subscriber the defendant's conduct in holding themselves out as being willing, at a price,to respond to such requests placed them in the category of volunteering information. Accepting that the defendant's motive for acting was one of profit the Court turned to what was considered:

> ".. the real question: Is it in the interest of the community, is it for the welfare of society, that the protection which the law throws around communications made in legitimate self-defence, or from a bona fide sense of duty, should be extended to communications made from motives of self-interest by persons who trade for profit in the characters of other people?"(168)

The Privy Council were clearly of the opinion that this question should be answered in the negative and that the defence of qualified privilege should not be afforded to the particular defendants.

The case of MacIntosh v. Dun is clear authority for the proposition that a financial motive may well vitiate any claim that a disclosure is made in the public interest. The case was, however, distinguished in the later decision of the House of Lords in London Association for Protection of Trade v. Greenland (169) The decision of the House of Lords marked the end of a chaotic course of litigation stigmatised by the Lord Chancellor as presenting an "unedifying spectacle". As in MacIntosh v. Dun the case centred on admittedly defamatory comments in a credit report communicated by an official of a trade protection society to one of its clients and the extent to which this communication might benefit from qualified privilege.

After considering a variety of definitions concerned with the nature and extent of qualified privilege and accepting that considerations of the public interest were predominant in this area, Lord Buckmaster stated that no exhaustive list could be devised of the circumstances under which qualified privilege would attach to communications:

"Indeed, the circumstances that constitute a

> privileged occasion can themselves never be catalogued and rendered exact. New arrangements of business, even new habits of life, may create unexpected combinations of circumstances which, although they differ from well-known instances of privileged occasion, may none the less fall within the plain yet flexible language of the definition to which I have referred."(170)

Distinguishing MacIntosh v. Dun on the basis on the lack of any profit motive on the part of the present appellants, who as an unincorporated association were not legally permitted to trade for profit, it was unanimously held that the communication was privileged, the association was regarded as constituting an extension of its members' own personalities. In these circumstances, it was considered, an individual trader would be entitled to make enquiries as to the financial circumstances of a person with whom he proposed to deal. It was ,however, stated by Earl Loreburn in what he described as a "doubting" rather than a dissenting judgment that:

> ".. I cannot think that privilege should be allowed unless there is not merely good faith but also real care to make enquiry only in reliable quarters, and to verify it where possible. The absence of such care may, no

> doubt, be evidence of malice, but it is also relevant on the point whether there is privilege or not and may, in my judgment, be fatal to the privilege even if malice is disproved."(171)

It would appear that this is where the matter rests at the moment. In respect of the activities of credit reference agencies, the Younger Committee recommended that, in return for their being required to grant subject access, the defence of qualified privilege should be extended regardless of whether an agency operated on a profit or a non-profit making basis.(172) As initially introduced into Parliament, the Consumer Credit Bill proposed to give effect to this recommendation providing that:

> "Qualified privilege applies to the publication of any defamatory material referring to the financial standing of an individual -
>
> (a) where the matter is published to a licensed credit reference agency for the purpose of its business; or
>
> (b) where the information is published by such an agency in the course of its business."(173)

This proposal was subjected to considerable criticism, it being argued in particular that qualified privilege had hitherto attached to particular communications with the status of the transmitter or recipient being of secondary importance. The proposed formulation would, it was argued, remove the requirement that the agency, or any person transmitting information to them, should act in the course of a duty.(174) This view was accepted by the Government and, as enacted, the Consumer Credit Act makes no reference to the availability of the defence of qualified privilege.

In 1975 the White Paper, Computers and Privacy,(175) announcing the appointment of the Lindop Committee indicated that the committee should consider the question whether:

> ".. computer users (and perhaps their informants) (should) be entitled to the defence of qualified privilege in defamation proceedings at the suit of a person who has been given access to information held about him?"(176)

In their report the Lindop Committee were unequivocally of the view that no special treatment should be offered to computer users in respect of liability for defamation, concluding that:

> "All information systems holding personal information about people should be operated with care and a proper regard for the interests of the people concerned. This is no less so - and may be more so - in the case of information systems which include computers. Those who use such systems must ultimately be responsible for the risks that they create, and be ready to compensate those whom they may damage if they do not attend to those risks with sufficient care."(177)

Such a conclusion is to be readily supported. The extent of the data users liability in defamation remains less clear cut however. Attempting to synthesize existing authorities on this point a variety of situations can be identified and propositions tentatively proposed. First, in the situation where information is held by the user for his own purposes with no intention that it be communicated to any third party but where this information is required to be disclosed to the subject under the access provisions. Here it seems clear that the defence of qualified privilege will apply; subject to the requirement that the data truly be held for business purposes.

More complex problems arise when the data is transferred to a third party (similar considerations will apply in the event that a third party source whose

disclosures are discovered by the subject is the target for defamation proceedings). Perhaps the major consideration in this case is whether the party initiating the communication did so with a view to profit. In this situation MacIntosh v. Dun supports the proposition that qualified privilege will not attach to the communication. The status of this decision may be open to question. In respect of the operations of credit reference agencies, the Younger Committee based their recommendations on the premise that it remained good law, a view that was repeated in the House of Commons with the Minister of State commenting that:

> "Where a credit reference agency is now operating on a non-profitmaking basis it enjoys a qualified privilege. When a company is operating on a profit-making business, it does not enjoy qualified privilege."(178)

However, it may be argued that the judgments in London Association for the Protection of Trade v. Greenlands regarded the existence of a profit motive as an evidentiary rather than a conclusory matter. Adopting this view, Scrutton LJ sitting in the Court of Appeal in the case of Watt v. Longsdon(179) remarked:

> "If MacIntosh v. Dun is rightly decided the duty to communicate does not arise where the communication is made in pursuance of a

> contract made for the private gain of the speaker. But after the decision of the House of Lords in London Association for the Protection of Trade v. Greenlands Ltd., MacIntosh v. Dun must not be relied on too strongly."(180)

Regardless of the precise weight to be afforded to it, the presence of a financial motive must be an important consideration in determining whether privilege will apply. It may of course be more difficult to assess this matter in relation to the generality of activities covered by the Data Protection Act than in the limited field of the supply of credit reports. It may well be that the data user will be engaged in business with a view to profit but unless the sale of data is a component of that business it may not be the case that a particular communication was made with a view to profit. An example might of the latter situation might involve an employer communicating the contents of a computerised personnel record describing an ex-employee as an agitator to other employers in the same line of business. In this case it seem clear that the defence of qualified privilege would be available and, therefore, that considerations of profit must attach to the particular transaction rather than to the data user's business as a whole.

In the event that no profit motive exists then the determination whether qualified privilege exists will

fall to be determined on the traditional lines whether the disclosure is justified by recourse to considerations of public duty or private or public interest. Detailed consideration of the extent of these concepts is outside the scope of this work. It is submitted, however, that the existence of the Data Protection Principles and the Data Protection Register must be a factor to be taken into account. Although the fact that a user has nominated particular categories of recipients for data held by him cannot affect a determination whether qualified privilege arises, in the event of an unauthorised disclosure which does not come within the scope of any of the Act's exemptions this may be considered a relevant factor in determining questions of public interest and duty.

Regardless of the legal issues involved in an action for defamation, one practical point may serve to substantially limit its utility. Whilst legal aid may be available to an individual who wishes to pursue an action for compensation under the Data Protection Act, this facility is not available to anyone contemplating an action for defamation. In view of the notoriously high costs involved in the latter form of proceedings it may be considered doubtful whether many data subjects would be in a position to seek compensation on this basis.

Wrongful Disclosure of Data

In addition to requiring that data be accurate the data protection principles also require that the user specify the circumstances under which he will disclose information to third parties and that he maintain the data in circumstances of reasonable security. Any breach of these requirements may, as has been discussed, result in the service of an enforcement notice. Additionally, it is provided that an affected data subject may be able to bring a claim for compensation. In this respect the Act provides that:

> "An individual who is the subject of personal data held by a data user or in respect of which services are provided by a person carrying on a computer bureau and who suffers damage by reason of -
>
> (a) the loss of the data;
>
> (b) the destruction of the data without the authority of the data user or, as the case may be, of the person carrying on the bureau; or
>
> (c) .. the disclosure of the data, or access having been obtained to the data, without such authority as aforesaid.
>
> shall be entitled to compensation from the data user or, as the case may be, the person

> carrying on the bureau for that damage and for any distress which the individual has suffered by reason of the loss, destruction, disclosure or access."(181)

Once again it is to be noted that a degree of financial damage is a prerequisite to a claim under this heading. An individual who is distressed when, for example, a print out of his medical record is discovered on a rubbish tip will have no claim under the Act.

The above provision provides for compensation in a variety of circumstances; the loss or destruction of data, the fact of its disclosure to a third party or that a third party has obtained access to the data. It is only in the first of these circumstances that the connivance of the data user himself does not serve as a bar to civil liability.

It would appear that a considerable degree of overlap might exist between the situations where data is lost and where it is destroyed. It may be argued that the destruction of data inevitably results in its loss. By contrast, however, the fact that the data user no longer knows where the data is located does not mean that it has ceased to exist. In similar vein, there is a degree of overlap between the disclosing of data and the obtaining of access to it, the distinction perhaps lying in the fact that disclosure requires the

connivance of the data user or of his employees whereas access might be unauthorised. This latter possibility concerns the activities of computer hackers who seek to obtain access, normally by means of telephonic communications, with a data base with a view to inspecting the information contained therein. As has been previously discussed, a user whose data is accessed in this fashion may be regarded as being in breach of the eighth data protection principle requiring the maintenance of "appropriate security precautions"(182).

Although the Act refers to compensation being paid where loss is suffered because of disclosure of data it is further provided that no entitlement will arise where the disclosure is to a party coming within a category described in the user's register entry. Again, no compensation will be payable in the event that the disclosure is sanctioned by one of the exemptions to the non-disclosure principle although where the disclosure is made by a person other that the data user in the mistaken belief that it is sanctioned under an exemption the user may be held liable unless he can establish the statutory defence. In this situation it might be reasonable to require that a user demonstrate the existence of a system designed to ensure that proper consideration is given to any request for disclosure made on the basis of an exemption.

In the event that the data is lost, the user will be obliged to compensate a data subject who has suffered damage as a result. An example might be provided in the case of data services which offer, for a price, to store details of subscriber's credit card arrangements and insurance policy numbers. In the event that this data is lost and, for example, a credit card is abused or insurance policy surrendered it would appear that an action would arise under this heading. Liability is not, however, absolute; the Act providing that in respect of any action for compensation brought under this section that:

> ".. it shall be a defence to prove that he had taken such care as in all the circumstances was reasonably required to prevent the loss, destruction, disclosure or access in question."(183)

In respect of the remaining heads of liability it is provided that this will only arise when the act or omission occurs without the authority of the data user. This produces the seemingly absurd result that if the user orders that data be destroyed or that a disclosure be made outside the scope of those permitted in his register entry, far from this being regarded as an aggravating circumstance, it will serve as a total defence to the subject's suit. In this situation, the subject's only remaining option would be to consider

the possibility of an action in delict or for breach of contract. It may also be the case that the user will incur the wrath of the Registrar, in the form, perhaps, of an enforcement notice but this may be of small consolation to a subject who has suffered financial loss.

In the situation where the data is either wrongfully disclosed to a third party or that party is allowed to obtain access to the data the Act provides for a further action to be made available to the data subject. In the event that he has suffered damage which would entitle him to compensation under the above provision and is able to satisfy the court:

> "..that there is a substantial risk of further disclosure of or access to the data .. the court may order the erasure of the data."(184)

It is only in this extreme situation that the Act provides a solution matching the expressed fears of the consequences of data processing. The individual is, in effect, permitted to argue that the fact that personal data is held causes concern and acts as an inhibiting factor upon his quality of life. The underlying logic behind the Act's provision appears strange. The individual has been harmed and, therefore, is entitled to anticipate future harm. Until actual harm is caused,

however, the individual is, under the terms of the Act, not entitled to anticipate it and any concerns which the holding of information may cause him are, effectively, to be dismissed as a figment of the imagination. The stable door shuts to the echo of the departing horse. Even in the event that an individual can establish that personal data has been used in violation of the Act's provisions, he will still be required to establish that the action has caused him "damage". Whilst it may be argued that this requirement is justified where the data subject is seeking compensation there appears no valid reason why it should also apply where he is seeking erasure of the data due to the data users previous malpractices. In such a situation a lessening of the criteria, with the subject merely being required to demonstrate distress, would appear appropriate.

Finally, in considering the remedies that may be available to an aggrieved data subject, brief mention must be made of the possibility that the data user may be considered to have violated an obligation of confidence owed to the data subject. The doctrine of breach of confidence is an ill defined aspect of Scots law (its application in English law being little more certain)(185). The obligation can arise either under an express contractual provision or by implication from the nature of the contractual or quasi-contractual relationship between the parties. The extent of the

obligation will vary from case to case. In general terms a party receiving information is obliged to act in respect of that information in a manner compatible with the legitimate expectations of the supplying party. The classical example of an obligation of confidence arises in the doctor-patient relationship. Here, information is supplied by the patient on the understanding that it will be used only for health care purposes. This illustration also serves to illustrate the evolving nature of the obligation of confidence. In reference to the doctor patient relationship, it has been commented that:

> "Had Hippocrates been faced with an extensive organisation within his profession he might have adopted a different phraseology. it is no longer practicable to look upon the single physician as the patient's sole confidant in any serious illness, and it is assumed.. that any contact with the complex medical machinery of today implies acquiescence in some degree of extended confidence."(186)

The existence of an obligation of confidence will assume especial importance in the situation where information is disclosed to, or access to it is obtained by, a third party. The fact that a disclosure comes within a category specified in the user's Register entry will not prevail over an obligation of

confidence, although it may be evidence against the existence of such an obligation. Again, the fact that the making of a disclosure is sanctioned under one of the exceptions to the non-disclosure principle, will not confer any degree of immunity upon the data user. It is, however, recognised, that in certain circumstances, the public interest in disclosure might override the private interest in confidence and, for example, the disclosure of medical information in connection with the investigation of a serious crime might not serve to found an action for breach of confidence.

It may be doubted whether individual remedies, whether created under the legislation or existing under the provisions of the general law, will have more than an ancilliary role to play in the battle between individual liberties and modern data processing capabilities. Given the nature of the remedies this would appear inevitable. From the beginnings of the debate concerning the role of the computer in modern informational practices the point has been made, time and again, that concrete evidence of abuse is lacking. The perceived dangers and the potential threat to individual liberties are so substantial, however, that far from diminishing the need for legislative action this finding has prompted the introduction of preventative measures. Whilst individuals must always assume at least a measure of responsibility for their

own affairs; and whilst an individual who has suffered loss through some isolated example of abuse or error should be compensated for any consequential loss, the prime danger is of the calculated and widespread use of computer power to interfere in the lives of large numbers of individuals. The task of preventing such generalised abuse can only be fulfilled by a specialised supervisory agency. An analogy may perhaps be drawn with the prevention and detection of crime. The task is one for society; everyone, it may be argued, has at lest a moral responsibility to facilitate its attainment, the law recognises the right of any citizen witnessing criminal conduct to make a "citizens arrest" and the victim of crime may well have a claim to be compensated for any loss suffered. Despite all these factors, few would seriously suggest that responsibility for the prevention and detection of crime could be left to the individual members of society, rather, police forces are established as specialised regulatory agencies. In the same way, direct responsibility for the enforcement of the data protection principles must rest with the Registrar and any individual rights and remedies conferred under the statute must be seen as ancilliary to this task.

Footnotes

1. Art.8.

2. Sch.1 (7th Data Protection Principle).

3. See; Marsh (Ed.), Public Access to Government Held Information. Stevens, 1987. P.35 et seq.

4. Adopted by the Committee of Ministers at its 70th Session on 29 April 1982.

5. [1987] 1 WLR 1248.

6. The debate on this point appears to have been pursued with particular enthusiasm in the United States. Whilst Westin has argued that "personal information .. should be defined as a property right.." (Privacy and Freedom, op cit p.324.). Miller, by contrast, has stated that: "One of the most facile and legalistic approaches to safeguarding privacy that has been offered to date is the notion that personal information is a species of property." (The Assault on Privacy op cit p.211)

7. In England, the offence of theft is defined in the Theft Act as consisting of the dishonest appropriation of another's property (s.1). In Scotland, theft is a common law offence the essence of which has been defined as "the felonious taking and carrying away of the property of another." (Hume. Commentaries)

8. See Scottish Law Commission Consultative Memorandum No.68 on Computer Crime, para 4.24.

9. [1967] 2 AC 46.

10. Ibid p.127. C.f. dicta of Lord Dilhorne ibid at pp.89-90.

11. [1979] Crim. LR 183.

12. Ibid p.184.

13. [1979] 2 All ER 620.

14. Ibid pp.630-1.

15. 1987 SCCR 402.

16. Ibid p.408.

17. 149 DLR (3d) 583.

18. S.283(1).

19. Supra pp.599-600.

20. Ibid p.595.

21. S.158.

22. S.145(8).

23. S.158(5).

24. 13th Annual Report of the Director General of Fair Trading. June 1987

25. S.158(1).

26. Federal Data Protection Act s.34.

27. S.157(1).

28. S.56.

29. Fair Credit Reporting Act 1970 S.615.

30. Ibid S.609 providing that an individual is entitled to be be informed as to the "nature and substance" of information held relating to him.

31. The Consumer Credit (Credit Reference Agency) Regulations 1977, SI 329, reg 3.

32. S.158(2)(c) of the Act fixed a fee of 25 pence in this respect. This was raised to £1 under the Consumer Credit (Increase of Monetary Amounts) Order 1983, SI 1571.

33. SI 329/1977 Supra Schedule 1.

34. S.160(1)(a).

35. S.160(1)(b).

36. S.160(2).

37. S.160(4).

38. S.21(1)(a).

39. S.21(1). This provision can be contrasted with its counterpart in the Consumer Credit Act which requires (S.158(5)) that an applicant be supplied with a copy of his file translated, if necessary into "plain English". This appears a more 'user

friendly' formulation than that adopted in the Data Protection Act.

40. S.21(4)((a).

41. The question when a user's attempts to satisfy himself as to the identity of an applicant for subject access degenerates into an attempt to restrict the application of the subject access provisions may be significant. It has been reported (the 'Observer' 15 November 1987) that "most police and government searches require the application to be countersigned by 'a person of standing within the community' - as for a passport form - to confirm the applicant's identity." Such a requirement may, it is submitted, be considered excessive.

42. Guideline No.1 (First Series) p.21.

43. Guideline No.5 (Second Series) para 2.21.

44. Ibid para 2.22.

45. S.21(9).

46. [1986] AC 112.

47. [1883] 24 Ch.D. 317.

48. Supra p.173.

49. [1984] AC 778.

50. Ibid p.805.

51. Guideline No.5 (Second Series) para 2.33.

52. Harvey v. Harvey [1860] 22 D 1198.

53. Shades of the Prison House. Inaugural Lecture of Professor J M Thomson. University Of Strathclyde 1985. C.f. 1975 SLT (News) 157.

54. S.21(2).

55. Third Report of the Data Protection Registrar p.43.

56. Ibid p.24.

57. Supra para 22.35.

58. Data Protection (Subject Access) (Fees) Regulations 1987 SI No.1507. S.1.

59. 'Bulletin' University of Strathclyde. December 1987.

60. 'Glasgow Herald' 28 December 1987.

61. Art.8(b).

62. Supra para 22.36.

63. Supra s.36.

64. Art.8(b).

65. S.35(2).

66. S.21(8).

67. S.10.

68. S.13(6).

69. S.35.

70. 'Glasgow Herald' 28 December 1987.

71. S.21(8).

72. S.21(6).

73. Consumer Credit (Credit Reference Agency) Regulations 1977. SI No.329. Reg.3

74. Clause 21(6) 1982 Bill.

75. Art.8(b).

76. In Denmark, the Private Registers Act provides in s.5(1) that requests for access are to be met within 4 weeks.

77. The Swedish Data Act provides in s.10 that requests for access are to be met "as soon as possible.

78. S.21(6).

79. S.35.

80. S.35(2).

81. S.35(3).

82. Official Report (Standing Committee H) 22 March 1984 Col 464.

83. S.21(7).

84. Supra

85. Official Report (Standing Committee H) 22 March 1984 Col 464.

86. Art.9(2).

87. S.21(4)(b).

88. S.21(5).

89. [1978] AC 171.

90. Ibid p.200.

91. Hanbury. Equality and Privilege in English Law ((1952) 68 LQR 173 at 181.

92. S.4(4).

93. S.25(5). This provision applies only in relation to private sector data banks. Within the public sector, the right of access is unqualified.

94. S.28(1).

95. Supra

96. See, however p.424 supra concerning the possibility of abuse of the access provisions and the exceptions to the non-disclosure principles at the suit of a third party.

97. Although discussion will concentrate upon the application of the exceptions to the subject access provisions applying where data is held by a police authority, it must be noted that the exceptions are also applicable in respect of data held in connection with the collection or assessment of any tax or duty.

98. Supra

99. Supra para 8.03.

100. Ibid para 8.23.

101. Martin. Op.cit p.3.

102. Ibid p.4.

103. Ibid.

104. Official Report (Standing Committee H) 5 April 1984 Col 635.

105. Baldwin and Kinsey. Police Powers and

Politics. Quartet, 1982.

106. Guardian 31 October 1985.

107. Simitis. Data Protection - Experiences and Tendencies. Op cit p.6.

108. S.25(2).

109. S.30(2).

110. S.190.

111. SI No. 1905.

112. See Art 6 and also the provisions of the Council of Minister's Recommendation (81)1 concerning automated medical data banks which contains detailed provisions considerably more stringent than those found in the Convention. Inter alia, it is recommended that every data bank should operate subject to specific regulations devised by the national supervisory agency and providing detailed provisions relating to all the main aspects of the data bank's operations and management.

113. Art.8(2)(b).

114. S.29(1).

115. SI No.1903.

116. Ibid s.4(2)(a).

117. Ibid s.4(2)(b).

118. Ibid s.4(6)(c).

119. S.40.

120. S.29(2).

121. Official Report (Standing Committee H) 10 April 1984 Cols 780-1.

122. Ibid Col 781.

123. Supra para 24.11.

124. SI No 1904.

125. Ibid s.4(3).

126. S.34(2).

127. Official Report (Standing Committee H) 3 April 1984 Col 599.

128. S.45.

129. SI No.1906.

130. 'Observer' 30 January 1983.

131. S.31(1).

132. S.31(2).

133. Guideline No.6 (Second Series) para c4.3.

134. S.34(1).

135. S.34(4).

136. S.34(3).

137. Art.8(c).

138. S.25.

139. S.159(1).

140. S.159(2).

141. S.159(5)(b).

142. S.159(5).

143. Supra

144. Consumer Credit (Credit Reference Agency) Regulations op cit Reg.4.

145. S.22(4).

146. S.36(2).

147. S.22(2)(a).

148. S.10(3)(b).

149. S.36.

150. S.I. 1985 No.1465. Rule 19.

151 S.36.

152. S.3(2) of the Private Registers Act. It is further provided that a list of the parties so notified is to be submitted to the data subject.

153. Official Report (Standing Committee H) 13 March 1984 Col 358.

154. Ibid Col 363.

155. Official Report (Standing Committee H) 15 March 1984 Col 378.

156. Official Report (Standing Committee H) 13 March 1984 Col 359.

157. Supra paras 556-8.

158. Supra para 22.07.

159. Supra pp.429-30.

160. S.22(1).

161. S.22(3).

162. Official Report (Standing Committee H) 22 February 1984 Col 164.

163. S.10(2).

164. S.3(G)(1).

165. Parke B. in Toogood v. Spyring 1 C.M.&R. 181 at 193.

166. [1908] AC 390.

167. Ibid p.399.

168. Ibid p.400.

169. [1916] 2 AC 15.

170. Ibid pp.22-3.

171. Ibid pp.28-9.

172. Cmnd 5012 para 273.

173. Clause 136.

174. Official Report (Standing Committee D) 31 January 1974 Cols 604-6.

175. Cmnd 6353.

176. Ibid para 35.

177. Supra para 32.16.

178. Official Report (Standing Committee D) 5 February 1974 Col 610.

179. [1930] 1 KB 129.

180. Ibid p.148.

181. S.23.

182. Supra p.344. Given the failure of the prosecution in the cases of Oxford v. Moss and Grant v. Allan op cit it would not appear that a person obtaining unauthorised access to information will face any criminal sanctions in respect of this aspect of his behaviour.

183. S.23(3).

184. S.24.

185. See, most recently, the obiter comments of the Inner House in the case of Lord Advocate v. Scotsman Publications Limited and Others 'The Times' 25 April 1988, concerning the extent to which an undisputed obligation of confidence can be enforced against a third party who has come into possession of the information in question.

186. Simitis. Verbal presentation op cit.

Chapter Six

Conclusion - Beyond 1984

Conclusion - Beyond 1984

The lyrics of a recent pop song state that:

"Every breath you take
Every move you make
Every bond you break
Every step you take
Every single day
Every single way
I'll be watching you"(1)

In the song, the words are those of a rejected lover but they may equally serve as an anthem for the computer age and can be analysed in terms of the potential for societal surveillance resulting from advances in technology. Spy satellites travelling hundreds of miles above the planet's surface can photograph, in the most minute detail, earthborne activities. The Hong Kong government has been reported as testing a system for detecting, by means of the fitting of electronic transmitters, the movements of ~~individual of~~ individual cars with a view to charging tolls dependent upon the extent of road use.(2) In the United Kingdom, the use of camera's for traffic management purposes is relatively commonplace,(3) whilst experiments have been conducted with cameras trained on vehicle number plates and linked to the

police national computer with a view to identifying stolen vehicles.(4) Large gatherings of individuals are frequently monitored by video cameras whilst the use of such monitoring techniques in sensitive areas of cities has been seen as a means of reducing the need for a constant and, perhaps provocative, police presence. Although such pictures currently have to be viewed and interpreted by humans, the technology permitting automated recognition of faces is proceeding apace whilst the use of computers to enhance the quality and clarity of photographic images is well advanced. Telephone conversations may be routinely filtered through national security computers programmed to identify conversations which may be of interest to their human controllers.(5) Electronic recording devices are being introduced by credit card companies permitting instantaneous production of data concerning the time and place at which our purchases were made. Even the sanctuary of our personal thoughts is threatened by moves towards the use of polygraphs in employment matters.

If the above presentation identifies the threats which may be posed by technological advances, it would be perverse to attempt to deny the benefits which may also flow from their introduction. For every example of potential abuse, many actual or potential benefits can also be identified. The task for legal regulation is to maximise the advantages of technology whilst

minimising the resultant dangers. These dangers can be divided into two categories, first in terms of the impact of technology upon an individual, the consequences that may result from inaccurate identification as a terrorist or a poor credit risk. Beyond this, the application of technology possesses implications for society as a whole. It is stated that:

"the price of liberty is eternal vigilance"(6)

and that is a sentiment which may command widespread support. If the proposition is that the price of a substantial reduction in the crime rate is that of eternal surveillance, the degree of assent may be less.

The common feature of all these aspects of technology is that they generate information, they can thus be identified as forms of information technology. This has been identified as having a number of features which pose particular dangers for individual rights and liberties. Particular concern may be expressed at the novel pervasiveness of its applications and also at the extent to which the human intervention may be reduced to the role of a cipher, mechanically complying with the expressed wishes of the machine without any scope for interpretation or discretion.

The development of data protection legislation constitutes a partial response to the above dangers. In

attempting to assess the merits both of the concept of data protection and of its particular application in the United Kingdom, the point must be borne in mind that it cannot provide a solution to all aspects of information technology. Data protection applies in respect of the processing of personal data, in the case of the United Kingdom; data relating to a "living, identifiable individual". Where the effects of information technology have society wide implications data protection can have little direct impact. An illustration of this wider impact of the introduction of information technology can be seen with the changes in policing strategy which have been introduced or are which are contemplated resulting from the development of computerised data bases and the availability of processing facilities. In West Germany, the technique known as "Rasterfahndung" has been invoked to some effect and under circumstances of some controversy. The best known application of this technique occurred during the search for an alleged terrorist. Here, it was suspected that the terrorist was based in Hamburg. Obtaining data used for billing purposes from the Electricity Board the police processed and correlated the data in order to identify premises whose electricity consumption, including breaks during certain periods, matched their information as to the suspect's movements and life style. In the event, the results pointed to a small number of premises, the suspect subsequently being arrested at one of these.

The use of new technology for the purposes of detecting what may generally be regarded as heinous crimes cannot be condemned. It has been recognised, however, that the technique raises several significant issues. The analysis of the data obviously meant that data relating to very many innocent people was subjected to scrutiny, any match would inevitably put the individual concerned under the suspicion of being a terrorist.(7)

It would appear that, under the Data Protection Act, any police authority would be entitled to seek access to similar data on the basis that disclosure would be in the interests of crime detection. A further example of the use of personal data for policing purposes can be seen with the development of police controlled data banks. To date these have been most extensively deployed in Northern Ireland although increasingly computer systems are being used for intelligence gathering and processing purposes as a matter of routine. Two possible consequences have been identified as resulting from this development. First, there may be an increasing demand for information, the acquisition of which may involve the police in a more intrusive role. Second, and more significantly it has been suggested that:

> "The next step is to use the databases to target particular groups with selected characteristics irrespective of whether there

> is any reasonable suspicion that any particular individual is thought to have committed an offence. Everyone in the group is then treated as a suspect and made subject to regular monitoring and surveillance. In other words the traditional policing process in which the police begin with a crime and look for a suspect is reversed."(8)

Although such developments, together with other changes in society such as the increasing reliance upon means testing as the basis for eligibility for state benefits and the necessity to maintain detailed records of individuals places of residence in connection with the implementation of the "poll tax", are greatly facilitated by the processing power of the computer the issues involved extend beyond any question of the involvement of the computer and of their impact upon any particular individual. They call for a widespread debate as to the nature of today's and tomorrow's societies. Data protection legislation cannot substitute for such a general survey.(9)

The increasing value of, and reliance upon, information challenges existing criteria for the allocation of this resource. At the present time, information is allocated almost on a feudal basis. Ownership is vested in a few with the majority possessing extremely restricted title. Just as changes in western society prompted an

opening up of ownership rights in respect of physical property so, it is argued, a similar reform will be required in the area of information. Whilst these factors may possess some significance in the private sector their real impact may be considered to lie in the public sector. If decisions directly or indirectly affecting substantial aspects of an individual's life are to be made on the basis of recorded information the claim of that individual to participate in the informational process appears stronger. Initially, this may find expression in the claim for freedom of information but the implications extend further towards issues such as that of parliamentary accountability.

If the limitation of the scope of legislation to the situation where personal data is processed creates lacunae in the protection afforded to individuals against the dangers of computer abuse, a similar criticism can be levelled at the concept of the data user as the subject of the legislative controls. The marriage of the computer and telecommunications serves in many cases to render irrelevant the question of physical or legal control of data. Given the computer's capacity for linkage, the key issue is that of access to data. Recent proposals for the creation of a Government data network highlight the dangers involved in this area.(10) This system is proposes to link the records and administration of the Department of Health and Social Security, Customs and Excise, Inland Revenue

and the Home Office. Although each of these departments would, no doubt, be regarded as a data user in respect of their own holdings of data the ready possibility of accessing data held by another department would render positively misleading any statements of data holdings on the Data Protection Register whilst an attempt by an individual to make use of the subject access provisions would be reduced almost to the level of farce. Although such a data network would not be totally removed from the Registrar's sphere of control; he has little control regarding the issues of principle involved in such a development. By way of contrast, it may be noted that when a similar proposal for the creation of a national data centre was mooted in the United States in the 1960's these were subjected to extensive discussion and, following a critical report from a committee of the House of Representatives, the proposals were dropped.(11) The United States proposals, being defined by the technology of the time, constituted a more obvious target for criticism as the data centre would have been a single physical entity. The development of networks lowers the profile of such a development without making any corresponding reduction in the level of the potential dangers.

The remorseless advance of technology raises two key issues. First is the need for a greater degree of public debate and discussion concerning the social, cultural and political implications of new technology.

These may indeed threaten the role of Parliament. It has been commented that:

> ".. the problem for parliamentary institutions, posed by rapid technological change, is that of keeping pace. If nothing is done, a decision is made. Yet the very technicality of the changes makes it difficult for the lay politician (and indeed those advising him or her) to comprehend all the ramifications."(12)

In the United Kingdom, it may argued that the making of policy decisions is increasingly regarded as lying within the province of the executive with Parliament fulfilling a reactive role. Such a situation bodes ill for the maintenance of democratic control over the exploitation of information technology.

A second issue concerns the question whether, given the difficulty of controlling the uses to which technology is put, there should be a requirement for the technology itself to provide safeguards. An illustration of the issues involved can be seen in the case of Amstrad Consumer Electronics plc v. British Phonographic Industry(13) concerning the question whether the manufacturer of audio equipment should be permitted to include a facility which would facilitate the making of copies of audio tapes in violation of any copyright interests which might subsist in those tapes.

The issue has arisen again in relation to digital recordings with conflict arising between the manufacturers of hardware and representatives of the artists whose work appears on disc or tape. Here it has been suggested that the hardware should be designed in such a way as to prevent or at least inhibit the making of copies. Within the computer field, the suggestion has been made that:

> ". like cars have to meet certain safety requirements before their use is permitted, both the hardware and software must be equipped with a minimum of built-in protective devices excluding certain dangers and facilitating control. By no means a utopian expectation. Experience in the telecommunication sector confirms that the collection of personal data for payment purposes, can, for example by modifying the smart cards, be substantially reduced."(14)

Such an approach cannot be characterised as a "Luddite" resistance to technological development but stems, rather, from a responsible desire to maximise the nett benefit of such developments. In what may be regarded as a first step towards the establishment of technical standards, the Hessian Act of 1986 requires that public sector data users supply the Data protection Commissioner with extensive information concerning the

technical and organisational measures taken in order to ensure compliance with the substantive requirements of the legislation.(15) No similar provision operates under the Data Protection Act. Although breach of the eighth data protection principle requiring the maintenance of appropriate security measures may lead to the service of an enforcement notice, such a determination can only be made retrospectively.

In terms of the wider impact of informational practices the role of data protection legislation must be limited. The most that could be hoped would be that its tenets, concerned mainly with the collection, storage and dissemination of data, would influence the form of future legislative developments. The evidence to date would suggest that this hope may be in vain. In his third report the Registrar notes his concern with three aspects of government policy with regard to information which, he considered, paid inadequate regard to data protection considerations.(16) Under the Representation of the People (Amendment) Regulations 1985 electoral registrars whose registers were maintained on computer, were empowered to supply computer compatible copies of the register or to supply the relevant information in the form of sets of address labels. These regulations were introduced despite the Registrar's objections which were principally on the basis that individuals were given no opportunity to object to their data being used in this way. Although the activities of electoral

registration officers are excluded from the scope of the Data Protection Act which provides an exemption where a data user is statutorily required to publish information,(17) behaviour of this nature contravenes the principle that information supplied for one purpose should not be put to another use. Similar considerations apply in relation to the trade in the registers of company shareholders. Again, these are publicly available documents but their use as the basis of a mailing list is not consistent with the original purpose for which the information was collected and published. The most worrying development subsequent to the passage of the Data Protection Act has arisen in connection with the proposed abolition of the system of domestic rates and its replacement by the system of community charges, the "poll tax". By moving from a system where charges were levied on property to one where they are imposed upon individual residents the new tax requires the acquisition of information concerning individuals. To a greater extent than hitherto, details will be recorded as to an individual's place of residence and any changes thereto. Again, in large part, this information will be exempted from the provisions of the Data Protection Act. In respect of the legislation providing for the introduction of this system to Scotland, the Abolition of Domestic Rates (Scotland) Act 1987, no attempt as made to seek the Registrar's views on relevant aspects of the scheme.(18) A measure of consultation was

essayed with reference to the current proposals to apply the system within England and Wales. To date, however, this does not appear to have proved satisfactory with the Registrar feeling compelled to protest at the form which the legislation appeared to be taking. In December 1987 he was quoted as stating:

> "I feel confident that Ministers and Parliament did not contemplate that future legislation would pay no regard to the spirit of the Data Protection Act which, in turn aims to satisfy the requirements of the Council of Europe Convention."(19)

It may be doubted whether such confidence is not misplaced. Whilst the independence of the Data Protection Registrar may be unimpeachable, it may be argued that in the wider context of information policy, independence may be equated with impotence. Although, given the lack in the United Kingdom of a written constitution enshrining fundamental rights and ensuring judicial scrutiny of the constitutionality of the legislature's actions, the scope for comparison may be limited; it is instructive to compare developments in the United Kingdom in relation to the introduction of the community charge with the decision of the German Constitutional Court in relation to a proposed national census. In the United Kingdom, initially in Scotland, the creation of a Community Charge Register listing

those individuals liable to pay the charge constitutes an essential feature of the scheme. In the compilation of this Register, it has been stated, a variety of sources of information will be utilised. Although individual's will be obliged to volunteer information as to their own situation the completeness of the Register will be checked by reference to the electoral roll with access also sought by Registration Officers to the records of building societies, medical practitioners. In debating the introduction of enabling regulations reference was made to a number of petitions which had been presented to Parliament opposing the introduction of the new system. This prompted the comment from the Minister of State at the Scottish Office:

> "The hon. Member for Renfrew, West and Inverclyde (Mr. Graham), in a telling intervention, asked what was the point of all the petitions that he and his hon. friends had been submitting. As my hon. Friend the Member for Stockton, South (Mr. Devlin) pointed out, they could be a useful source of names and addresses for the community charge registration officer."(20)

Asked to confirm that:

> ".. from now on the names and addresses on

> petitions will be used for purposes of gathering the poll tax?"(21)

the Minister responded:

> "That is broadly what I suggested."(22)

Such a statement appears to demonstrate an attitude towards the principles of data protection which borders on the contemptuous. A radically different approach can be seen in the decision of the German Constitutional court in which it declared unconstitutional certain of the provisions of the Census Act of 1983.(23) This Act obliged citizens to supply personal information in conjunction with a planned census. In their decision, the Court held that the Act infringed Articles 1 and 2 of the Basic Law ("Grundgesetz). These provide, inter alia, that:

> "The dignity of man shall be inviolable. To respect and protect it shall be the duty of all state authority.
>
> Everyone shall have the right to free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or the moral code."

Referring to its previous decisions, the Court stated that the individual's right to freely develop his personality required that he be permitted to:

> "decide for himself - based on the idea of self determination - when and within what limits facts about one's personal life shall be disclosed."(24)

The justification for informational self determination was put as follows:

> "If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu, and cannot estimate sufficiently the knowledge of parties to whom communication may possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure/influence (=i.e. self-determined).. If he reckons that participation in an assembly or a citizens initiative .. will be registered officially and that personal risks may result from it, he may possibly renounce the exercise of his respective rights .. This would not only impair his chances of development but would also impair the common good, because self

> determination is an elementary functional condition of a free democratic community based on its citizens' capacity to act and to cooperate."(25)

It is the final sentence of the above quotation which is, it is submitted, of critical significance. The advent of the computer may have served to increase at a practical level, the potential consequences of data processing for the average citizen. The Court commented in this context, that:

> ".. under conditions of automatic data-processing, "insignificant" data thus no longer exist."(26)

The point remains, however, that the threat to the individual comes from the activities of those who hold data - and control the processing facilities. Whilst the German Constitutional Court recognises this fact the comments of the Minister of State indicate a refusal to accept that a balance has to be struck between the legitimate needs of effective law enforcement and the maintenance of a society that is free and democratic in fact rather than in rhetoric.

In terms of its wider impact, the influence of the Data Protection Act appears, to date, to be limited. In part this may stem from the relative novelty of its

institutional arrangements and bureaucratic uncertainty as to its rightful position within the corridors of power. The passage of time may serve to clarify these issues. A more pessimistic analysis of the likely impact of the legislation would suggest that the above examples are indicative of the general governmental attitude towards the concept of data protection. The point has been made previously that the spirit of openness which is inherent in the concept is in sharp juxtaposition to the climate of secrecy which traditionally, and it may be argued increasingly, surrounds governmental activities. On this analysis, the passage of data protection legislation was an act of pure pragmatism motivated by the need to protect commercial interests. The circumstances under which the legislation was enacted, coupled with the fact that in almost every area where the Convention affords discretion to national authorities, the provisions of the Data Protection Act adopt the most minimalist attitude compatible with bare compliance with the international requirements. Given this background, it would not be surprising were the Data Protection Act to be regarded as an isolated measure whose impact and influence would not extend beyond the comparatively narrow confines of the automated processing of personal data.

Moving from questions as to the wider role of information in modern society attention must be paid to

the internal merits of the scheme of regulation adopted within the Data Protection Act. Initially, it may be noted that legislative approaches in this field are in a state of flux. It has been commented that:

> "Data protection legislation is a very modern and typical example of laws that may not last for ever."(27)

As enacted, the Data Protection Act attempts to comply with the requirements of the Convention. This was opened for signature in 1981 but was drawn up in the light of the technology of the 1970's. It may be noted that more recent data protection statutes, such as that of the innovating Lander of Hesse, considerably expand upon the provisions of the Convention. Developments within the Council of Europe itself have not ceased with the Convention. In particular, it has been recognised that the sweeping statements of principle found in the Convention need to be tailored more closely to the practices and problems encountered in specific areas of processing activity. To this end, recommendations have been drawn up by the Council of Ministers covering such matters as the operation of medical data banks(28) and the use of personal data for the purposes of direct mailing.(29) It must be open to doubt, how far the United Kingdom's legislation will comply with these requirements. In particular, the latter recommendation provides that:

> "The collection of data from an individual for any reason other than normal customer or contributor relations should be permissable for direct marketing purposes only on condition that this has been expressly stated at the time of collection."(30)

The Data Protection Act contains no equivalent provision whilst the code of practice issued by the Advertising Association merely states that:

> "The Data Protection register being the primary source of reference for data subjects about data users, the requirements of transparency will normally be satisfied by the data user's registration for direct marketing of the sources, uses and disclosures of personal data as well as by the nature of the transactions themselves."(31)

Again, in relation to "automated medical data banks", the Council of Europe recommend, inter alia, that:

> "Every automated medical data bank should be subject to its own specific regulations.."(32)

It is further recommended that advance public notification be given of plans to establish such a data bank. Once again, it must be doubted whether the Data

Protection Act conforms with the letter, let alone the spirit of the Recommendation.

In general terms it may be concluded that the evolving trend appears to signify a move away from the notion of data protection as a monolithic, somewhat abstract topic towards its acceptance as an integral component of particular processing activities. Whilst, given the rapidity of change in this field, there may always be need for general statements of principle, this must be supplemented by more relevant and precise sectoral provisions. The Data Protection Act appears ill fitted to serve such a role. Subject to limited exceptions, there is no provision for the creation of definitive and authoritative rules applicable in particular areas. Whilst voluntary codes of practice can play a valuable role they are no substitute for precise legal guidance. As enacted, the Data Protection Act can be criticised as having taken a snapshot view of technology, indeed the technology of the early 1970's, and provided no mechanism for its updating short of the introduction of amending legislation. Given the notorious pressure upon Parliamentary time and the apparent lack of governmental enthusiasm for the topic it might be argued that this may not prove to be either an effective or an efficient procedure.

Turning to the content of data protection legislation in general, and that of the Data Protection Act in

particular, a number of issues are worthy of comment. An issue striking at the very heart of the legislation concerns the question whether its ambit should be restricted to the computer field or whether at least some manual records should also be included. The Data Protection Act is largely premised on the basis that the involvement of the computer poses novel issues of scale processing and accessing of data requiring special legal treatment. In large part, however, it is submitted, such a view pays insufficient regard to the wider impact of the computer. Just as the industrial revolution transformed the physical, social and economic environments of the 18th and 19th centuries so the computer revolution is promoting similar changes in the information, social and economic environments of the 20th century. Such a profound change in the landscape is not to be considered technology dependent. Concern, rather, may be considered to lie with the effects produced rather in the means by which these are attained. The effect of the computer has been to produce an environment in which recorded information increasingly replaces personal assessment as the basis for decisions affecting individuals. This trend is magnified by the use of computers but is not restricted to their area of operation. If this analysis is accepted, the approach of the United Kingdom legislation, in common with that of other jurisdictions, must be regarded as mistaken in restricting its application to the computer field.

Although, there will be a need for new legislation to pay particular regard to novel dangers posed by the application of new technology it is submitted that the main thrust of legislation should be purpose rather than technology orientated. There is, therefore, a need for a qualitative assessment to be made of the dangers that may arise from the use of information in particular contexts and for necessary preventative measures to be enforced. Whilst the use or otherwise of a computer may be a relevant factor in making such a determination it should not be the only or, indeed, the decisive factor. A partial model for such an approach may be seen in the provisions of the Consumer Credit Act which apply to all credit reference agencies regardless of the storage techniques used.(33)

Questions of the scope of the legislation inevitably effect the numbers of those required to comply with its provisions and, therefore the means by which compliance with its requirements can best be secured. The earliest data protection statutes were unanimous in advocating the introduction of a system of universal licensing or registration as the basis for control. Such a system offers advantages but it does serve to place limits upon the numbers who can be subjected to a reasonable degree of supervision. The vast numbers involved constitutes a major argument against the extension of data protection legislation to manual data bases. It is submitted that the advent of the personal

computer has served to transform the arguments in this area. Given the pace of technical development any definitions esssayed in this area must inevitably be broadly drawn. Equally inevitably, this will ensure that a large proportion of computer owner's will come within their scope. Even given the sizeable number of staff employed by the Data Protection Registrar, most users can expect to be subjected to a minimal degree of scrutiny. In this event, the fees charged for registration may be considered as a form of taxation upon computer owners, compliance with the Act a bureaucratic burden and compliance with the principles a similar imposition. To this extent, it is submitted, the registration requirements may be positively harmful to the best interests of data subjects both in terms of their influence upon the perceptions of data users and of their persuasive effect in limiting the scope of the legislation. It may be doubted whether the Data Protection Register serves an useful purpose in informing data subjects as to likely sources of relevant personal data. Although it may facilitate the attainment of an overall perspective of the nature and scale of processing activities it may be considered that this could be achieved through other means, for example, the commissioning of surveys of computer use. Preservation of the interests of data subjects requires, it is submitted, that all data users be required to comply with the substantive provisions of the legislation with more extensive supervision

reserved for those whose activities are manifestly more intrusive or threatening to individual rights. The United Kingdom approach bears all the hallmarks of the application of the lowest common denominator, swamps the registrar and the public with a mass of largely irrelevant and useless information the sifting of which must divert attention away from attempts to control undesirable practices.

In the final analysis, the Data Protection Act can best be judged by the criteria laid down by the then Home Secretary during its second reading debate. This was, he said, a measure intended:

> ".. to meet public concern, to bring us into line with Europe and to protect our international, commercial and trading interests."(34)

First then, does the Data Protection Act comply with the requirements of the Convention. In view of the case law of the European Court of Human Rights it may be doubted whether the extent of the exemptions provided for under the legislation would be considered "necessary in a democratic society" in the absence of any alternative procedures whilst the level of fee which may be required as a prerequisite to subject access cannot unequivocally be regarded as "reasonable". It is, however, a moot question how the

terms of the Convention might be enforced. The Convention itself contains no provisions relating to this point although it does provide for the establishment of a consultative committee to be composed of representatives of those states which have ratified the Convention and which is empowered to:

> "at the request of a party, express an opinion on any question concerning the application of this convention."(35)

Such opinions would not appear to be binding. At the State level it would appear that in the event that any other signatory imposed barriers against the flow of data to or from the United Kingdom the only legal response might be an action before the International Court of Justice alleging a violation of a treaty obligation. The procedures available to an individual in the event, for example, that a request for access had been rejected by the United Kingdom authorities on the basis that one of the Act's exceptions refusal of access appear even more limited. The right of individual petition established under the European Convention on Human Rights is not extended to the present Convention. The only basis, it is submitted, upon which such a course of action might be competent would be in the event it could be argued that the individual's right of privacy, as guaranteed by article 8 of the Human Rights Convention, had been violated;

the provisions of the Convention being cited as evidence of accepted standards in this area. The absence of any general facility permitting individual challenge of the provisions of national data protection legislation perhaps lends a measure of force to the United States criticism of the Convention as having little to do with the protection of the individual. It must, of course, be noted that the OECD Guidelines, largely promoted by the United States, are not binding upon states and no right of individual challenge exists whatsoever.

Beyond the issue of international compatibility, the internal merits of the Act must be considered. Here, the prognosis is somewhat gloomy. Data protection legislation inevitably requires the making of compromises with competing, and often conflicting, interests requiring to be weighed and balanced. In almost every instance, however, where the interests of the data user (particularly public sector users) conflict with those of the subject, the conflict is resolved in the former's favour. Although it would be disingeneous to deny that the Act does provide benefits to individuals, data protection legislation must be seen as an initial stage in the development of information policies designed to meet the challenges of the computer age. As the direction of any journey is often determined by that of its initial steps, the concern must be that, from an individual's perspective,

the Act provides an unsatisfactory basis for future legislative developments.

Footnotes

1. 'Police'.

2. 'The Observer' 22 May, 1987.

3. e.g. the CITRAC system used in Glasgow.

4. Campbell and Connor, op cit p.50.

5. 'Sunday Express' 13 March 1988.

6. Mill, op cit.

7. Simitis. Beyond 1984: The Law and Information Technology in Tomorrow's Society. Proceedings of the Fourteenth Colloquy on European law. Lisbon 26-8 September 1984. P.88.

8. Hillyard and Percy-Smith. The Coercive State. Fontana, 1988. P.277.

9. Even the question whether the development of computerised data banks serves to increase the operational authority of police forces is one which does not appear to have been satisfactorily answered. Some evidence (New Statesman, 29 June, 1984) suggests that the introduction of computerisation may, indeed, have been followed by a drop in the crime detection rate although the extent to which this may be affected by factors other than computerisation is, of course, uncertain.

10 Third Report of the Data Protection Registrar, p.5.

11. The Computer and the Invasion of Privacy, op cit.

12. Kirby. Every Move You Make. (1986) 9 Transnational Data and Communications Report (No.6) 19 at 21.

13. [1986] F.S.R. 159.

14. Simitis. Data Protection - Experiences and Tendencies. Op cit pp.19-20.

15. S.6.

16. Third Report of the Data Protection Registrar, pp.4-6.

17. S.34(1).

18. Third Report of the Data Protection Registrar, p.4.

19. 'Glasgow Herald' 4 December 1987.

20. 130 Official Report (House of Commons) 29 March 1988 Col 851.

21. Ibid.

22. Ibid.

23. [1984] 5 H.R.L.J. 95.

24. Ibid p.100.

25. Ibid pp.100-1.

26. Ibid p.102.

27. Freese. Transnational Data Regulation ; the Realities. Op cit. The Icelandic Data Protection Act of 1981 acted on this principle by providing that the legislation was to be abrogated three years after coming into force.

28. Rec 81/1.

29. Rec 85/20.

30. Para 2.4. The representative of the United Kingdom reserved the right of his Government to comply or not to comple with this provision. In view of the status of this document as constituting merely a recommndation to member states such an approach poses no current problems but it must be noted that the current Convention began life as a series of recommendations.

31. Para 3.1.5.

32. Para 1.2.

33. To a certain extent recent legislative developments appear to recognise the inappropriateness of the involvement of the computer as the sole criteria for triggering the application of controls over data practices. The provisions of the Consumer Credit Act have previously been noted whilst, subsequent to the passage of the Data Protection Act, the Access to

Personal Files Act, 1987 establishes a right for individuals to obtain access to certain housing and social work records (to be specified in Regulations to be made under the Act) maintained by local authorities with the concomitant right to secure the erasure of any incorrect information. As with the Consumer Credit Act, however, the legislation provides no control over general informational practices and policies in this field. Finally, the mmm Bill, currently before Parliament proposes to extend the rights of subject access, currently applicable in the situation where medical data is subjected to automated processing, to similar manual records.

Whilst any extension to the range of information available to an individual and any increase upon the level of his influence over the use to which personal data might be put is to be welcomed the attempt to separate the subject access principle from the remainder of the data protection principles can provide, at best, a partial solution to the problems of informational abuse.

34. 40 Official Report (House of Commons) 11 April 1983 Col 562.

35. Art 19.

Bibliography

Bibliography

1. Official Reports

United Kingdom

Report of the Committee on Consumer Credit. Cmnd 4596, 1971.

Report of the Committee on Privacy. Cmnd 5012, 1972.

Computers and Privacy. Cmnd 6353, 1975.

Report of the Committee on Data Protection. Cmnd 7341, 1978.

Data Protection. Cmnd 8539, 1982.

Reports of the Data Protection Registrar. July 1985, 1986 and 1987.

Guidelines on the Data Protection Act (Two series). Office of the Data Protection Registrar.

Breach of Confidence. Reports of the Law Commissions. Law Com. Rep. No.110. (Cmnd 8388) Scot. Law Com. Rep. No.90 (1984).

United States

The Computer and the Invasion of Privacy. Hearings before a Sub-Committee of the Committee on Government Operations House of Representatives, 1966.

Personal Privacy in an Information Society. Report of the Privacy Protection Commission, 1977

France

The Computerisation of Society. S.M. Nora. A Report to the President of France, 1980.

OECD

Information, Computer and Communication Policies for the 80's. 1982

Council of Europe

Beyond 1984: The Law and Information Technology in Tomorrow's Society. 1985

2. Books

Bing J (Ed) A Decade of Computers and Law. Universtetsforlaget, 1980.

Bourn C and Benyon J	Data Protection. Perspectives on Information Privacy. University of Leicester, 1983.
Burnham D	The Rise of the Computer State. Weidenfeld and Nicolson 1980.
Campbell C (Ed)	Data Processing and the Law. Sweet and Maxwell, 1984.
Campbell D and Connor S	On the Record. Michael Joseph, 1986.
Cohen R	Whose File is it Anyway? NCCL, 1982.
Cornwell R and Staunton M	Data Protection: Putting the Record Straight. NCCL, 1985
Delbridge R	Consuming Secrets. Burnett, 1982.
Flaherty D	Privacy and Government Data Banks. Mansell, 1979.
Flaherty D	Protecting Privacy in Two-Way Electronic Services. Mansell,1985.
Freedman W	The Right of Privacy in the Computer Age. Quorum, 1987.
Hewitt P	Privacy: The Information Gatherers. NCCL, 1977.
Hewitt P	The Abuse of Power. Martin Robertson, 1982.
Hillyard P and Percy-Smith J	The Coercive State. Fontana, 1988.
Hondius F	Emerging Data Protection in Europe. North Holland, 1975.
Madgwick D and Smythe T	The Invasion of Privacy. Pitman, 1974.
Marsh N (Ed)	Public Access to Government Held Information. Stevens, 1987.
Michael J	The Politics of Secrecy. Penguin, 1982.
Millard C	Legal Protection of Computer Programs and Data. Sweet and Maxwell, 1985.
Miller, A.	The Assault on Privacy. Ann Arbor, 1970.
Rostoker M and Rines R	Computer Jurisprudence. Oceana, 1986.

Rule J — The Politics of Privacy. Elsevier,1981.

Scottish Consumer Council — Rare Access. 1982.

Sieghart P — Privacy and Computers. Latimer, 1977.

Simons G — Privacy in the Computer Age. NCC, 1982.

Tapper C — Computer Law (3rd Ed.). Longman, 1983.

Turn R (Ed) — Transborder Data Flows. American Association of Information Processing Societies, 1979.

Wacks R — The Protection of Privacy. Sweet and Maxwell, 1980.

Weeramantry C — The Slumbering Sentinels. Penguin, 1983.

Westin A — Privacy and Freedom. Bodley Head, 1970.

Westin A — Information Technology in a Democracy. Harvard, 1971.

Westin and Baker — Data Banks in a Free Society

Will I — The Big Brother Society. Harrap, 1983.

Wilson D — The Secrets File. Heinemann, 1984.

3. Articles

Austin R — The Data Protection Act 1984: The Public Law Implications. 1984 Public Law 618.

Borrie G — Licensing Practice Under the Consumer Credit Act. 1982 Journal of Business Law 91.

Flaherty D — Protecting Privacy in Police Information Systems. 36 University of Toronto Law Journal (1986) 116.

Flaherty D — Government Surveillance and Bureaucratic Accountability. 11 Science Technology and Human Values (1986) 11.

Flaherty D — The Need for an American Privacy Protection Commission. 1984 Government Information Quarterly 235.

Gordon H — The Interface of Living Systems and Computers: The Legal Issues of Privacy

1981 Computer/Law Journal 877.

Hammond R — Quantum Physics, Econometric Models and Property Rights in Information. 27 McGill LLaw Journal (1981) 47.

Hammond R — Theft of Information. 100 Law Quarterly Review (1984) 252.

Hirshleifer J — Privacy: Its Origin, Function and Future. The Journal of Legal Studies (1980) 649.

Kirsch W — The Protection of Privacy and Transborder Data Flows of Personal Data. 1982 Legal Issues of European Integration 22.

Libling D F — The Concept of Property: Property in Intangibles. 94 Law Quarterly Review(1978) 104.

McLaughlin J — Intrusions Upon Informational Seclusion in the Computer Age. 17 John Marshall Law Review (1984) 831.

Michael J — Open Government and Data Protection. 8 British Journal of Law and Society (1981) 265.

Oliver P — Data Protection and Censuses Under the West German Constitution 1984 Public Law 199.

Patrick P — Privacy restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and the OECD Guidelines. Jurimetrics Journal (1981) 405.

Plishner J — Its None of Your Business. Or is It? California Addresses the Computer Age. 8 Rutgers Computer and Technology Law Journal 235.

Pounder C — Data Protection and the Police. 10 Journal of Law and Society (1983) 109.

Riley T — Data Protection Today and Some Trends. 17 Law/Technology 3.

Simitis S — Data Protection - Experiences and Tendencies. 19 Law/Technology 3.

Simitis S — Reviewing Privacy in an Information Society. 135 University of Pennsylvania Law Review (1987) 707.

Solomon T — Personal Privacy and the 1984 Syndrome. 7 Western New England Law Review 753.

Washburn P — Computers and Privacy. 3 Computer/Law Journal 189.