International Data Protection Standards and British Experience

B.W. Napier*

1. The Different Stages of Development of Information Technology Law in the UK

Within the new subject of information technology law, data protection occupies a relatively well-established sector. Indeed, the stage has now been reached when reform of the first attempts at regulation is appropriate. The British legislation of 1984\(^1\) is now being closely examined with a view to reform, both in the light of changing domestic priorities and change at the level of the EC. It is thus a good time to confront several important questions going to the foundation of any such laws, and to examine a number of issues which may be seen as particularly pressing. First and foremost, what legal interests are we seeking to protect within the context of data protection? Secondly, how are these interests threatened? Should we be concerned primarily with the data protection dangers posed by the acts of the State or by those of private industry? Thirdly, on a practical level, how can we accommodate the conflicting demands of commerce which favour the free flow of information and bodies concerned with the protection of civil liberties? And, last but certainly not least important, how and to what extent does the constantly-evolving technology of communications endanger basic human personal and democratic rights?

These questions are briefly examined below in the particular context of UK law and experience, but it will, I think, be readily agreed that they are questions relevant for all developed countries. It is also evident that, given the nature of the technology, both problems and their solutions extend beyond national boundaries. «Creating, implementing, and improving privacy and data protection laws and practices is a matter of pressing public concern in the Western world»\(^2\). Within the EC, the growing need

---

* Professor in the Queen Mary and Westfield College University of London.
\(^1\) Data Protection Act 1984.
\(^2\) D. Flaherty, Protecting Privacy in Surveillance Societies (1989), p. XIV.
for co-operation and mutual understanding between the Member States in data protection matters has now been given added impetus by co-ordinated programme of reform advanced by the European Commission. This movement is spearheaded by the draft Data Protection Directive, promulgated in 1990, which is now being considered by the Community’s law making institutions.

2. BACKGROUND TO DATA PROTECTION LEGISLATION IN UK

2.1. Privacy and the Common Law

Data protection issues are often considered by lawyers under the heading of privacy protection, and it is thus appropriate to begin by considering the legal background to this classification, before going on to look at more detailed technical concerns.

The common law (of England though not of the USA\(^3\)) has had great difficulty in accepting that privacy represents a value that requires legal protection. Nowhere is this better illustrated than in a recently decided case: *Kaye v Robertson*\(^4\). A journalist invaded the hospital room of television star who had suffered a serious accident and got an «exclusive» story from the semi-conscious celebrity. The star obtained an injunction preventing publication of the story under the rules of the common law but only with great difficulty, on a technical argument which sympathetic judges were able to use, while noting «the failure of both the common law of England and statute to protect in an effective way the personal privacy of individual citizens»\(^5\). This well-publicised case led to the appointment of a Commission of Inquiry (Calcutt) which recommended important changes in the criminal law governing the press to give recognition to the need to protect privacy. These changes, it must be said, have not yet been implemented. Even more recently, the interest of the popular press in Britain in the private lives of the Royal Family and politicians has fuelled the debate over whether such intervention is desirable. But even assuming legal restrictions on sensational journalism are introduced, it will only be this special aspect of privacy that is likely to find protection under the


\(^5\)Per Bingham L.J. at 70.
law\textsuperscript{6}. The privacy interest associated with data protection is seen as something separate. Another way of putting this is to say that, in Britain, the conceptual basis for data protection laws remains unclear, and this has been and is a major weakness in creating any coherent regulatory system. This leads to a basic problem for those who associate data protection with privacy protection, for it is obviously hard to defend controls designed to secure an effective regime of data privacy, when no such regime exists for privacy in general. But of course privacy protection (in the sense of acknowledging the right of the individual to be left alone) provides only one possible explanation for data protection laws, as we shall see below\textsuperscript{7}.

Discovering other explanations is not always easy. Consider, for example, the purpose of the Data Protection Act, as stated in the preamble: «To regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information». The important point is that the Act nowhere says \textit{why} such regulation is in order.

The refusal to endorse privacy protection as a legitimate objective in English law has meant that the rules we have are fairly narrowly conceived, compared to our continental neighbours. In France the legislation which encompasses data protection issues is notably broader both in application and objective than the equivalent in Britain\textsuperscript{8}. One difference is that in France (and in Germany and Netherlands) data protection controls are not restricted to automatically-processed data. Conversely, we in Britain have no equivalent to the French law of 17 July 1970, granting to individuals a right to have the privacy of their private life respected\textsuperscript{9}.

### 2.2. Deregulation and Legislative Intervention in the 1980s

Quite apart from the conceptual weakness of English common law, which has to do with the narrow-mindedness of legislators and judges over

\textsuperscript{6}The Calcutt Commission took as its working definition of privacy: «the right of the individual to be protected against intrusion into his personal life or affairs, or of those of his family, by direct physical means or by publication of information».

\textsuperscript{7}For example, human rights law may provide at least a partial justification. Interpreting article 8 of the European Convention the European Court of Human Rights has held that a British individual has the right to see social work files which relating to his years as a teenager in the care of a local authority: \textit{Gaskin} Case Eur Crt HR, Case No. 2/198/146/200, [1990] 1 FLR 167, ECrHR.

\textsuperscript{8}Brian Napier, «Data Protection and Secrecy in Britain» Franco-British Studies, No. 13, Spring 1992, 91.

\textsuperscript{9}Article 9, Code Civil. «Chacun a droit au respect de sa vie privee...». 
a number of years, there has been another quite separate barrier to creating an effective legal regime for data protection, and this is of recent creation. During the 1980s in Britain the policies of government were directed towards «deregulation» and the general reduction of administrative burdens on businesses. This tendency has most obviously been seen in the area of labour law, where the collective rights of unions and the individual rights of workers have sharply declined. The United Kingdom government has been and still is out of step with its European partners within the Community in social matters — witness the isolation of the United Kingdom in the aftermath of the European Union Treaty signed at Maastricht in February this year10 — but this has not been enough to deflect the United Kingdom government from its strongly-held views. Nor has it been troubled by other instances of international criticism from outside the Community — for example from the International Labour Organisation. In the field of labour law, there have several instances when international standards viewed as «inappropriate» by the government because of its commitment to deregulation were simply rejected. Yet, at a time when, in labour law, international obligations were being abandoned, paradoxically the UK embraced the principle of data protection, and indeed enacted legislation to give it effect. The 1984 Data Protection Act was the United Kingdom's answer to and implementation of the Council of Europe's Convention 108 of 1981. But any apparent inconsistency is explained when one examines the motivation behind government action — for the reason for British acceptance of data protection law was primarily commercial and pragmatic. It was based on a fear of the exclusion of the UK from the lucrative European market in information, following the Council of Europe Convention, and the prospect of other international instruments11. There was a fear that data transfers to countries without legislative protection in place might be blocked, and this fear proved more potent than any ideological commitment to the primacy of market forces.

The protection of human rights, it should be stressed, was not the main reason for changing the law, although government has found it convenient from time to time to refer to this as its main reason for acting.

From the British point of view, therefore, the present changes taking place in data protection law have a particular interest. In essence, what is happening at Community level is that data protection is being incorporated in 'hard' law. The topic is moving out of the worthy but too often marginal

area of Human Rights law – the province of the European Convention of Human Rights and the Council of Europe Convention No. 108 – into the area of business law, carrying significant economic consequences. This transition really should come as no surprise since one of the arguments for harmonisation within the EC is the need to equalise business costs of firms operating within the Community. Data protection entails business costs, just as does compliance with planning law or environmental controls. Backing for this new ‘commercial’ interpretation is to be found in the treaty base for the proposed EC Directive on data protection. This is Article 100A, which of course refers to measures necessary for the completion of the Single European Market. To quote the introduction to the Commission’s draft directive:

if the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross border flow of data might be impeded just when it is becoming essential to the activities of business enterprises and research bodies and to collaboration between Member States’ authorities in the frontier-free area provided for in Article 8A of the Treaty.

The irony, for the British at least, is that their own government appreciated this point very clearly at the time when it produced its own domestic legislation, nearly a decade ago. But the present Conservative government of the UK manifests a strong, residual opposition to Community standard making in this area, not only because of its commitment to minimising bureaucratic restrictions on business, but also because of its evolving views on the proper regulatory competence of Brussels.

Of course, equalisation of business costs – important though such an objective is – is not the only basis for Community action. A further powerful reason for harmonisation is the need to grant effective Community-wide protection to individuals’ rights. But in the end of the day the reality of upgrading data protection standards is to make data protection more burdensome and costly for businesses, while benefiting individuals.

Whatever the precise outcome for Community law (and yet another factor likely to influence this is the re-drafting of the draft Data Protection Directive now being undertaken in the light of views expressed by the European Parliament) it seems undeniable that important change is on the way. But until that comes about, the Member States with data protection legislation have to operate within the existing legal framework as best they can, and understand how their law is evolving. In Britain we have recently

12 COM (90) 314 final, 13 September 1990, para. 6.
seen some very interesting developments in our domestic law, which may perhaps be of interest from a comparative point of view. Certainly the issues which arise should have an interest which is not limited by national boundaries or the differences between common law and civilian legal systems.

In order to explain these interesting developments, a brief description of the British data protection legislation must first be given\textsuperscript{13}.

3. The Data Protection Act 1984

3.1. General Scheme of the Act

The 1984 Act is closely based on the scheme which underlies the parent Council of Europe Convention. Protection is provided for living individuals only. A system of registration for data users is put in place, and this operates through a quasi-governmental organisation, the Office of the Data Protection Registrar. Registration requires disclosure of the purposes for which data held by particular data users is to be put. Individual data-subjects may interrogate the register free of charge to see what automatically-processed data purposes have been entered on it. Through the Register they may discover what firms (and individuals) hold personal data relating to them. The Register does not give direct information about the data itself, but it allows for requests to be made by the data subject to the firms (and others) who actually hold the computerised information. When such requests are made, the data user must comply but may charge a fee of up to £10 for answering. There are currently around 150,000 entries on Register. The scheme only covers material held on automated systems, i.e. computers; other registers of information fall outside the scope of the legislation.

The Act envisages the protection of individual citizens (i.e. the data subjects) against three types of wrong: (a) use of personal data that are inaccurate, incomplete or not relevant to purpose; (b) the possibility of unauthorised access to or examination of personal data; (c) the use of data for a purpose other than that for which collected.

In a limited range of circumstances individuals whose rights are not respected may sue for compensation and obtain rectification or erasure of inaccurate data. But in practice enforcement is generally left to the Regi-
strar, who has powers both to act on his own initiative and to act after receiving a complaint.

The Registrar has a responsibility to maintain register, to offer advice and guidance, to pursue complaints and to apply sanctions. He has the job also of ensuring that data collection and processing is carried on in compliance with certain broadly-expressed data protection principles, as given in the Act. Actual enforcement of these principles takes place before a specialised court – the Data Protection Tribunal. This is the body to which appeal may be made from rulings of the Registrar, and it occupies a very important position, given the generality of the Principles themselves. Much depends on how the principles are interpreted by the Registrar, and the Tribunal provides a check on that interpretation. As we shall see below, the practical impact of the 1984 Act in a number of sensitive and difficult areas is being determined by the growing caselaw of this body.

The Act applies both the public and private sector, but there are substantial exemptions for activities deemed to be in the public interest. There are also several different levels of exemption. For example, national security is a reason for excluding application of the Act in toto from certain types of personal data; but the exemption under the heading of 'prosecution of crime' only gives exclusion from disclosure provisions.

3.2. Strengths and Weaknesses

First and foremost, mention must be made of the commitment and energy of Registrar and his officials. On taking up office they were faced with a daunting task, which involved nothing less than having to educate society to accept a wholly new form of regulation. In some ways, however, this may have been an advantage. For the absence of pre-existing law has permitted flexibility in the creation of new standards. That flexibility is also a feature of the eight data protection principles, which are characterised by an open texture which places a great premium on interpretation. For example, the first and most important is that «The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully». This leaves much to discretion of Registrar. To what extent, for example, does this allow for compromise between conflicting demands of different data users?

Flexibility certainly has advantages, but there is another side of the coin. Flexibility makes it difficult to predict the state of the law. Certainty is an important legal value put in jeopardy by discretion and there is no doubt that those countries (like the United Kingdom) which place faith in the
'guideline' approach to the drawing up of standards give extensive powers to the body or individual charged with giving an authoritative interpretation of the meaning of such norms.

The work of the Data Protection Tribunal is thus of primary importance in shaping the content of the obligations imposed by the legislation, via the framework of the Act. It has, moreover, become increasingly important as the Registrar, in the last few years, has progressed towards actual enforcement and not just the education and persuasion of data users and the public.

As the role of the Registrar has changed, so too has public awareness of the efficacy of the scheme he has to operate. The process of registration of all data-users, as a means of organising the regulation of information processing, has proved very time-consuming and expensive, and it is now one of the aspects of the scheme which may be changed.\(^\text{14}\)

Many commentators have also come to the conclusion that general principles are not enough, and there is a need to further develop sectoral codes to clarify the meaning of the Data Protection Principles in a practical way. This kind of development has already occurred at the level of the Council of Europe, as we shall see below.

Another area of concern is the Act's coverage. Manual files holding personal data are not covered by the Data Protection Act - and this feature is exploited by a number of organisations holding sensitive and controversial personal data.\(^\text{15}\)

From the point of view of civil liberties and freedom of information, the argument for extending regulatory controls to such bodies is very strong. But, when the actual purpose and original intention of the British Act is considered, the lack of coverage is quite understandable - though this is not to say it becomes excusable. As we have seen above, the Data Protection Act was never intended to be part of a freedom of information programme, any more than it was part of a governmental commitment to

\(^{14}\) This was an important recommendation of the major internal review of the Act held by Home Office in 1990.

\(^{15}\) For example, the body known as the Economic League, which is the subject of a recent book, M. Hollingsworth and C. Tremayne, *The Economic League. The Silent McCarthyism* (1989). The League is a body which supplies information on the political activities of job seekers to potential employers. It is funded by employers who subscribe to its service. Much of its work leads to the creation of 'blacklists' of union activists, who find it hard in consequence to find employment. Note that, in consequence of the reform introduced by the Employment Act 1990, s. 1, it is now unlawful to refuse employment to someone on the grounds of his membership (or non-membership) of a trade union.
the protection of privacy interests. The government has consistently objected to such moves to extend the Act’s coverage, and it is hardly surprising that it has never accepted — and still does not accept — the need to include manual records.

Another matter relates to the way in which changes in technology may render quite ineffectual protections which have their origins in thinking more than a decade old. For example, the British police have just introduced a new central computer to handle intelligence. This has twice processing power and nearly five times memory of predecessor. It can respond in three seconds to queries made of it, and the computer holds not just facts but also «intelligence» information — i.e. opinions often based on what has been said but not verified about individuals. The introduction of such technology obviously makes even more important the exemption under the Act allowed for police-held data within the general regulatory framework.

Technological change is of course to be expected in this fast-moving area, and it is hardly surprising therefore that a regulatory framework put in place to guard against threats posed by the technology of the 1970s is less than satisfactory today. In particular, advances in data processing mean that the phenomenon of «interconnectivity» — the possibility of linking together different computer systems, which may be situated in different countries — has become centrally important, in a way that could hardly have been imagined a decade ago16. One illustration of the present trend may be found in a recent news item, which announces a new system for detecting credit-card fraud. A central computer will check authorisation requests sent in by retailers against the pattern of spending associated with the customer in question; an apparent break in an established pattern will result in the alerting of police to a possible crime17.

Perhaps, however, the major weakness in the United Kingdom’s system of data protection law relates to the relatively low power of control it gives to the individual whose personal data have been recorded on computer. As we shall see, the movement at EC level is towards recognition of a right of control with regard to the uses to which such data may be put — and correspondingly a right to be informed in order to allow a proper choice to be made.


17 The system has been developed by Barclays Bank in London. In 1993 it is hoped to introduce a fully-automated version of the system, which relies on artificial intelligence to scrutinise buying patterns. See The Times, 18 September 1992.
The Council of Europe Convention, however, does not go so far as this, and neither does the British legislation. The individual enjoys no right of veto on the use to which his personal data is put, under either regime. Provided the purposes is legitimate — in effect, registered within the British scheme — and the data protection principles are followed, the individual can have no complaint in law about what happens to his or her personal data.

4. ROLE OF INTERNATIONAL AND COMMUNITY STANDARDS


The Data Protection Convention of 1981 has proved immensely important in setting standards and models for countries adopting legislation, and still is influential in the evolution of EC standards.

For example, the Schengen Information System, regulating cross-border police co-operation between a number of EC countries, is regulated by a Convention between the states concerned. It is provided under that Convention that personal data may only be transmitted between states when each Contracting Party has taken necessary measures to achieve a level of protection at least equal to that resulting from the Council of Europe Convention. The Schengen Convention is likely to come into force in 1993. But of course in one important sense the Council of Europe’s recommendation has failed — despite the positive recommendation made by the Commission as long ago as 1981 it has never been ratified by all the Member States, only by seven of them. The failure to adopt, on a Community-wide basis, Convention No. 108 provided a strong reason for developing another binding Community standard, and the present draft Directive is the outcome of that movement.

Since the Council of Europe’s Convention was introduced there have been two important developments in relation to it.

First, a growing realisation that general guidance on data use is not enough to give adequate protection. It has become accepted, one might say, that the balance between flexibility and certainty has swung too much towards the former. For this reason the past ten years have seen, at the level of the Council of Europe, the development of a growing number of sectoral codes. In area of employment, medical data, direct marketing, etc. These do not have the status of the parent Convention and are not binding on Member States in a strictly legal sense, but they are important both because they reflect the range of economic and regulatory activities in which data protection is perceived as important.
That they can have an important impact on practice is shown by the Schengen agreement, by which, in addition to compliance with the parent convention, arrangements have to comply with what is laid down in Recommendation dealing with use of personal data in the police sector\(^{18}\).

Secondly, it has become accepted that the old concept of privacy, understood as meaning as «the right to be left alone», is quite inadequate in modern conditions. Increasingly, there are demands for data subjects to have not just knowledge of who holds their personal data, but also control over the use to which others seek to put this information. Specific technological advances (e.g. telemetry, interactive mail, electronic mail) are seen as carrying their own special risks.

Despite the valiant attempts made from within the Council of Europe to adapt to new demands, the underlying problem has been that the Council of Europe's standards were not binding. And for that reason they could not guarantee the harmonisation of protection that was increasingly seen as desirable within the Community.

4.2. The Draft EC Data Protection Directive (SYN 287, September 1990)

In September 1990 the Commission of the European Community issued two Draft Directives in relation to Data Protection: the Draft Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data\(^{19}\), and the Draft Directive on the Protection of Personal Privacy in the Context of Public Digital Telecommunication Networks\(^{20}\). In both cases we are still quite a long way off from knowing what the final version of these standards will be, but the general principles set out in these proposals are likely to remain intact.

Work is most advanced on the Draft Data Protection Directive. The latest indications are that there are still many differences between the Member States and the Commission with regard to the desirable features of a harmonised data protection law. The European Parliament has given its Opinion on the Directive and, at the time of writing, a re-draft is expected. It is predicted that a Common Position will not be reached before the end of 1992, and final adoption of the Directive is unlikely before well into 1993. It is probable that Member States will have two years after adoption to bring the Directive into force.

\(^{18}\) Recommendation R (87) 15 of 17 September 1987.

\(^{19}\) COM (90) 314 final – SYN 257, 13/9/1990.

4.3. The Draft Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data

The Draft Directive has as its Treaty base, Article 100A, which concerns measures for the completion of the Single Market, although it also draws authority from the principle that Community law will respect human rights law. The point of departure is that differing data protection standards within the Community create unequal trading conditions – and thus harmonisation is both desirable and necessary. Some of the impetus for the introduction of this Draft Directive appears to have come from the activities of certain Data Protection authorities within the EC (notably the French), who have issued transfer prohibition notices in respect of data to be transferred to another EC Member State (including the UK) on the ground that the recipient state does not accord equivalent protection under its domestic law. This has occurred even where both states are signatories to the Council of Europe Convention, and is a clear barrier to the establishment of a Single Market. Under the proposed regime this barrier will not exist: thus the Summary of the Draft Directive states:

«Since every individual will enjoy in each Member State an equivalent, high level of protection... the Member States will no longer be able to restrict the flow of such data in the Community on grounds of the protection of the data subject».

Accordingly, the Draft Directive seeks to harmonise the laws of Member States, providing the highest level of protection available within the EC.

The definitions set out in Art. 2 are in general similar to those contained in the British Data Protection Act, though there are some changes of terminology21. One important change of substance, however, is the new definition of «personal data file (file)» in Art. 2 (c). This is defined as

«any set of personal data... undergoing automatic processing or which, although not undergoing automatic processing, are structured and accessible in an organized collection according to specific criteria in such a way as to facilitate their use or combination» (emphasis added).

The effect is that, for the first time, manual records are included within the scope of Data Protection, as this definition is clearly wide enough to

21 For example, the Draft Directive uses the term «controller of the file» instead of «data user» and the term «supervisory authority» instead of «Registrar». Throughout this section the Data Protection Act terminology is used wherever possible.
encompass manual filling systems. As already mentioned, the United Kingdom Government remains opposed to this extension to cover manual data, and the issue whether this should be a feature of the final version of the Directive remains open.

Two categories of file are excluded from the scope of the Draft Directive: files held by an individual solely for private and personal purposes; and files held by non-profit making bodies solely relating to members, providing that the members have consented to being included in the file and there is no communication of its contents to third parties. The Draft Directive also makes a distinction between private and public sector files. «Public sector» means all authorities governed by public law, except where they carry out commercial activities, and includes private bodies when they exercise official authority. The conditions under which the creation, processing and communication of data files is lawful differ between the public and private sectors, but the rights of data subjects and the obligations of data users are common to both.

It should be noted, however, that the latest indications are that the public/private distinction will not survive in the revised version of the Draft Directive; the general view now is that any different treatment of the two sectors should be a matter for national discretion within a broad general regulatory framework.

4.4. Private Sector Processing

The lawfulness of collecting and processing personal data by the private sector is governed by a number of important principles. The general principle contained in Art. 8 (1) is that to be lawful these activities must be consented to by the data subject. Consent means «informed consent». «Consent» in this context is defined by Art. 12, which provides that the consent is only valid if the data user makes full disclosure and if the consent is express and specific to the actual use and intended disclosure of the data. The data subject is entitled to withdraw this consent at any time, though without retroactive effect.24

---

22 Art. 3 (2).
23 Defined by Art. (12) (a) to mean:
\( a) \) the purpose of the files and the types of data;
\( b) \) the type of use and the recipients of communication of the file: and
\( c) \) the name and address of the data user.
24 Art. 12 (c).
There are, however, three circumstances where this express, informed consent is not required:

a) where the processing is carried out under a contractual or «quasi-contractual relationship of trust» between data user and subject, provided the processing is necessary for the discharge of the obligations of this relationship;

b) where the data are from public sources and are used solely for correspondence purposes; or

c) where the data user has a legitimate interest in processing the data, and the data subject's interest does not prevail25.

In addition to the requirement for informed consent, Art. 9 also requires the data user to inform the subject at the time of first communication of the data or when third parties are first offered the possibility of on-line consultation of the file26. If the data subject objects, communication and other processing must cease unless the data user is authorised by law to continue. Presumably any such legal authorization will be under Art. 9 (1) (a) and (c). It will be of particular interest to see what the legislature makes of the requirement to balance the user's interests against those of the subject. The Draft Directive does recognise that in some circumstances the requirement to inform will be impossible or involve disproportionate effort. In such a case, the Registrar may be empowered by national law to authorise a derogation from Art. 9 (1), and he may also do so if there is an «overriding» legitimate interest of the data user or a third party27. However, it is clear from the language of Art. 9 (3) that such a derogation must be authorised in advance; it will not be up to the data user to make this decision.

The obligation to register is limited to those files which might be communicated, though Member States are given power to require the registration of other private sector files28. The UK continues to argue that in place of a general obligation to notify both the data subject and the supervisory authority, there should be a system of declarations issued on request by data users. Such a system was proposed as part of the Home Office' own 1990 review of the Data Protection Act, but it is not yet clear whether this view will find support at Community level.

25 Art. 9 (1) (a)-(c).
26 There is, however, no obligation to inform if the data is derived from public sources and used only for correspondence purposes - Art. 9 (2).
27 Art. 9 (3).
28 Art. 11.
4.5. Rights of Data Subjects

In addition to the right of informed consent examined above, data subjects are to be given a number of new rights. The most important of these are:

a) the right to be given information at the time data is collected from them about the uses to be made of the data and the voluntariness or otherwise of their answers - Art. 13.

b) the right to oppose processing for legitimate reasons - Art. 14 (1).

c) the right not to have decisions made on the basis of data or personality profiling29 - Art. 14 (2).

d) the right to obtain the erasure of data held for market research or advertising purposes - Art. 14 (6).

The other rights of the data subject already given by the Data Protection Act are included in the Draft Directive, although the right of access to medical records may be limited to access through a doctor30, and the right to correction or erasure of data is supplemented by a new right of «blocking»31. «Blocking» appears to mean the technical solution that the data remain on file but are flagged so as to be inaccessible for certain purposes (e.g. third party access). Art. 14 (8) provides that the data subject is to have a judicial remedy if any of his rights are infringed.

Additionally, Art. 21 would establish an individual right to compensation in respect of damage suffered as a result of contravention of the principles of the Draft Directive. National laws may provide a defence that the security obligation in Art. 18 has been complied with, or where the processing of data has been sub-contracted to a third party that the requirements in Art. 22 have been met.

4.6. Obligations of Data Users

Art. 16 of the Draft Directive sets out five principles which are roughly equivalent to the Data Protection Principles contained in Sch. 1 of the Data Protection Act 1984. These are to be enshrined in national laws, and the data user will be obliged to comply with them.

29 The concern here appears, according to the Explanatory Memorandum, to be that the element of human discretion might be taken out of decision making by the use of e.g. credit scoring, thus depriving the subject of the possibility of putting forward evidence outside that used in the profile so as to influence the decision-making process.

30 Art. 14 (4).

31 Art. 14 (5) and (7).
Art. 17 makes provision for the prohibition of processing sensitive data. This category of data includes racial, political or religious information, information on trade union membership, and information on health or sexual activity. Data of this type may only be processed with the express, voluntary consent of the data subject, although derogation from this provision is permissible on public interest grounds if the law specifies the types of data to be processed, the persons who will have access, and the safeguards to be taken against abuse and unauthorised access.

A further prohibition is contained in Art. 17 (3) which is of particular relevance to employment data and to organisations such as credit reference agencies and banks. This is the provision that data on criminal convictions shall only be held in public sector files. It seems unlikely that this provision of the Draft Directive will survive the EC legislative process.

The data user's security obligations, set out in Art. 18, are far more detailed than those presently in force under the Data Protection Act. Additionally, the Commission has powers under Art. 29 to make regulations with respect to security precautions.

5. CONCLUSIONS

5.1. Need to Update Data Protection Legislation

Changes in technology and business practice mean that standards that refer back to 1970s are quite inadequate in the modern context. The technology is already in place that will allow the most intrusive surveillance of individual behaviour via electronic traces, and the interconnection of different computer systems makes the degree of control very much more extensive. An example has already been given showing how the technology can monitor individual spending patterns and detect 'unusual' purchases by credit-cards. Only by recognising the existence, in some form, of a right of veto for the data subject over the use to which their personal data use is put this new danger be met.

If anyone doubts the complexity of the problems which are now emerging, consider for a moment the web of electronic transactions which cross countries and even continents as a consequence of the most ordinary activities.

The following example makes the point. Imagine an American business

---

32 Art. 17 (1).
33 It is taken from an article by J. Reidenberg, «Personal Information and Global Inter-
traveller wanting to fly from Rome to Paris, rent a car at the airport, drive
to a meeting near Paris, spend the night in Reims and fly from Paris to
New York. Such a programme will necessarily involve different service
providers - travel agent, airlines, hotel, car rental company, and credit
card company. Furthermore, the journey will inevitably be based on several
computer reservation systems, which are likely to be interlinked. The travel
agent will handle and coordinate the overall plans, and this is likely to
include information on personal habits (smoker/non-smoker) and financial
status. If the flight Rome-Paris is by Air France then information must go
to Air France in Paris. The hotel in Reims might be part of multinational
chain with central data processing in London, and the car rental firm may
have outsourced its reservation and billing system in Germany. Payment is
likely to be on a US credit card. The point is, how can you even begin to
regulate such a complex set of transactions and communications?
Perhaps you say you cannot - but in the case you are forced to accept
that data protection will be regulated only by the law of the market. And
while many corporations set high standards, it would be naive to expect
that all do. Neither are high data protection standards likely to add much
to a company's attractiveness in the market place. As one commentator has
observed, as computer networks dramatically increase the number of actors
with access to personal information, transparency in the network infra-
structure has the nefarious effect of obscuring responsibility for personal
information. Paradoxically, transparency can, thus, decrease the visibility
and accountability of those controlling personal information. Put more
simply, the high standards of data protection observed by any one firm can
be breached easily by others with whom the data is exchanged, and it is
exceptionally difficult to identify who is to blame.
Those who put their force in market forces as the preferred regulator
of business services must thus accept that effective data protection is unlikely
to emerge as a consequence of competition between firms.

5.2. Data Protection and Constitutional Rights

So far in this paper we have concentrated on the tension between data
protection and business interests. This emphasis is justified because in the
modern world it is increasingly the need of business for free information
flow that seems to pose the greatest threat to privacy. But it shouId not be

connection: the Challenge of Regulatory Convergence» Project Promethee, Perspectives n.
18-19, 1991, p. 27.
forgotten that there is another dimension too, which involves threats posed by the state. The need to protect individuals against encroachment by the state, was the message behind George Orwell's 1984. Data protection is not just about protecting private law rights, it is about ensuring the climate necessary for democracy, and giving to individuals the context in which they can properly exercise their fundamental rights. This chain of reasoning takes us to consider the German concept of «informational self-determination»\textsuperscript{34} and its importance within public law in safeguarding the necessary liberties and rights of citizens. The preservation of democracy is, arguably, the ultimate reason for data protection standards - but it is a subject in its own right, and one which must be left for examination on another occasion.