NEW EUROPEAN DIRECTIONS IN DATA PROTECTION*

by

Colin Tapper[1]

Abstract

This article examines the direction being taken by the European Community in response to increasing threats in the field of data protection. At present the Community appears to be on the brink of making significant changes in the form of its response to these perceived threats. It seems likely that the draft proposals will be fairly controversial. While there seems little immediate prospect of the enactment of amendments to the data protection laws of most European states, it is not too early for the potential impact of this initiative to be assessed, thereby.giving an indication of the direction in which this branch of the law in likely to move in Europe - one which is likely to have an impact well beyond the boundaries of the Community.

Introduction

The computer is so universal a device, both in the range of its applications and in its geographical penetration, that developments in any one part of the world can rarely be isolated, but rather have effects elsewhere. This consideration applies just as much within a supra-national entity such as the European Community as anywhere else, so there is constant pressure for the creation of harmonised, if not common, developments throughout the member states. In their turn developments in so large a grouping of modern states have still more powerful an effect on other jurisdictions. Sometimes even the European Community is forced to act in response to pressure from outside, as in the case of the protection of semi-conductor chips,[2] or of computer software.[3] In the area of data protection it has tended to take the initiative itself. At present the Community appears to be on the brink of

---

* This terminology is itself controversial and question-begging, since one of the issues relates to the extent to which concern should be limited to the automated storage and processing of information, and how far it should be extended to manual records, in other words, whether the emphasis should shift from "data protection" to "privacy". The U.K. Registrar has noted that the concept of privacy is not used in the United Kingdom's Data Protection legislation, 7th Annual Report (1991) para. 3.

1 Vice President, Magdalen College, Oxford and All Souls Reader in Law.

2 See the Council Directive on the legal protection of topologies of semiconductor products (87/54/EEC)(OJ No. L 24/36)(27 January 1987), responding to the passage in the United States of the Semiconductor Chip Protection Act 1984, and together stimulating the passage in the United Kingdom of the Semiconductor Products (Protection of Topography) Regulations 1987 (S.I. 1497).

3 See Council Directive on the Legal Protection of Computer Programs (91/250/EEC)(14 May 1991) due to be implemented by member states by 1 January 1993.

making significant changes in the form of its response to perceived threats in this area. It seems likely that the draft proposals will be little less controversial than those relating to computer software.[4] While there seems little immediate prospect of the enactment of amendments to the data protection laws of most European states,[5] it is not too early for the potential impact of this initiative to be assessed.

1. Development of Data Protection in Europe

The first legislative steps to protect personal information in response to the threats perceived to arise[6] were taken in individual jurisdictions, such as the Land of Hessen,[7] and the Kingdom of Sweden.[8] The first attempt to arrive at a more comprehensive and consolidated European approach was taken not by the European Community, but by the broader-based[9] Council of Europe.[10] A number of preliminary meetings and recommendations[11] eventually culminated in the promulgation of a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which was opened for signature in Strasbourg on 28 January 1981. It was determined that the model should be one whereby signatory states agreed to legislate according to a common model, rather than one which merely provided reciprocal national protection.[12] Given the disparity of relevant provisions in different member states, and indeed complete absence of provision in some, reciprocal provision would be far from providing for a

---

4 Some 158 amendments to the draft directive were tabled when it was debated by the European Parliament in February 1992, so many that they were referred back to the Legal Affairs and Citizens' Rights Committee for consolidation.

5 In the United Kingdom the Data Protection Registrar has himself stated that "the recommendations I have made for changes to the Data Protection Act, together with those from the departmental Committee, will have to take a back seat whilst consideration of the Draft Directive takes place. In the light of this, it seems unlikely that the Data Protection Act will be changed for a few years." 7th Report chapter 3 (presented to Parliament June 1991).

6 See Tapper *Computer Law* (4th ed., 1990) pp. 318-322 for a critique of this perception.

7 Data Protection Act 1970.

8 Data Law 1973.

9 Sweden is a member of the Council but not (yet) of the Community, and its representatives played a significant role in the formulation of the Council's initiative.

10 The relevant working parties worked in close consultation also with representatives of the Organisation for Economic Co-operation and Development, and four of the latter's nonEuropean members, Australia, Canada, Japan, and the United States, were individually represented on the Council's advisory committee of experts.

11 See Resolution (73) 22 Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector paras. 1-11 for an account of these early efforts.

12 Like the Berne Copyright Convention, for example.

common minimum standard of treatment. It should be noted however that despite the justification advanced[13] for this view that the other model was contrary to "the idea that all persons should enjoy basically the same rights", the Convention gave signatories significant options to extend its scope and to derogate from its provisions in particular areas. Nor did it in any way preclude signatories from adopting more extensive protection if they chose to do so. The result therefore did little to promote equality of treatment in different jurisdictions.

Scope of the Council of Europe's Convention

Although the Council of Europe had started with proposals for the private sector,[14] it had speedily assimilated the public sector,[15] which was generally perceived to offer the more potent threat to individual privacy. When these preliminary recommendations were superseded by the Convention it too applied to both public and private sectors,[16] thus eliminating potentially difficult demarcation problems. Application to the public sector is however somewhat diluted by specific entitlement[17] to derogate from the provisions of the Convention in relation to necessary measures in the interests of "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences". The interpretation of such categories could well provide fertile material for controversy. There is also an entitlement[18] for a signatory to give notice of its intention not to apply the Convention to "certain categories of automated personal data files".

On the other hand the Convention explicitly[19] gives signatories the option[20] to extend its provisions in relation to data relating not to human beings as such, but to "groups of persons, associations, foundations, companies, corporations and other bodies consisting directly or indirectly of individuals", and interestingly whether or not such entities are accorded legal personality in the jurisdiction in question. Its potentially greatest extension is however to nonautomatic processing of such data,[21] thus opening the door to the protection of privacy as opposed to data.

---

13 Explanatory Report para. 12.

14 Resolution (73) 22.

15 Resolution (74) 29.

16 Art. 3.2.

17 Art. 9.2a.

18 Art. 3.2a.

19 Art. 3.2b.

20 It is not clear why such specific provision is necessary since the Convention does not purport to do more than provide minimum protection which any signatory is at complete liberty to augment.

21 By art. 3.2c.

It should also be noted that the Convention is not restricted in its scope to European jurisdictions, but is open for adherence to non-European states.[22]

Transborder Data Flow

It is interesting to note that by the time of the promulgation of the Convention a fresh problem had surfaced in the area. No longer was attention concentrated solely on the deleterious consequences for individuals of encroachment upon their privacy. As different jurisdictions legislated to prevent such encroachment[23] so it came to be perceived that differential protection might lead commercial dealers in personal information to shift their operations to the jurisdictions in which they were least restricted, and where the costs of compliance with local rules were lowest. This concern was associated with desire to protect local data processing industries which were often struggling to compete with large overseas competitors, especially those situated in the United States. Such competition was particularly formidable in the light of the huge size, enormous wealth and technical sophistication of the market for such services in the United States. These considerations became the focus for concern over "transborder data flow" as it came to be called.[24] At this point some tension is visible between the basic principle of the free flow of information provided for by Article 10 of the European Convention on Human Rights, and the thrust of the Convention on automatic data processing. In practice the latter concern seems to have prevailed since although the Convention provides that,[25]

> "A Party shall not, for the sole purpose of the protection of privacy prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.";

it also, in the next subclause, allowed liberal derogation in respect of transfer to a Party not offering "equivalent protection".

The possibility of imposing such restrictions, and indeed the reality of existing restrictions already under domestic legislation in various European states, created the further fear that unless "equivalent protection" was granted in the remaining jurisdictions, measures would be taken to prevent dataflow to those dragging their feet. This was certainly a powerful motivating factor behind the British decision to legislate in the form of the Data Protection Act 1984 as openly admitted in the relevant White Paper,[26]

---

22 Its title deliberately omitted the adjective "European" to emphasise this point.

23 By the time of promulgation constitutional amendments had been passed in three European states, and legislation in seven others, while preparation for such legislation was said to be advanced in a further five.

24 See Explanatory Report to the Convention paras. 8-10.

25 Art. 12.2.

26 Data Protection Cmnd. 8359 (1982) para. 2.

> "without legislation firms operating in the United Kingdom may be at a disadvantage compared with those based in countries which have data protection legislation. When the Council of Europe Data Protection Convention comes into force it will confirm the right of countries with data protection legislation to refuse to allow personal information to be sent to other countries which do not have comparable safeguards. This could threaten firms with international interests operating in this country and the activities of British computer bureaux which increasingly process data for customers in many different countries."

Data Protection Act 1984

The response of the British government was to enact legislation accepting the basic pattern of the Convention, but at the least possible cost. Part of that pattern involved acceptance of an approach which defined the area of application very widely, and then embodied wide principles with potential application over the whole field. This departed quite radically from the recommendations of the Lindop Committee, which had previously considered the question.[27] That body had taken the view that it would be more appropriate for detailed codes of practice to be enforced in particular fields.[28] It should be noted though that neither the Convention nor the Data Protection Act 1984 is inconsistent with the implementation of Codes of Practice. Indeed soon after the promulgation of the Convention the Council of Europe began publishing a series of recommendations relating to different fields of activity.[29] Similarly the Data Protection Act 1984 imposes[30] upon the Registrar a duty[31] to encourage the preparation of Codes of Practice where he considers it appropriate.[32]

The Act proceeds on the basis that data users will register their uses with the Registrar, furnishing him with relevant information on the collection, storage and dissemination of data. By the fees levied such registration is intended to contribute to the financing of the system,[33] and by

---

27 Cmnd. 7341 (1978).

28 This is similar to the approach taken in respect of public bodies in the United States under the Privacy Act 1974.

29 Including Automated Medical Data Banks (R (81)1); Computerised Legal Information Systems (R (83)3); Scientific Research and Statistics (R (83)10); Direct Marketing (R (85)20); Social Security (R (86)1); Police (R (87)15); Employment (R (89)2); and Payment (R (90)10).

30 Sect. 36(4).

31 Which he regards as important to the implementation of the legislation, see Second Annual Report of the Registrar para. 9 (June 1986).

32 Such Codes have been published in a number of areas including Travel Agencies; Advertising; Schools; Social Services; Local Authority Computer Systems; Libraries; Citizens' Advice Bureaux; Universities and other tertiary educational bodies; Direct Marketing; Pensions; Police; Employment; Computer Bureaux; and Pharmacists.

33 It was intended to be self-financing, but in only one year before 1989 did receipts exceed expenditure (according to Fifth Annual Report App. 5 para.

the declarations made to establish the foundation for enforcement. Subject to a number of exclusions and exemptions in whole or in part in respect of particular types of data,[34] the Act provides for enforcement through the ordinary courts by way of a mixture of civil remedies and criminal sanctions. Such enforcement encompasses provision for access to information by data subjects, and provision for rectification and erasure in certain circumstances.

During the currency of the Act the Registrar has conducted a number of surveys to assess the state of public opinion in relation to the operation of the Act, and to solicit suggestions for improvement. The working of the Act was also considered by a Home Office-led inter-departmental Committee reporting in 1990. This Committee broadly endorsed the operation of the Act, and in particular its application to both public and private sectors, and its limitation to automatically processed records,[35] and to information relating to human beings. Its principal recommendation designed to reduce the bureaucratic impact of the system was to eliminate the role of registration by making the data protection principles directly applicable upon data users, and employing declarations to data subjects as the vehicle for communicating the purposes for which data are held. This Report has itself been the subject of consideration by the House of Commons Home Affairs Committee, and the government has published its own response to the conclusions of that body. These documents are generally more specific in their orientation and deal with particular areas of concern. On the subject of the future of registration where the Registrar was more supportive of the principle of the current system, the Committee deferred to his view by refraining from endorsing the recommendation, and the government indicated that no steps would be taken in this respect pending further negotiation of the terms of the new European Community Directive.

2. Draft Directive

The first reaction of the European Community[36] to the initiative of the Council of Europe was to urge its member states to sign, implement, and ratify the Convention before the end of 1982.[37] This recommendation was accompanied by an intimation that if it were not complied with the Community would itself bring forward an instrument implementing measures of data protection under relevant provisions of the Treaty. By 1990

---

6 after which the form of accounts appears to have changed), and the break even point has continuously been postponed.

34 For fuller treatment of the Data Protection Act 1984 see the numerous monographs which discuss the Act including Niblett *Data Protection Act 1984 (1984): Gulleford Data Protection in Practice (1986): Chalton and Gaskill Data Protection Law (1988): and Chalton, Gaskill and Sterling (eds.) Encyclopedia of Data Protection (1988, updated).*

35 In this respect departing from a view commonly expressed by members of the public, see for example Third Annual Report of Registrar para. 8(a).

36 Which has observer status at Council of Europe meetings, and is in close contact with all proceedings and recommendations.

37 Commission Recommendation of 29 July 1981 (81/679/EEC).

the Commission noted that only seven member states had ratified the Convention, and of those one had no domestic legislation implementing it. It took the view that the Convention was, in any case, ineffective to promote sufficiently similar approaches in different states, partly because of the local options in relation to manual information and artificial persons, and partly because it left the process of implementation to local laws which differed greatly in their detail and in their practical effect. Such diversity was regarded as a serious obstacle to the completion of the internal market,[38] and a possible impediment to the development of relations with states outside the Community. For these reasons the Commission determined to propose a number of different measures as a package. These comprised first, a general framework directive implementing a high level of data protection in all member states; second, a meeting of representatives of member states to extend protection to data relating to matters not covered by Community law; third a declaration of the application of the general directive to the institutions of the Community as such to the European Convention; fourth, a sectoral directive implementing such data protection in the telecommunications sector; fifth, accession by the Community as such to the European Convention; and sixth the adoption of a two-year action plan to improve information security within the Community.

Public Sector

The first instalment of this programme is the draft Council Directive.[39] It deals both with public[40] and private[41] sectors, and most importantly extends to manual as well as automated records.[42] In relation to the public sector it provides[43] that files can be created and data processed only in so far as necessary for the performance of the tasks of the public authority in control of the file, and it seems that the purpose for creating the file must be signified at that time.[44] Any other processing of data is

---

38 Especially in relation to telecommunications equipment and services.

39 COM (90) 314 Final - SYN 287. 40.

40 Though here mandatory only in so far as the public activity is within the scope of Community activity.

41 Excluding files held by individuals solely for private and personal purposes, or by nonprofit-making bodies so long as the data relate only to the members and are not communicated to third parties, though it seems that a data subject may always consent to such communication, see Art. 8.

42 See definitions in Art. 2 of (c) "personal data file" as including data "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 of combination; and of (d) "processing" to mean "the following operations, whether or not performed by automated means: the recording, storage, or combination of data, and their alteration, use or communication, including transmission, dissemination, retrieval, blocking and erasure."

43 Article 5.1 (a).

44 Art. 16.1(b) requires that purposes be made specific, and the commentary interprets this to signify that they should be narrowly defined; Art. 7.2 provides that the purpose must be notified to a supervisory authority; and

permitted only with the consent[45] of the data subject, or not precluded by his legitimate interests, or if it is necessary to "ward off an imminent threat to public order or a serious infringement of the rights of others", or if it is effected under a Community law[46] or of a Member State conforming with the Directive. It cannot be claimed that this provision is a model of clarity. In particular the concepts of necessity, legitimate interests, imminent threat, and serious infringement are left undefined, and are clearly quite nebulous and capable of varying interpretation. The interaction of the two parts is also obscure. Since the first part appears not to require consent of the data subject, but only necessity for the intended purpose, it is not clear why an authority wishing to change the use of a particular file but apprehending that data subjects would not consent to such a change, should not simply act under the first part and create a new file.

The communication of personal data held in the public sector is made the subject of separate provision.[47] Although communication is not defined it seems to connote communication outside the entity holding the data.[48] Such communication is permitted only to the extent that it is necessary for the performance of the tasks of either communicating or requesting entity in the public sector,[49] or if requested by "a natural or legal person"[50] in the private sector, then only if the requesting party invokes a legitimate interest, and that interest prevails over any interest of the data subject.[51] Provision is made for specification by Member States of when communication is lawful, presumably so as to inhibit wrangles over relative interest. There is a curious safeguard in relation to communication outside the public sector to the effect that the data subject shall be informed of the communication. The oddity is that it appears to be capable of taking effect after the communication has been made, though one would have imagined that the purpose of the provision would be to permit the assertion of an interest in the communication not being made. It is further qualified by explicit provision for this to be replaced by prior authorisation by a supervisory authority. It is left unclear whether such prior authorisation is intended to be

---

Article 5.1(b) comes into effect when it is proposed to process data for some other purpose. It seems also to be supposed that the "tasks" of a relevant public authority may readily be identified.

45 Which must be informed consent obtained by the procedures established by Art. 12.

46 Or measure pursuant thereto.

47 By Art. 6.

48 Though this implies lines of demarcation which may not be entirely clear, for example is communication to an employee of the same entity but in a quite different department a communication for these purposes?

49 It appears to be assumed that the request will always be for communication to the body making the request, and not to a third party.

50 Apparently excluding bodies without formal legal personality.

51 Which is left unqualified, though whether because any interest is presumed automatically to be legitimate remains unclear.

specific or generic. The latter seems more practicable, but also to be far less responsive to the assertion of interest by the data subject.

Provision is further made[52] for advance[53] registration of public sector files from which personal data might be communicated with a supervisory authority. It seems that here "might" refers not to possibilities but to intentions as one of the matters to be notified is the identity of third parties to whom such communication might be made.[54]

Private Sector

The regulation of private sector processing is still more burdensome. Member states are required to ban the recording or use of personal data which does not conform with the provisions of the Directive, unless the data subject consents, or the processing is carried out under a contract or in the course of a quasi-contractual relationship and is necessary for its discharge, or uses only publicly accessible data and then only for "correspondence purposes", or where the controller of the file is pursuing a legitimate interest over which the interest of the data subject does not prevail. The obligation is naturally enough normally put on the controller of the file, but in the case of on-line consultation is also placed upon the user.[55] It is very difficult to appreciate quite how this will operate, since it is likely to be the case that users will have no means of knowing whether consents of the subject have been obtained in accordance with Article 12 or whether data has been collected in compliance with Article 13, and it would seem most unjust to subject them to liability in case of breach.

In the private area the controller is under an obligation to inform the data subject at the time of the first communication relating to him, or when the data are first made available for on-line access. This obligation applies to all legitimate data processing, except only in the case where the information is available from publicly accessible sources, and is used only for correspondence. This seems intolerably burdensome. For example in relation to a legal database in a common law jurisdiction it would apparently involve making contact with every person identified in every reported case before making it available. This would clearly involve immense delay, and expense. Although there is provision[56] for derogation from this requirement, it does seem to create a bureaucratic nightmare. Here too there is provision for notification to a supervisory authority though in contrast to the provision for the public sector no explicit reference is made to registration.

---

52 By Art. 7.

53 Though whether in advance of creation or first communication is not entirely clear.

54 Though as against this view it could be urged that the terminology changes in relation to the private sector where notification is required only when communication is "intended to be communicated".

55 Art. 8.2.

56 In Art. 10.

Rights of Data Subjects

The Directive specifies particular rights for data subjects. These relate to the nature of consent,[57] the collection of data,[58] and a number of miscellaneous rights.[59] It is not appropriate to consider these in minute detail, but, as elsewhere, the drafting seems very loose, and leaves important questions unresolved. One example will suffice to indicate the nature of this concern. Art. 14.2 grants a data subject the right, "Not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality." Such a provision teems with uncertainty, and cries out for clarification. Suppose a private adoption agency automatically screens out applicants who have confessed to offences of child abuse.[60] It would be necessary to know whether such screening amounted to the definition of a profile or personality. It is unclear whether the profile is what must not be processed, or what must not be the result of processing. It is unclear whether conduct refers to the past so as to prevent unfairly based assessments of what the subject has done, or to the future so as to prevent unfairly based assessments of what he might do, or both. It might be very difficult to determine when such an assessment was solely based on the relevant profile.[61] These rights are then made subject to limitation for a number of reasons, such as national security, defence, and criminal proceedings. Some of the concepts are however rather more obscurely expressed, such as "a duly established paramount economic and financial interest of a Member State", and "the equivalent right of another individual and the rights and freedoms of others". Such phraseology must quicken the pulses of professional advisers. Although for some reason segregated into the chapter dubbed "Data Quality" the Directive also prohibits any[62] processing of data "revealing ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership, and of data concerning health or sexual life, without express and written consent, freely given, of the data subject."[63] Such a blanket prohibition seems quite unworkable, for example, must every library with an automated catalogue

---

57 Art. 12.

58 Art. 13.

59 Art. 14.

60 Data relating to confession rather than convictions has been chosen so as to evade the prohibition in Art 17.3 of the private holding of data concerning criminal convictions, a technique which itself indicates the unsatisfactory operation of the provisions.

61 Presumably its interaction with a major premise relating to the possession of such a profile, such as the one implicit in the example, that no person with a conviction for an offence involving child abuse is eligible for consideration for adopting a child, would not be enough to prevent the possession of such a profile being the sole basis for the decision, but it is not hard to imagine borderline cases.

62 Subject only to derogation on "important public interest grounds" by Art. 17.2, yet another example of the use of vague and undefined terminology.

63 Art. 17.1.

expressly seek the permission of a prominent politician who has published a book entitled "My Political Credo" before it operates the system? The same sub-division restricts data concerning criminal convictions to public sector files.[64] This seems too broad in allowing for no exceptions, and too narrow in being restricted to data concerning criminal convictions, and thus not referring to any other information such as that relating to confessions of crimes, as used in the example above.

The Directive states[65] familiar principles relating to the quality of data derived from the Council of Europe's Convention. It is however encouraging to find in the context of data security at least some reference to the sort of balancing exercise which it is submitted[66] ought to dominate the whole approach to this area,

> "Such measures shall ensure, in respect of automated files, an appropriate level of security having regard to the state of the art in this field, the cost of taking the measures, the nature of the data to be protected and the assessment of the potential risks."

A similar need for balancing is perceived in relation to the application of the Directive to the media of communication, where it is explicitly provided[67] that derogations may be made "in so far as they are necessary to reconcile the right to privacy with the rules governing freedom of information and of the press."

A further welcome feature is the encouragement which the Directive offers[68] for drawing up codes of practice for particular areas. It is only when the general platitudes of the Directive are reduced to specific and practical proposals that they can begin to become effective in influencing conduct.

Miscellaneous Provisions

The Directive devotes a separate chapter[69] to Liability and Sanctions. It imposes primary civil liability upon the controller of the data, and imposes upon him a legal burden of proving that he has complied with the relevant principles[70] relating to data quality and security. It further requires "dissuasive", apparently criminal, sanctions to be applied by Member States to ensure compliance.

---

64 Art. 17.3.

65 In Art. 16.

66 For further elaboration of this view see Tapper *Computer Law* (4th ed. 1990) pp. 327-328.

67 Art. 19.

68 Art. 20.

69 Ch. VII.

70 Stated in Arts. 16 and 18.

Transborder data flow is specifically addressed in Chapter VIII[71] which provides a mechanism providing for the prohibition, and derogation from such prohibition, in case of proposed transfers of data to countries not offering "adequate" levels of protection. It is not clear why this terminology has been substituted for the "equivalent" level required by the Council of Europe's Convention, though it has been suggested[72] that it is, if different, a less stringent standard.

The remaining parts of the Directive establish the administrative machinery for operating the Directive which include setting up an advisory Working Party on the Protection of Personal Data.[73] It is envisaged that this body will submit annual reports to Member States on the working of the Directive, and the situation relating to the protection of personal data in Member Countries. There is further provision[74] for setting up an Advisory Committee to assist the Commission in its rulé making powers, since it is envisaged that this area contributes to the completion of the internal market, and is thus within the remit of the Commission.

3. Responses

Although it is too early to assess responses to the draft Directive in detail,[75] still less the reaction of the Commission to suggestions for amendment,[76] it is worth noting the initial reactions which have so far been published, as these may give some indication of lines of criticism to which reaction can be expected, given the Commission's normal practice.

At an official level the Council of Ministers of the European Community has welcomed the Directive, and agreed to apply its principles to public sector data processing in areas outside the areas covered by the Treaty of Rome. In the same instrument the Commission undertook to apply the principles within the area of Community activity for which it was responsible and to urge other Community institutions to do the same pending the passage of formal measures to accomplish this.

The preliminary, and cautious, response of the British government to the Directive was to endorse the principles of the Directive but to engage in a consultative exercise[77] before making recommendations for legislative

---

71 Which somewhat mysteriously refers to transfers to *third* countries, without indicating which is the *second* country in this computation.

72 By a British government spokeswoman, Mrs. Rumbold, in addressing the European Committee of the House of Commons on 5th June 1991.

73 Art. 27.

74 Art. 30.

75 At the time of writing the author has no access to the full report of Legal Affairs Committee of the European Parliament which has proposed a large number of amendments to the draft.

76 Which has not been published, and perhaps not even formulated, at the time of writing.

77 Initially circulating a detailed comparison of the draft Directive and the U.K. provisions to more than two hundred bodies known to have an

change.[78] In its official response to the report of the Committee the government was still guarded, and in particular drew attention to the tension between the influence of free market and privacy elements in the draft, perhaps signalling its intention to promote further consideration of the British approach which has tended to be more receptive to business anxieties about the cost and bureaucratic overload of protection.

Data Protection Registrar's Response

A fuller explanation of the views of the Data Protection Registrar[79] of the United Kingdom was published in December 1990. He advocated a drastic restructuring of the Directive so as to attach prominence to the provisions relating to data principles and quality,[80] and to subordinate detailed regulation such as that relating to subject notification.[81]

He was also most concerned about the range of the directive, arguing on the one hand for a reduction in its coverage of manual information,[82] and on the other for an extension in its application to non-profit organisations. In many case he felt that the detailed regulation of the Directive was more suited to providing possible options for compliance with the general principles, than to having mandatory force. A more general concern was that the Directive did not distinguish adequately between the rules applicable to public and private sectors, and in particular that some exemptions should also apply to the private sector.[83] On the other hand he felt that some public sector exemptions were too sweeping, for example those of Article 6 allowing communication of public sector information to meet the needs of other public sector bodies.[84] Some of the provisions were felt to be alien to

---

interest in data protection. The Commission itself sponsored a similar exercise which was attended by the U.K. Registrar.

78 See First Annual Report of the Home Affairs Committee on the work of the Data Protection Registrar para. 9.

79 Mr. Howe.

80 Identified as being contained in arts. 16 and 14 (in that order).

81 In arts. 9 and 13.

82 By restricting it to manual information used in conjunction with automated systems, for example indexing systems, and leaving other specially sensitive areas to separate provision.

83 For example to allow some information about criminal convictions to be held.

84 Thus permitting cross-matching too readily.

the common law tradition,[85] for example that forbidding specified uses of profile and personality as defined by personal data.[86]

Response of European Committee of the House of Commons

The matter was then debated in the European Standing Committee of the House of Commons.[87] In that debate many of the points made by the Registrar were repeated, especially the objection to universal extension to manual data,[88] to the more lenient treatment of information in the public sector, to the restriction on private sector holding of personal data relating to criminal convictions, to the universal ban on profiling,[89] and to the treatment of personal databanks held by the media.[90] Soon afterwards the Registrar in the United Kingdom adverted once again to the draft Directive in his annual report to Parliament.[91] In addition to many of the preceding points he rehearsed there his apprehension lest the encouragement offered to the development of Codes of Conduct in Article 20 should be regarded as a self-regulatory substitute for direct enforcement. The Article leaves this open to interpretation, though it seems more likely that the Registrar's preferred approach that such Codes should merely be educational and exemplificatory of the working out of the general provisions into detailed rules reflects the intentions of the framers.

Response of European Parliament

Most recently the matter has been debated in the European Parliament.[92] It seems that some 158 amendments to the draft Directive were originally tabled, though these were referred back to the Legal Affairs and Citizens' Rights Committee for consolidation. The Committee had questioned the need to impose the highest standard of protection by amalgamating the highest levels of all member countries, and proposed more balancing between the practical needs of business and the protection of individual privacy. Among the more detailed recommendations were the

---

85 It has been suggested that a first draft of the draft Directive was shown to the Germans and drastically rewritten to conform more closely with the scheme of protection there, see Report of Proceedings of European Standing Committee B of the House of Commons, 5th June 1991, speech of Mr. Peter Bottomley.

86 Art. 14.2, which the Registrar noted was taken from the French Data Protection Law.

87 On 5th June 1991.

88 At least in part on account of the cost.

89 Which it was felt would lead to still more scatter gun an approach to junk mail shots.

90 Members of the Committee had received strong lobbying on this matter.

91 Pursuant to the Data Protection Act 1984 sect. 36(5).

92 This section of the article relies upon the analysis presented by Stewart Dresner in 9(3)*Applied Computer and Communications Law* 5 (March 1992), as the debates of the European Parliament were not available to the author at the time of writing.

elimination of the difference between private and public sectors; substitution of references to "data" for those to "data files"; preference for opting-out rather than opting-in for mailing lists in particular; adoption of a more subject specific and discretionary approach to transborder data-flow;[93] and rejection of the width of the derogation proposed for the media of communication.[94]

This lengthy catalogue of proposed amendments, liable to be afforced in the course of debate, is likely to delay the preparation of a revised text of the Directive, and in any event the European Parliament has asked for a further opportunity for review before the final text is passed to the Council of Ministers for adoption. Given that it has sensibly been decided that it would be pointless to change the British Act until agreement has been reached on the terms of the Directive, it is not surprising to find that the English Registrar has concluded that, "it now seems unlikely that the Data Protection Act will be changed for a few years."[95]

New Approach of the Council of Europe

A different response to the current situation has been made by the progenitor of the current approach, the Council of Europe. Recognising the difficulties and delays inherent in any proposal to harmonise the provisions of public law in different jurisdictions the Council has, imaginatively and realistically, looked instead to the private sector. There is already a burgeoning trade in personal information, and it makes sense to seek to regulate it by appealing to the self-interest of those engaged in this trade. Already there are powers under national legislation to prohibit the transfer of personal information across national borders.[96] The Council of Europe has accordingly drafted[97] some model contractual provisions for the supply and use of data which it is hoped will at least go some way to ensuring that under such contracts equivalent protection is offered to that secured by the Council of Europe's Convention, and thus under its terms permitting transborder communication.

---

93 It had been argued in the United Kingdom that the financial services industry would be crippled by the Directive as it stood, especially with regard to transborder data-flow between the United Kingdom and the United States and Japan.

94 In this respect contrary to the tenor of the lobbying of the European Committee B which had been urged to seek more protection for such media.

95 Seventh Annual Report para. 3.

96 In the United Kingdom under sect. 12 of the Data Protection Act 1984. This was first invoked on 3rd December 1990 in respect of the transfer of mailing information by a British company to the United States to a congeries of organisations suspected of fraudulent mail order trading.

97 T-PD (91) "Revised version of proposed clauses for inclusion in a model contract designed to ensure equivalent data protection in the context of transborder dataflows."

The scheme envisages the grant of a licence to use personal data, the licensor warranting the satisfaction of, in effect,[98] the principles of the Council's convention. In return the licensee agrees, in effect,[99] to abide by the data processing principles of the Convention. Both parties agree to permit access and rectification, without excessive expense, by data subjects. This provision seems rather vague in that it fails to specify when rectification can be insisted upon, and what is to count as "excessive" expense. Licensees are required to indemnify licensors in respect of breach of the contractual terms or fault in relation to its subject matter, and there are provisions for compulsory arbitration[100] and termination.

4. Conclusion

While it seems unlikely that the European Community's draft directive will be implemented in its current form, and will perhaps not be implemented in any form for some time, it does give an indication of the direction in which this branch of the law in likely to move in Europe, and one which is likely to have an impact well beyond the boundaries of the Community.

---

98 And in virtually identical terms.

99 And again in virtually identical terminology.

100 An arbitrator is specifically enjoined to resolve disputes by reference to the general principles of data protection as laid down in the Convention, and to take into account any relevant judgement of the European Court of Human Rights.