UIC John Marshall Journal of Information Technology & Privacy Law

Volume 6
Issue 1 *Computer/Law Journal - Summer 1985*

Article 5

Summer 1985

The Legislative Control of Data Processing - The British Approach, 6 Computer L.J. 143 (1985)

Nigel Savage

Chris Edwards

THE LEGISLATIVE CONTROL OF DATA PROCESSING—THE BRITISH APPROACH

by NIGEL SAVAGE*
& CHRIS EDWARDS**

TABLE OF CONTENTS

I. BACKGROUND TO THE LEGISLATION

The Data Protection Act of 1984 ("DPA" or "Act")[1] received the Royal Assent on July 12, 1984, and the United Kingdom thereby joined eight other western European countries[2] that have enacted data protection legislation. In general, the legislation reflects the "European Ap-

* Dr. Savage is Principal Lecturer in Computing Law at Trent Polytechnic, Nottingham, England.

** Dr. Edwards was formerly Professor of Industrial Administration at Carnegie-Mellon University, Pittsburgh, USA. Currently, he is Professor of Management Information Systems at Cranfield School of Management, England.

1. UK Data Protection Act of 1984 [hereinafter cited as DPA], 1 HALSBURY'S STATUTES OF ENGLAND, CURRENT STATUTES SERVICE (Butterworths) 1189 (1984), *reprinted in* N. SAVAGE & C. EDWARDS, A GUIDE TO THE DATA PROTECTION ACT 104-53 (1984).

2. Austria, Denmark, Federal Republic of Germany, France, Iceland, Luxembourg, Norway and Sweden.

proach"[3] to data protection, with a centralist philosophy, namely the creation of a central agency administered by a Data Protection Registrar.

The objectives of the DPA were summarized in the course of the Parliamentary debates on the legislation by the Under-Secretary of State at the Home Office:

> [T]he Bill is drafted to fulfill two purposes. The first is to protect private individuals from the threat of the use of erroneous information about them — or indeed, the misuse of correct information about them — held on computers. The second is to provide that protection in a form that will enable us to satisfy the Council of Europe Convention on Data Processing so as to enable our own data processing industry to participate freely in the European market.[4]

In particular, the legislation enables the United Kingdom to ratify the Council of Europe Data Protection Convention[5] and thereby remove possible impediments to the free flow of data between the United Kingdom and other countries that are party to the convention.

The DPA is concerned only with computer-based information systems. Its provisions draw on a number of government reports and White Papers highlighting the threat to privacy posed by automatic processing.[6] For example, in 1972 the Younger Report[7] argued that the government should seek to ensure compliance with the following ten principles:

1. Information should be regarded as held for a specific purpose and not be used, without appropriate authorization, for other purposes. . . .
2. Access to information should be confined to those authorized to have it for the purpose for which it was supplied . . . .
3. The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose. . . .
4. In computerized 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. . . .

---

3. Burkert, *Institutions of Data Protection: An Attempt at a Functional Explanation of European National Data Protection Laws*, 3 COMPUTER L. J. 167, 169 (1982).

4. 443 PARL. DEB., H.L. (5th ser.) 509 (1983) (statement of Lord Eton).

5. Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Council of Europe, Strasbourg, 28 I. 1981, 1981 Europ. T.S. No. 108.

6. *See, e.g.*, WHITE PAPER, DATA PROTECTION: THE GOVERNMENT'S PROPOSALS FOR LEGISLATION, CMD. NO. 8539 (1982) [hereinafter cited as 1982 WHITE PAPER]; DATA PROTECTION COMMITTEE, REPORT, CMD. NO. 7341 (1978) [hereinafter cited as LINDOP REPORT]; WHITE PAPER, COMPUTERS AND PRIVACY, CMD. NO. 6353 (1975) [hereinafter cited as 1975 WHITE PAPER]; YOUNGER COMMITTEE ON PRIVACY, REPORT, CMD. NO. 5012 (1972) [hereinafter cited as YOUNGER REPORT].

7. YOUNGER REPORT, *supra* note 6.

5. There should be arrangements whereby the subject could be told about the information held concerning him. . . .
6. 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. . . .
7. A monitoring system should be provided to facilitate the detection of any violation of the security system. . . .
8. In the design of information systems, periods should be specified beyond which the information should not be retained . . . .
9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information. . . .
10. Care should be taken in coding value judgments.[8]

The Government's response to the Younger Report was to promise a White Paper, which was delayed until 1975. In it, the Government agreed that "the time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy."[9] The Government proposed that legislation should establish a statutory agency, the Data Protection Authority, to supervise a new legal framework. In order to obtain detailed advice as to the composition of the Authority, a Data Protection Committee was established under the chairmanship of Sir Norman Lindop.[10]

In 1978, the Committee produced the Lindop Report,[11] which proposed that the Data Protection Authority would have the major task of ensuring compliance with a number of data protection principles which would be enshrined in legislation. A particular feature of the Lindop Report was its emphasis on flexibility:

> [A] single set of rules to govern all handling of personal data by computers simply will not do. The legislation must provide a means of finding appropriate balances between all legitimate interests. The scheme of regulation must therefore be a flexible one: flexible as between different cases, different times and different interests.[12]

Consistent with this approach, the Lindop Report proposed that the newly-established Authority should be specifically required to draw up codes of practice, after appropriate consultations with computer users and other interested bodies. The codes would be promulgated by statutory instruments, thus giving them the force of law, and failure to comply with a code would result in the imposition of criminal sanctions.[13] A further task of the Authority would be the establishment and opera-

8. *Id.* at ¶¶ 592-600.
9. 1975 WHITE PAPER, *supra* note 6, at ¶ 30.
10. *Id.* at ¶ 31.
11. LINDOP REPORT, *supra* note 6.
12. *Id.* at ¶ 7.
13. *Id.* at ¶ 12.

tion of a register of data processors. The system of registration would not, however, involve any form of official approval by the Authority; registration would be automatic upon application.[14]

The government's approach to legislative control of data processing was much less rigorous than the approach proposed in the Lindop Report.[15] The government rejected the idea of a Data Protection Authority in favor of a Registrar of Data Protection appointed by the Crown, who "may need a staff of about 20," with the Registrar being responsible for the creation and maintenance of a registrar of "data users."[16] The government also rejected the idea of codes of practice having the force of law. Although they saw "some value in codes of practice in this field" and acknowledged that "organizations may wish to prepare such Codes as a guide to their members," the government did "not consider that these Codes should have the force of law or that it would be practicable, without imposing an unacceptable burden on resources, to cover the whole field of personal data systems with statutory codes of practice within any reasonable timescale."[17] The Government did, however, agree to the imposition of a general duty on 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 date protection principles."[18]

II. THE DATA PROTECTION ACT OF 1984

A. SCOPE OF THE ACT

As stated above, the Act is concerned exclusively with automatically processed information. Consistent with other European countries, the Council of Europe and the European Parliament, the government felt that computers create unique risks to individual privacy. The 1975 White Paper considered that computer operations have five features which pose such a special threat:

(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 accessible from many different points;
(3) they make it possible for data to be transferred quickly from one information system to another;
(4) they make it possible for data to be combined in ways which might not otherwise be practicable;

14. *Id.* at ¶¶ 17, 18.
15. *See* 1982 WHITE PAPER, *supra* note 6.
16. *Id.* at ¶¶ 8-11.
17. *Id.* at ¶ 8.
18. DPA, *supra* note 1, § 36(4).

(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 the records, or what is happening to them.[19]

Arguably, concerns for individual privacy do not justify separate treatment for computer systems. The creation and assertion of privacy rights with respect to personal information ought not to be dependent exclusively on the method of storage. Indeed, by restricting the legislation to automatically processed information,[20] privacy standards can be lawfully evaded by simply transferring sensitive information to manual files.[21]

No constitutional factors inhibiting the extent to which privacy legislation can be extended to all data processing activities exist in the United Kingdom, and the DPA therefore extends to all "data users,"[22] irrespective of whether they are in the private or public sector.[23] The Act defines data users as persons who hold data.[24] A person "holds" data if three conditions exist. First, the data must be part of a collection of data processed, or intended to be processed, by or for the person, on equipment operating automatically. Second, the person must control the contents and use of the data. Third, the data must be in the form in which they will be, or have been, processed.[25] It is therefore not necessary for a person to own, or even see, a computer in order to be a data user. If, for example, the services of a bureau were engaged,[26] then the one engaging those services would become a data user and would be re-

---

19. 1975 WHITE PAPER, *supra* note 6, at ¶ 6.

20. Data Protection Bill of 1983, H.C. Bill No. 51, 1983-84 Sess.

21. [I]t is simply not the case that computerised data files pose the main threat to individual privacy in this country . . . The majority of complaints about personal records which come to the NCCL concern records which are not computerised, such as education records . . .

At a meeting of the Commissioners in London in November 1982, it became clear that, with the exception of Denmark, the Data Commissioners from nine countries were all able — either through specific legislative provision or through administrative policy — to regulate and to deal with complaints about manual records. Many of the Commissioners reported that the majority of complaints which they received concerned non-computerised data. The Austrian Commissioner estimated, for example, that 80% of the complaints he received were of this kind. Similarly, in the USA Privacy Act, no distinction is drawn between manual and computerised systems. In confining this bill to automatically processed data, the British Government is flying in the face of international experience.

National Council for Civil Liberties, 1984 Briefing, ¶ 2.1.

22. DPA, *supra* note 1, § 1(5).

23. *Id.* § 38(1).

24. *Id.* § 1(5).

25. *Id.*

26. A person carries on a "computer bureau" if he provides other persons with services in respect of data, and a person provides such services if—

(a) as agent for other persons he causes data held by them to be processed . . .; or

quired to register under the Act, even though someone else was doing the processing. Therefore, the number of potential data users in the United Kingdom is enormous, including government departments and agencies, nationalized industries, local authorities, corporate bodies, small businesses and even home computer users.[27]

The DPA seeks to give all individuals a number of basic rights with respect to "personal data." Such individuals are referred to under the Act as "data subjects"—that is, anyone who is the subject of personal data.[28] Personal data is defined as information recorded in a form which can be processed automatically and which relates to a data subject who can be identified from it.[29] The definition includes purely factual information and matters of opinion about a given data subject, but not any "indication of the intentions of the data user in respect of that individual."[30] There is, therefore, some room for the astute data user to disguise opinions as intentions and thus frustrate the rights given to data subjects.

B. THE REGISTRAR AND REGISTRATION

The Registrar has a central role to play in this legislative scheme. On a relatively modest budget he is required to initiate and supervise the registration procedure, enforce the data protection principles, advise on the operation of the DPA, and encourage bodies to draw up codes of practice. A particularly important aspect of the Registrar's functions will be dealing with complaints from data subjects and conciliating disputes between data subjects and data users. A case could be made for separating the two functions of standard setting and handling complaints. For example, the Australian Law Reform Commission considered that:

> [A]rguments in favour of separating these functions are that public understanding of the system would be enhanced by keeping grievance handling and standard setting functions separate, and that cooperation with record keepers in the formulation of Codes of Practice would be improved if the Board were not simultaneously dealing with individual complaints against record keepers.[31]

(b) he allows other persons the use of equipment in his possession for the processing . . . of data held by them.

Id. § 1(6).

27. Home computer users are within the subject matter of the Act unless personal data held by them is concerned only with the management of their "personal, family or household affairs or held . . . only for recreational purposes." *Id.* at § 33(1).

28. *Id.* § 1(4).

29. *Id.* § 1(3).

30. *Id.*

31. AUSTRALIAN L. REFORM COMMISSION, DISCUSSION PAPER NO. 14, PRIVACY AND PERSONAL INFORMATION ¶ 180 (1980).

Under the DPA however, the two functions are combined. In the words of the Minister of State at the Home Office:

> [T]he Registrar is in effect the guardian of the data subjects' rights or, perhaps, a Data Protection Ombudsman. It is to him that data subjects will turn if they believe that data users are breaching any of the principles, and it would be for him to uphold their rights by taking whatever action is appropriate, bearing in mind always his duty to promote the observance of the Principles.[32]

Given the relatively small staff at his disposal, the majority of the Registrar's activities and investigations are likely to be initiated by actual complaints from data subjects. The Registrar has the authority to consider any complaint that the data protection principles, or any of the provisions of the Act, have been or are being contravened. Indeed, if the complaint appears to raise a matter of substance, he must consider it.[33] A complaint may be concerned with a data subject's statutory right of access and challenge, in which case the Registrar may simply refer him to the courts. If, however, he receives several complaints about the activities of a given data user, he may decide to investigate the processing activities of the user with a view to serving an enforcement notice.

All data users are required to provide certain information for entry into the register of data users. This register will be open for inspection by the public. A person who is not registered and not exempt from registration is absolutely prohibited from holding personal data. Furthermore, the use or dissemination of data in a manner inconsistent with a registration entry is also prohibited.[34]

Most of the countries in Europe that have data protection laws provide for some form of institutionalized supervision. Some require data users to obtain a license before they can process personal data; the granting of such license is dependent on official approval of the data collection in terms of use, purpose, disclosures and security arrangements.[35] Other systems simply require registration of data users.[36] Such registration implies no official approval of the data collection but renders it legitimate once the application has been made. In these countries, the function of registration is simply to identify systems and facilitate supervision and compliance with standards. The British approach is something of a combination of these two approaches, perhaps

---

32. Report of Standing Committee H on the Data Protection Bill, 12th Sitting, March 15, 1984 (John Hart-Chairman), col. 365, 391.

33. DPA, *supra* note 1, § 36(2).

34. *Id.* § 5.

35. The Swedish system is "usually associated with the licensing approach." Burkert, *supra* note 3, at 176.

36. The German system is "regarded to be the prototype of a substantive approach." *Id.*

favoring the latter.[37]

Under the DPA, data users are required to provide the Registrar with sufficient information to "present an informative picture of their activity."[38] This will include a description of the personal data to be held, the purposes for which it is held or used, the sources from which it is obtained, the person to whom it is disclosed, and countries to which it may be transferred. Once an application has been accepted, the data user may engage in all the activities covered by the application. The Registrar may refuse to accept a registration application only on grounds of insufficient information or non-compliance with the data protection principles.[39] Data users have a right to appeal against such refusal to a specially created Data Protection Tribunal. It is perhaps a measure of the government's priorities in terms of data protection that data users have a tribunal through which appeals can be heard, while data subjects seeking judicial support for their statutory rights against data users are directed to the ordinary civil courts. In the majority of cases, registration will be a mere formality. The 1982 White Paper stated the expectation that most applicants will be registered without question.[40] In essence, the register will serve two purposes. First, it will assist the Registrar in promoting the compliance with the principles by placing the onus on data users to identify themselves and to specify their processing activities. Second, it is intended to serve as an "audit trail" to assist data subjects who wish to track down personal data.

C. Data Protection Principles and their Enforcement

The Act is underpinned by eight principles drawn from the convention. They are expressed in very general terms and for that reason are not enforceable directly through the courts, but instead, indirectly by the Registrar. The principles require that data: are obtained and processed fairly; are held only for specified and lawful purposes; are not used or disclosed in a manner inconsistent with a registration entry; are adequate, relevant and accurate; are not retained longer than necessary; are available for inspection by data subjects; and are protected by appropriate security measures to prevent unauthorized access, disclosure or destruction.[41]

The Registrar has wide supervisory powers to ensure that persons

37. *See id.* at 175-76.

38. Report of Standing Committee H on the Data Protection Bill, 9th Sitting, March 6, 1984 (John Hart-Chairman), col. 253, 264.

39. DPA, *supra* note 1, § 7(2).

40. 1982 White Paper, *supra* note 6, at ¶ 9.

41. *See* DPA, *supra* note 1, § 2, sched. 1.

observe the principles.[42] For example, he may issue an enforcement notice requiring a data user to comply with the principles within a specified time period. Thus, if a data user unjustifiably denies access to data subjects or refuses to correct inaccurate data, and informal persuasion fails, the Registrar may decide to issue such a notice. In the case of gross or persistent contravention, a deregistration notice may be more appropriate. Such a notice would effectively prohibit or limit the processing activities of the data user involved.

The Registrar also has the power to prohibit the transfer of data to a place outside the United Kingdom by serving a transfer prohibition notice on a person. The important factor in transfer border data flows is whether the ultimate destination of the data is a country that is party to the convention and therefore has equivalent data protection laws to those of the United Kingdom. If, for example, a data user wishes to transfer data to the United States, the Registrar may issue a transfer prohibition notice if he believes that such transfer will contravene, or lead to a contravention of, any of the principles. In deciding whether to serve such a notice, the Registrar must consider whether the notice is required to prevent damage or distress to any person. Furthermore, he must have regard to the overall desirability of facilitating the free transfer of data between the United Kingdom and other states and territories.[43]

D. Rights of Data Subjects

The DPA creates four basic rights for data subjects:

> (1) the right of access to personal data; (2) the right to apply to the courts to have inaccurate data rectified or erased; (3) the right to seek compensation for damages suffered where data held is inaccurate; and (4) the right to claim compensation where personal data are lost or where there is unauthorised access.[44]

In the case of a denial of access[45] or a request to rectify inaccurate data,[46] data subjects may choose to file a direct complaint with the Registrar rather than initiate litigation to enforce their rights.

1. *Access and Correction*

The right of access and the right to challenge the accuracy of data are fundamental protections recognized under most systems of data protection. A report to the United States Senate on the subject of criminal

42. *See id.* §§ 10-12.
43. *Id.* § 12(4).
44. *Id.* §§ 21-24.
45. *Id.* § 21(8).
46. *Id.* § 24.

records summarized the rationale behind the principle of access in the following terms:

> First, an important cause of fear and distrust of computerized data systems has been the feelings of powerlessness they provoke in many citizens. The computer has come to symbolize the unresponsiveness and insensitivity of modern life. Whatever may be thought of these reactions, it is at least clear that genuine rights of access and challenge would do much to disarm this hostility.
>
> Second, such rights promise to be the most viable of all the possible methods to guarantee the accuracy of data systems. Unlike more complex internal mechanisms, they are triggered by the most powerful and consistent of motives, individual self-interest.
>
> Finally, it should now be plain that if any future system is to win public acceptance, it must offer persuasive evidence that it is quite seriously concerned with the rights and interests of those whose lives it will record. The Committee can imagine no more effective evidence than authentic rights of access and challenge.[47]

Under the DPA requests for access must be in writing and accompanied by a fee not exceeding the statutory maximum. The requirement to pay a fee is designed principally to cover the operational costs that access imposes on data users and to deter frivolous requests.[48]

Data users are not obliged to comply with a request unless they are supplied with such information as they may reasonably require in order to establish the identity of the person making the request. The requirements imposed by a data user will vary according to the sensitivity of the data. In some cases, it may be sufficient to require the subject to state an account number, whereas for highly sensitive data, specific identifying information, such as a notarized signature, may be sought.[49] Where the data contains information relating to another individual who can be identified from the information, that individual's consent must be obtained. If it cannot be obtained, or if the individual refuses permission, the data user must supply as much of the information as can be supplied without disclosing the identity of the individual.[50]

If access is to be effective in terms of the overall objectives of the

---

47. S. REP. NO. 93-1183, 93d Cong., 2d Sess. 4, *reprinted in* 1974 U.S. CODE CONG. & AD. NEWS 6916, 6936.

48. DPA, *supra* note 1, at 21(2). The fee is expected to be fixed at somewhere between three pounds and eight pounds. In Sweden the law provides that one inquiry per year per individual may be made free of charge. In Germany a fee of ten marks is made, which is refundable if the record is inaccurate. *See* F. HONDIUS, EMERGING DATA PROTECTION IN EUROPE 154 (1975).

49. The Act does not impose criminal penalties on a person who impersonates a data subject. However, such impersonation could attract a prosecution under the Forgery and Counterfeiting Act, 1981, ch. 45, §§ 9(1)(a), 10(1)(c).

50. In general, data users are required to comply with a request for access within forty days. DPA, *supra* note 1, at § 21(6). In the case of examination results not an-

legislation it must involve not only a right to know but also a right to challenge or elaborate information held by a data user. The right to challenge is a common feature of those legal systems that provide protection for information privacy. Indeed, under existing United Kingdom credit law a consumer is entitled to require a credit agency to add to its files a notice of correction.[51] The DPA does not, however, give data subjects a direct right to require data to be corrected. Instead, inaccurate data can be corrected only by taking legal action or by an enforcement notice issued as a result of a complaint to the Registrar. The court also has the power to order data to be erased, but only where data subjects can establish that they have suffered loss due to unauthorized disclosure or access to the data. In addition, there must be a substantial risk of further disclosure or access.[52]

2. *Compensation*

The Lindop Committee recommended that a new civil remedy be introduced for illicit data handling; an individual would be entitled to compensation "for any ascertainable damage which he could prove he had suffered as the foreseeable result of the users automatic handling of personal information about the data subjects in breach of a Code of Practice which applied to such handling."[53] The general law of tort in England gives individuals some protection against the disclosure or misuse of confidential information. There is, however, nothing approaching a general right of privacy.[54]

The DPA introduces two very limited rights to compensation for improper data handling. First, it creates a novel statutory civil liability for the processing of inaccurate data.[55] A defense to such a claim is that the data user took all reasonable care to ensure the accuracy of the data. Thus, the obligation to pay compensation arises only where the data user is at fault. Where the data was received from the data subject or from a third party and it is clear from the data that it was so received, no liability may arise under the DPA. Where a data subject makes a request for access to data and subsequently challenges the accuracy of data provided, an indication of the challenge must be included in the data or in any information extracted from it. A failure to include

---

nounced at the time of the request, the forty-day period commences once the results of the examination are announced. *Id.* § 35.

51. Consumer Credit Act, 1974, ch. 39, § 159(3). Data subjects have similar rights in the United States. Privacy Act of 1974, 5 U.S.C. § 522a(d) (1982).

52. DPA, *supra* note 1, § 24.

53. LINDOP REPORT, *supra* note 6, at 277.

54. *See, e.g.*, Coco v. A M Clark (Engineers) Ltd (1969) RPC 41; Duchess of Argyll v. Duke of Argyll (1967) Ch. 302.

55. DPA, *supra* note 1, § 22.

such an indication may render the data user liable to pay compensation even though he did not originate the data.

The second right to claim compensation provides redress where there has been a breach of the eighth data protection principle. A claim may be made where:

(1) data are lost;
(2) data are destroyed without the authority of the data user;
(3) data are disclosed without authority or access to data is obtained by a third party without the authority of the data user.[56]

A defense to any of the above claims is that the user or bureau took reasonable care to prevent the loss, destruction, disclosure or access in question. The remedy is limited in that it only extends to destruction, disclosure or access that is unauthorized by the data user. If, for example, a data user deliberately discloses data to an outsider causing damage to a data subject, there would be no obligation to pay compensation under the Act. If such a disclosure was to a person not specified in the data user's registration entry the Registrar could exercise his supervisory powers but such powers do not extend to awarding compensation. Restricting the scope of the remedy to unauthorized destruction or disclosure was justified by the government on the grounds that "the concept of paying compensation for damages which results from the dissemination of true information, regardless of any breach of confidence is a novel one which might not be considered solely in the text of automatic processing."[57] Under both claims for compensation the data subject must establish the necessary link between the damage caused and the particular inaccuracy, loss, or disclosure in question. Where damage is established, a claim may also be made for compensation for any distress suffered by reason of the loss, destruction, disclosure, or access to the data. Compensation, however, is not payable for distress alone; data subjects must first establish that they have suffered damage.[58]

E. EXEMPTIONS

The DPA exempts certain data processing activities from some or all of its requirements. There are three general exemptions which apply when:

1. the interests of the state and law enforcement agencies necessitate restricting the application of the Act, wholly or in part, on the

56. "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." *Id.* § 2, sched. 1, no. 8.

57. Standing Committee H. Data Protection Bill, 27 March 1984 col. 494.

58. DPA, *supra* note 1, at §§ 22(1), 23(1).

grounds that otherwise their activities would be prejudiced;[59]

2. the interests of data subjects, or the rights and freedom of others, demand some restrictions on the scope of the Act. For example, it may be permissible to deny access to an individual's medical records;[60] or
3. the data poses no threat to individual privacy. For example, payroll and accounting data held and used only for calculating remuneration or keeping records of transaction are exempt.[61] Such data are normally held as part of a contractual relationship between data user and data subject and its accuracy may be monitored through the receipt of invoice, etc.

III. COMPLIANCE PROBLEMS FOR DATA USERS

Although the DPA is being gradually implemented over a period of three years, its provisions are already presenting problems for large-scale corporate data users. As part of the registration process, data users are required to identify categories of data held, the use and purpose for which data are held, and any disclosures. Until now most organizations have exerted little control over the growth of information systems. Indeed, the trend has been in favor of "end user computing" which implies less central control of processing, allowing all personnel greater access to mainframe and microcomputer systems. For example, the sales representatives might use a microcomputer to process personal data on his clients' purchasing patterns or particular weaknesses without the knowledge or consent of his employer. In such circumstances the employer might be regarded as the data user and would therefore be required to include that data within his registration entry.[62]

In practice, therefore, the DPA requires organizations to exercise greater influence and control over the development of systems. In the same way that all organizations create a structure of authority as to who can transact on behalf of the organization, they are now required to initiate similar procedures with respect to processing personal data. In addition, there must be procedures for identifying new uses or pur-

---

59. For example, the Act provides that:

> [P]ersonal data held for any of the following purposes —
>
> (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,
>
> are exempt from the subject access provisions in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

Id. § 28(1).

60. *Id.* § 29(1).

61. *Id.* § 32.

62. On the other hand, the employee could be regarded as the data user and the employer a person carrying on a computer bureau.

poses for which data are held, as well as for controlling disclosures of personal data to outsiders.[63] The beneficial impact of the legislation is that organizations are required to undertake an information inventory, thus recognizing information systems as an organizational asset. In the same way that the use of other assets is periodically subjected to scrutiny, the information system will be required to be audited in reference to the data protection principles in order to ensure compliance with the DPA.

CONCLUSION

Once the DPA is fully implemented it should enable the United Kingdom to ratify the Council of Europe Data Protection Convention. Whether or not the legislation achieves its other objective, that of safeguarding the interest of data subjects, remains to be seen. Much will inevitably depend upon the attitude of the Registrar in terms of the standards of compliance that are set for data users and his willingness to support complaints by data subjects against delinquent data users. As Burkert observes:

> [T]he necessities of technology law demand wide agency discretion. Courts and administrative agencies always exercise discretion when they interpret law, but the margin in this area is relatively broad, the power of the agencies is relatively strong, and the area in which these agencies operate is extremely important because of its infrastructural character.[64]

A particularly significant area will be the level of detail provided by data users in describing, for registration purposes, the data they hold and its use or purpose. If the system of registration is to be of any real value to the Registrar in monitoring compliance with the principles, it must be reasonably specific in identifying use and purpose. Similarly, if it is to be of genuine assistance to data subjects in offering clues to where personal data on them is likely to be held, the information provided will need to be fairly specific. The great value of the DPA, initially at least, will be in generating greater awareness of the problems inherent in the growth of information systems and the need to exercise some control over the creation and use of such systems. While it does not solve all problems, the legislation does at least create a legal framework of basic rights for individuals upon which the legislature and the judiciary can build.

---

63. It is permissible for a data user to disclose data to his servant or agent for the purpose of enabling the servant or agent to perform his functions. DPA, *supra* note 1, § 34(6)(c).

64. Burkert, *supra* note 3, at 187.