Article

« Citizen's Privacy and Data Banks : Enforcement of the Standards in the Data Protection Act 1984 (U.K.) »

Jeremy McBride

Les Cahiers de droit, vol. 25, n° 3, 1984, p. 533-552.

Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (U.K.)

Jeremy McBRIDE *

En 1981, le Royaume-Uni ratifiait la Convention européenne pour la protection des individus relativement aux fichiers personnels informatisés. Le Parlement vient de donner effet à cette convention en droit interne en adoptant le Data Protection Act, 1984. *Le présent article a pour but de critiquer les points saillants de cette Loi, et en particulier l'institution du Registraire. L'auteur met l'accent sur les droits fondamentaux protégés par la Loi, ses mécanismes de mise en œuvre ainsi que sur les différents recours que peuvent instituer les citoyens en vertu de cette Loi.*

Pages

Introduction 533

1. **The 1984 Act and the Data Protection Principles** 536
2. **The Enforcement Machinery** 538
3. **The Scope for Judicial Review of the Registrar's Decisions** 550

Introduction

The *Data Protection Act* has just completed its second journey through the parliamentary processes (the first attempt was interrupted by the dissolution of Parliament for the general election last year) [1]. In the course of

* Lecturer, Faculty of Law, University of Birmingham.

1. The first *Data Protection Bill* was introduced in the House of Lords on 21st December 1982 and the second on 23rd June 1983.

Les Cahiers de Droit, vol. 25, n° 3, septembre 1984, p. 533-552

its progress through Parliament, there was hardly any change to the enforcement provisions proposed by the government and the criticism levelled at them was relatively muted. The controversy which has surrounded what is now the Data Protection Act has been primarily concerned with its substantive provisions — what sort of data is to be protected and against what the protection is required, as well as the question of what exemptions from the Act's provisions should be permitted [2]. It is not intended to go into this area but it is necessary to say something about the background to the Act as that does afford some explanation for the enforcement scheme that has been adopted.

In essence, the story of data protection in the U.K. is one of marked reluctance by the government to act even thought the problems had been identified as long ago as the 1950s and early 1960s, with attempts in the House of Lords to introduce general privacy legislation [3]. As concern grew, the Younger Committee was set up to examine the need for legislation against intrusions into privacy by private persons. In the area of data protection it favoured building upon existing concepts with the addition of a new wrong of unauthorised disclosure but no legislation was forthcoming [4]. The widespread introduction of computers gave rise to much greater concern and with the Lindop Committee in 1978, there was a thorough examination of the problem of data protection itself as opposed to the previous more generalised studies of the protection of privacy [5]. This Committee was also concerned with both public and private records, a recognition that the threat came from government as well as other individuals and private corporations. Lindop recommended the establishment of an authority to regulate the storage and disclosure of personal data. It took the view that the burden of enforcement should not be on the individual who would not have sufficient expertise and resources [6]. In particular it wanted a body with wide powers of investigation, to call witnesses and documents, and it would have been able to find breaches of the relevant standards, require change of practice and seek injunctions for this purpose, where necessary, and it would also have had the power to prosecute data users who did not take the appropriate action. The scheme was envisaged as being preventative rather than remedial and it made only limited proposals for civil actions by the data subject himself. It considered that with the « careful administration and the enforcement » of its scheme it would be unusual for a

2. See, for example, the N.C.C.L. Briefing Paper, *Data Protection Bill 1983*, London, 1983.
3. See, R. Wacks, *The Protection of Privacy*, London, 1980, p. 4–10.
4. *Report of the Committee on Privacy*, Cmnd. 5012 (1972) (Chairman : Kenneth Younger).
5. *Report of the Committee on Data Protection*, Cmnd. 7341 (1978) (Chairman : Sir Norman Lindop).
6. *Id.*, c. 19.

data subject to suffer damage. The Committee proposed, however, that a data subject should be able to recover compensation from a user for any ascertainable damage which he could prove he had suffered as the foreseeable result of the user's automatic handling of personal information about the data subject in breach of the relevant Code of Practice [7].

These proposals were not, however, met by any government initiatives and indeed after the customary period of consultation required following the production of a report by a committee which had canvassed views widely, there was then a government in power which had no sympathy with independent administrative agencies or quangos. Although procrastination became the order of the day, legislation ultimately proved impossible to avoid: a consequence of developments within the Council of Europe which galvanised the computer industry in the U.K. into calling for reform in an unholy alliance with the National Council for Civil Liberties. Although the right to privacy is protected by Article 8 of the Council of Europe's *European Convention on Human Rights* there has been no significant case-law developments in this area and in any event this was seen as a subject requiring a special treaty, which was adopted in 1981: the *European Convention for the Protection of Individuals with regard to the automatic processing of Personal Data* [8]. As a member of the Council of Europe there would be informal pressure on the U.K. to ratify it, but more significantly the fact that many other European countries were prepared to ratify it was the cause of considerable concern for the computer industry in this country; the Convention (as well as a number of domestic laws of European states predating it) does not permit transborder flows of data to countries which do not have any comparable data protection legislation [9]. These developments were a serious threat to the data processing industry and legislation was thus essential if their commercial interests were to be protected. The Act purports, therefore, to implement the provisions of the Convention — a necessary preliminary to ratification by the U.K. — but at most it is an attempt only to do the minimum required. This is true of the exemptions permitted; the unwillingness to take up the option to apply the proposed protection to manual files as well as to computerised or automatic systems [10] and it may also be an appropriate comment in the enforcement machinery which is going to be established.

The Act has established the office of a Data Protection Registrar (rather than an Authority but the constant reassurance has been that he will be a

7. *Id.*, c. 33.
8. E.T.S. No. 108 (1981).
9. *Id.*, art. 12.
10. *Id.*, art. 3(2)(c).

person of distinction) who will have a number of specific powers over those who use information kept on automatic systems and the backing of these powers with a criminal sanction certainly gives the impression that they have substance. Another initial impression is that there should be simplicity of operation in marked contrast to bodies such as the Equal Opportunities Commission (EOC) and the Commission for Racial Equality (CRE). The Registrar can do more than they can and the terms in which he is given the power to act do not include any express reference to the sort of preliminaries to action which have slowed down and entangled the CRE [11]. The appearance of simplicity may, however, be deceiving both in that it will not prevent constraints being read into the legislation and that there is actually an inadequate power base on which he can act. Thus it is quite possible that some « due process » limitations will have to be read into the Registrar's powers, although what exactly these will be will have to await the outcome of challenges to their exercise some time in the future. Moreover, the relative simplicity of the terms in which the Registrar's powers are expressed — saying generally that he can act when « satisfied » about a particular matter but without having any express provision about how that state of satisfaction is to be attained — may actually mean that he does not have appropriate investigative powers to be able to invoke his formidable enforcement powers. Furthermore the Act does contain a degree of jurisdictional complexity which may prove a hindrance in the long term; thus there is a tribunal system for appeals against decisions by the Registrar; the criminal courts will be used where those decisions are not respected but the ordinary civil courts will be the forum for the victim of any violation of the standards laid down by the Act; and there is also a good chance that the Divisional Court may also be involved as judicial review by the person using the data or by the person who is the subject of the data is by no means out of the question.

1. The 1984 Act and the Data Protection Principles

The Act is concerned with personal data, that is data consisting of information relating to a living individual who can be identified from the information, including any expression of opinion about the individual [12]. For the purposes of the Act the individual is referred to as the « data subject » and the person holding the data is the « data user » [13]. Although we are not

11. See, G. Applebey, « The Commission for Racial Equality and the "Spiders Web" », (1982) 1 *C.J.Q.* 301.
12. S. 1(3).
13. S. 1(4) and (5). The Act also applies to those who provide data processing services for others in what are termed a « computer bureau » ; s. 1(6).

concerned with the applicability of the standards protecting such data — there are broad exemptions for national security and the police as well as matter relating to the appointment of the judiciary[14] — it is important to bear in mind the standards themselves — known as the « data protection principles », because their observance is what the enforcement machinery should have as its goal and should, therefore, actually be capable of achieving. The principles themselves follow the Council of Europe Convention and in general terms embody the standards usually considered appropriate in this area. The data protection principles are set out in the First Schedule and are as follows :

1. information should be obtained lawfully and be processed fairly and lawfully ;
2. it should only be held for one or more specified purposes ;
3. it should not be used or disclosed in a manner incompatible with that purpose or purposes ;
4. it should be adequate, relevant and not excessive in relation to the specified purpose or purposes ;
5. it should be accurate and kept up to date ;
6. it should not be kept longer than necessary ;
7. an individual should be entitled to know whether data is held about him, to have access to it and, where appropriate, to have it corrected or erased ; and finally, in the case of people running computer bureaux ;
8. there should be adequate security measures.

Some elaboration of these principles is given in the second part of the schedule — a form of authoritative interpretation and although helpful, this is unlikely to eliminate the problems of applying the principles in particular situations[14a].

If these principles are to be observed by all data users — and it should be said that some already do respect them voluntarily — then there has to be an effective mechanism for checking the contents and use of data systems. The scale of the problem is vast and part of it is not actually knowing how many systems there are — estimates vary from the Home Office's cautious 80 000 to other estimates which may seem extravagant, varying as they do between 300 000 and half a million, but which in reality may be quite

14. S. 26–35.

14a. The principles can also be modified by the Home Secretary to provide additional safeguards in relation to personal data concerning the data subjects racial origin, political opinions, religious or other beliefs, physical or mental health or sexual life and criminal convictions ; s. 2(3).

accurate given the very high level of computer sales in the U.K.[15] Whatever the figure, it is unlikely that most data subjects will have the enthusiasm or the tenacity to use the access provision to discover the information held about them or to bring civil proceedings against those discovered to have violated the data protection principles. It would be almost impossible for any individual to calculate who might have information about him; in most cases anyway it is only likely to become an issue of importance to the individual when an adverse decision is taken in respect of him and the explanation, which may not actually be given to him, is that it was on the basis of information obtained or held by the decision-maker. If he gets to know of it then he might want a remedy but it is much more likely that he won't get to know of it, and in any event, if the data protection principles were being observed then the problem should not have arisen.

In view of the nature and scope of the problem, the Lindop Committee was surely right to concentrate on the preventative as opposed to the remedial action that should be taken, without, of course, ruling out individual remedies in particular cases. The *Data Protection Act* undoubtedly embodies this bifurcated approach but the civil remedies for the individual may have a larger role in data protection than might be imagined, although this is still very much a case of crystal-ball gazing as the Act's actual entry into force remains uncertain. This is because the date of commencement is left to be determined by the Home Secretary and even then the enforcement powers will not generally become operational until some two years after that[16].

2. The Enforcement Machinery

Under the Act, the introduction of a registration requirement for all data users covered by its provision is the crucial first stage of the enforcement scheme[17]. The register will contain the name and address of the data user; a description of the data and the purposes for which it is held; a description of the sources from which it is or will be obtained; a description of the persons to whom it may be disclosed; the countries to which it may be transferred and the address for the receipt of requests from data subjects for access to the data. It is an offence to hold such personal data without being registered or to disregard any provisions about the use of the data given in the register, e.g. to hold data other than that specified or to use it for an unspecified

15. House of Commons Standing Committee H, *Data Protection Bill*, Eighth Sitting, 1 March 1984, col. 233.
16. S. 42.
17. S. 4 and 5.

purpose [18]. The register will thus be the starting point for any individual seeking to learn about the data systems which may contain information about him and will also be the starting point for the monitoring activities to be undertaken by the Registrar.

The register has to be available for inspection by members of the public at all reasonable hours without charge although a charge can be made for a certified copy of the particulars contained in an entry in it [19]. It is possible to update one's entry in the register [20] and in any event entries must be renewed periodically — the precise period will be fixed by the Home Secretary but it will not be less than three yearly intervals [21]. Registration is not, however automatic; the application can be accepted or rejected by the Registrar, but he can only do the latter where (a) he considers that the particulars proposed for registration will not give sufficient information as to the matters to which they relate; or (b) he is satisfied that the applicant is likely to contravene any of the data protection principles; or (c) he considers that the information available to him is insufficient to satisfy him that the principles are not likely to be contravened [22].

In addition to his power over registration, the Registrar is also given a number of supervisory powers to ensure that the data protection principles are being observed by data users whose applications for registration have been accepted, namely the power to issue enforcement, deregistration and transfer prohibition notices.

The Registrar can serve an enforcement notice if he is satisfied that a registered person has contravened or is contravening any of the data protection principles and this notice can require him to take, within such time as is specified in the notice such steps as are so specified for complying with the principle or principles in question [23]. There must clearly be a relationship between the steps and the principles but the section seems to leave it to the Registrar to work out what are appropriate steps, although it does state that where it is a matter of inaccuracy the Registrar can require rectification or erasure of the data concerned, or the addition of a statement that the data subject regards the information as incorrector misleading, and where it is a case of the access principle not being observed then he must be satisfied that a request has actually been refused [24]. In deciding to serve the

18. S. 5(5). The restrictions also apply to the servants and agents of the data user; S. 5(3).
19. S. 9.
20. S. 6(3) and (4). It is also an offence for the data user not to apply for the updating of his address or to supply false or misleading information; S. 6(4) and (5).
21. S. 8.
22. S. 7.
23. S. 10.
24. S. 10(3) and (4).

notice he must consider whether the contravention has caused or is likely to cause any person damage or distress and the notice must state the principles he is satisfied have been or are being contravened and his reasons for reaching that conclusion [25]. It is an offence not to comply with an enforcement notice although it is a defence to prove that one exercised all due diligence to comply with it [26].

If the Registrar is satisfied that the principles have been or are being contravened and that compliance cannot be adequately secured by the service of an enforcement notice then he can serve the registered person with a deregistration notice, notifying him that he will remove the particulars concerning that person from the register at the end of a specified period [27]. Again the Registrar must consider whether the contravention has caused or is likely to cause damage or distress to any person and he must state the principles being contravened and his reasons for reaching that conclusion and deciding that compliance cannot be adequately secured by the service of an enforcement notice [28]. The effect of deregistration is, of course, to make the holding and use of the data by the data user a criminal offence.

Finally the Registrar can issue what is known as a transfer prohibition notice where it appears that a data user proposes to transfer personal data to a place outside the U.K. and he is satisfied *either* that the transfer is likely to contravene or will lead to a contravention of the data protection principles if the place is a country not a party to the Convention *or*, in the case of a country party to the Convention, that there will be a further transfer to another country not a party and the principles will be contravened or a breach of any additional principles that the Home Secretary has laid down relating to the racial origin of the data subject, his political opinions or religious or other beliefs, his physical or mental health or his sexual life or his criminal convictions [29]. In issuing the notice, which will prohibit any transfer either absolutely or until steps specified in the notice are taken, the Registrar must again consider whether it is needed to prevent damage or distress to any person and must also have regard to the general desirability of facilitating the free transfer of data between the U.K. and other states and territories [30]. The notice must specify the time when it is to take effect and contains the principles which the Registrar is satisfied are likely to be

25. S. 10(2) and (5).
26. S. 10(9).
27. S. 11.
28. S. 11(2) and (3).
29. Cl. 12. See fn. 14a *supra*.
30. S. 12(4).

contravened and his reasons for reaching that conclusion [31]. It is an offence not to comply with the notice, although there is again a defence of proving that one exercised all due diligence to avoid a contravention [32].

All refusals of registration and all notices, enforcement, deregistration and transfer prohibitions, served by the Registrar must contain particulars of the data users' rights of appeal to the Data Protection Tribunal [33]. In general no refusal or notice will take effect during the period in which an appeal can be lodged or while an appeal is considered, although in cases or urgency, the Registrar can specify that his decision must not be so suspended and in such cases it will take effect seven days after the refusal of registration or the service of the notice [34].

The Tribunal will consist of a legally qualified chairman and an equal number of persons to represent the interests of data users and person to represent the interests of data subjects [35]. Where the Tribunal considers that the refusal or notice against which the appeal is brought is not in accordance with the law or, to the extent that the refusal or notice involved an exercise of discretion by the Registrar, that he ought to have exercised his discretion differently, the Tribunal shall allow the appeal or substitute such other decision or notice as could have been made or served by the Registrar and in any other case it shall dismiss the appeal [36]. The Tribunal is empowered to review any determination of fact on which the refusal or notice in question was based, and it can also hear appeals simply against the Registrar's statement in a refusal or notice that his decision must take effect as a matter of urgency and thus cannot await the outcome of an appeal, such cases clearly putting the data user in a very bad light [37]. It is possible for the Registrar or the data user to appeal from the Tribunal on a point of law to one of the superior courts, that is the High Court, in England and Wales, the Court of Session in Scotland and the High Court in Northern Ireland [38].

The Registrar thus has, in theory, a formidable array of powers but before examining them a little more closely it is important to mention something about prosecution for offences contrary to the Act and the remedies that can be pursued by data subjects as these also have a bearing on the effectiveness of enforcement. As is apparent from what has been said, the

31. S. 12(5).
32. S. 12(10).
33. S. 10(5)(b), 11(3)(b) and 12(5)(b).
34. S. 10(6) and (7), 11(4) and (5) and 12(6) and (7).
35. S. 3(3)-(6) and Sched. 3, para. 2(1).
36. S. 14.
37. S. 14(2)-(4).
38. S. 14(5).

enforcement powers of the Registrar are clearly tied to the criminal sanction ; a failure to registrar, operation after deregistration and failure to comply with an enforcement or transfer prohibition notices are all criminal offences. The power of prosecution is vested in the Registrar or the Director of Public Prosecutions [39] and the fact that the Registrar can back his initial assessment that there is or is likely to be a contravention of the data protection principles with a criminal prosecution could prove to be an important and even decisive incentive to compliance.

Whether this actually works out in practice will depend very much on whether he shows an early willingness to use his muscle in an appropriate case ; such a display of force may not actually be forthcoming as formal decisions by the Registrar may not be taken for some time, since as shall be seen it is certainly intended that he enter into negotiations with data users and in any event may not have much choice to do otherwise, and as a refusal or a notice is a prerequisite to prosecution the criminal sanction may appear less intimidating in practice. It may also be undermined by the staffing contraints under which he is likely to operate, at least at the outset. It is envisaged that he will only have twenty support staff and given their other duties this may not be sufficient [40].

A further problem that prosecutions may give rise to is that this will produce another forum in which the Act and the Registrar's exercise of power will be examined, although non-compliance is to an extent a factual matter. It is not improbable that the validity of the Registrar's acts will be impugned and this will not be impermissible, at least where the appellate system has not been used.

The data subject is given a number of specific rights by the Act but, apart from inspection of the register itself [41], they are to be enforced in the ordinary civil courts and not in the Data Protection Tribunal. It may seem strange to set up a specialised tribunal, manned by those interested in the use of computers, and then not to use it, at least in the first instance, for all disputes raising issues of data protection. Of course, it is not uncommon for disputes raising fundamentally the same issue of principle but about different factual situations to be assigned to different jurisdiction (e.g. discrimination in relation to employment is dealt with the industrial

39. S. 19.(1) ; persons convicted of any offence under the Act are liable to a fine and the court can also order data material connected with the commission of an offence to be forfeited, destroyed or erased ; S. 19(2)-(5).

40. House of Commons Standing Committee H, *Data Protection Bill*, Eighth Sitting, 1 March 1984, col. 249.

41. S. 9.

tribunals but in relation to other matters is considered in the County Court) but here the difference in forum turns on the question of whether one is the data user or data subject. The Tribunal is seen as the preserve of the user and the Registrar, and while the proposed amendment that a subject as well as the Registrar could appeal against a Tribunal decision in favour of the user was rejected on the logical if not convincing ground that the Registrar was acting on behalf of the subject and it would be strange to allow the latter an appeal [42], it would probably have made more sense for the Tribunal to hear the claims that the subject is entitled to make.

Under the Act he is entitled to be informed by any data user whether the latter holds data on him, and to have a copy of it [42a]. A fee can be charged (to be fixed by the Secretary of State) and if a user has more than one entry in the register then separate requests (and fees) have to be made for each one [43]. The user can require sufficient information to satisfy himself as to the identity of the data subject and to be able to locate the data [44]. He can also refuse to give information where it will disclose information about someone else, even if it is just that the person is the source [45]. Otherwise the request must be satisfied within 40 days and if a court is satisfied that this has not been done, it can order the data user to do so unless it considers that the request is unreasonable (e.g. too frequent a demand) [46]. Having got the information a number of other rights might need be exercised. Thus the data subject has an action for compensation where he suffers damage by reason of the inaccurary of the data, that is it is incorrect or misleading as to any matter of fact [47]. If the data has been obtained from a third person or the data subject then compensation is not payable if the data indicates that it was so obtained and, where the data user has been so notified, that the data subject regards it as incorrect or misleading [48]. A data user can thus evade the responsibility of checking the accuracy of data obtained from others and any liability for damages by simply indicating that it was obtained from someone else. It is also a defence to prove that one has taken such care as in all the circumstances was reasonably required to ensure the data's accuracy at the material time [49].

42. House of Commons Standing Committee H, *Data Protection Bill*, Twelfth Sitting, 15 March 1984, cols. 391-392.

42a. S. 21.

43. S. 21(3).

44. S. 21(4).

45. S. 21(4)(b) and (5).

46. S. 21(6) and (8). The court has the power to inspect the data before making its determination but discovery of the data is not available to the data subject; S. 25(2).

47. S. 22.

48. S. 22(2).

49. S. 22(3).

A data subject can also recover compensation where he suffers loss by reason of the loss of the data or the destruction or the disclosure of the data, or access having been obtained to the data, without the authority of the data user and there is again the defence of all reasonable care being taken [50]. However, the court can order the erasure of the data where it is satisfied that there is a substantial risk of further disclosure of or access to the data without the user's authority [51]. Finally, the data subject can apply to the court for the rectification or erasure of data that is inaccurate, including any expression of opinion which appears to be based on the inaccurate data. However, in the case of data obtained from the data subject or a third party which complies with the requirements of section 22(2), namely, an indication that it was so obtained and that, where appropriate, the data subject regards the information as incorrect or misleading, the court may instead make an order requiring the data to be supplemented by such statement of true fact, relating to the matters dealt with by the data as the court may approve. If the requirements of section 22(2) have not been complied with then, instead of an order for rectification of erasure, the court can make such order as it thinks fit for securing compliance with those requirements, with or without a further order requiring the data to be supplemented by a statement of the true Facts which it has approved. [52]

The range of civil remedies, although greater than that proposed by Lindop, does not actually cover all the data protection principles. Thus there is no provision for compensating information obtained unlawfully or for erasing it. Nor is there provision for compensating or preventing the further use of data for an unregistered purpose. Nor for the authorised but improper disclosure of information. Nor for dealing with data users whose holding of data is not adequate or relevant or is excessive or is held for longer than necessary.

However the Home Office do not seem in any way embarrassed by this; indeed it is claimed that this is an intentional approach to the problem, it being felt that the existing civil remedies would cover those situations for which no new action is being created and would be entirely adequate for that purpose [53]. The particular actions suggested as useful are defamation, breach of confidence and of contract and negligence. This attitude certainly

50. S. 23.

51. S. 24(3); but in the case of data held by a computer bureau for someone else, the court must first take such steps as are reasonably practicable to give that person an opportunity to be heard.

52. S. 24(1) and (2).

53. House of Commons Standing Committee H, *Data Protection Bill*, Fifteenth Sitting, 27 March 1984, cols. 499-500.

supports the logic of making the data subject use the ordinary courts but is a little disingenuous as the scope of breach of confidence in particular is still uncertain and the Law Commission's proposals are not in process of being enacted [54]. Moreover, none of these actions will help deal with problems of adequacy, relevance, excessiveness or prolonged retention. It is also a little hollow to claim that there is no need for a civil remedy to deal with the holding of unregistered data as this is likely to be the beginning of all the data subject's problems. However, given that the holding of unregistered data is an offence, the data subject might, where the Registrar or the D.P.P. is unable or unwilling to prosecute the data user, be able to obtain an injunction to restrain its commission; at least there was some sympathy for this in the *Gouriet* case, where someone has actually suffered injury as a result of a breach of the criminal law [55].

In the House of Commons Standing Committee on the Bill there was some concern about the absence of any express reference in the provisions to compensation for injury to feelings, particularly since the exercise of the Registrar's powers were conditioned on the likelihood of damage or distress to a data subject but the civil remedies only referred to damage [56]. At first reassurance that the civil law now covers such injury was accepted but at the Report stage amendments were adopted allowing anyone suffering damage as a result of inaccuracy, loss or unauthorised disclosure or destruction to recover both for the damage and any distress suffered [57]. This formulation is designed to prevent the court from being overwhelmed by "speculative" actions for distress alone [58].

It might be desirable to have awards of punitive or exemplary damages, particularly in instances where there is oppressive handling or misuse of personal data by public officials but given that the sections only create a right to compensation this does not seem to be a possibility.

In the data subject's civil proceedings, information about the data user dug up by the Registrar may prove to be most helpful but it will not always be available. It will be available where there has been a conviction for non-compliance with a notice served by the Registrar but the notice itself, despite the inclusion of reasons, is not going to be admissible although future

54. *Breach of Confidence*, (Law Com. No. 110) Cmnd. 8388 (1981).

55. *Gouriet v. Union of Post Office Workers*, [1978] A.C. 435.

56. House of Commons Standing Committee H, *Data Protection Bill*, Fifteenth Sitting, 27 March 1984, cols. 477–488.

57. S. 22(1) and 23(1).

58. H.C. Debs., 5 June 1984, cols. 225-9. *Cf.* The Race Relations Act 1976, S. 57(4) and the Sex Discrimination Act 1975, S. 66(4) which allow compensation to be awarded solely for injury to feelings.

compliance might be evidence of an earlier default [59]. This also assumes that the Registrar even decides to serve a notice — he may gather evidence but decide that a notice is not necessary. It is unlikely that any evidence so gathered could be obtained through discovery [60].

Given the incompleteness of the remedies open to data subjects themselves and the more general observations that have already been made about individuals wanting or being able to track down abuses by data users, the Registrar should be the more significant enforcer of the data protection principles. As the Home Officer Minister, David Waddington put it, the Registrar is the guardian of the data subject [61] and it is to a number of uncertainties about his powers which must now be further examined. In the first place, what exactly does the Act mean by the Registrar being « satisfied » about certain matters before exercising his powers? How is he to be satisfied? Closely connected with this is the extent to which the Registrar will be able to investigate individual complaints by data subjects and what criteria he will use in doing so. Another uncertainty associated with the exercise of his powers, is the extent to which the principles of natural justice will have to be observed by the Registrar in relation to the data user — there is no express provision on this and yet his powers clearly can have a considerable impact on the business operations of the data user. Finally, arising out of all of these is the extent to which the Registrar's decisions can and will be subject to judicial review at the behest of either the data user who feels he has gone too far or of the data subject who feels he has not.

Apart from the Registrar's decision to refuse registration because he considers that the proposed particulars do not give sufficient information or because he considers that he has insufficient information to satisfy him that the data protection principles are unlikely to be contravened, all his powers are conditioned upon him being « satisfied » about a certain state of affairs: whether it is that the applicant is likely to contravene any of the data protection principles or that he has contravened them or that an enforcement

---

59. House of Commons Standing Committee H, *Data Protection Bill*, Sixteenth Sitting, 27 March 1984, cols. 508–511.

60. *Norwich Pharmacal Co. v. Customs and Excise Commissioners*, [1974] A.C. 133 where the Registrar's investigations are the result of a complaint his only obligation to the complainant is to notify him of his proposed course of action (s. 36(2)) but some information might emerge in a challenge to his refusal to take enforcement action; see Part 3 *infra*. A clause requiring the Registrar to notify data subjects libely to have suffered damage by reason of contraventions he has established was resisted as too onerous and withdrawn; House of Commons Standing Committee H, *Data Protection Bill*, Twenty-fifth Sitting, 26 April 1984, cols: 847–850.

61. House of Commons Standing Committee H, *Data Protection Bill*, Twelfth Sitting, 15 March 1984, col. 391.

notice is insufficient to stop further contraventions of them or that a transfer of data out of the country is likely to contravene or lead to a contravention of those principles. It is fair to assume that « satisfied » for these purposes means satisfied on the balance of probabilities as that is generally accepted as the appropriate standard for such decisions by administrative bodies but this only tells us about the level of evidence for a particular conclusion, and it should be said that the Act's provisions are exemplary in requiring the Registrar always to give reason to the data user for the conclusions he has reached. This requirement of reasons, of course, assumes that the Registrar will be able to find reasons and yet this is the very aspect of the Registrar's powers on which the Act is virtually silent. There is no express provision governing investigations into possible contraventions, except in response to individual complaints and in no case can he summon witnesses before him upon pain of contempt or even demand documents. That is not say that he cannot investigate possible breaches, it is just that his coercive power to do so is minimal. The only express power that he is given is tucked away in a schedule — a demotion as the original Bill had it in the main body of its provisions[62]. Schedule 4 gives the Registrar certain powers of entry and inspection for the purpose of detecting offences and contraventions of the data protection principles. He has to satisfy a circuit judge that there are reasonable grounds for suspecting an offence or contravention and that evidence of it will be found on specified premises and if the judge is satisfied a warrant will be issued authorising him or his servants to enter and search the premises, to inspect, examine, operate and test any data equipment and to seize any documents or other material which might be evidence. However, no warrant will be issued, except in cases of urgency or where the object of entry would be defeated, unless the Registrar has first given 7 days notice in writing to the occupier of the premises demanding access, that access was for a reasonable hour and was unreasonably refused and that the occupier has, after refusal, been notified by the Registrar of the application for the warrant and has had the opportunity of being heard by the judge on the question of whether or not it should be issued[63].

Although any power of entry, search and seizure is a considerable intrusion of privacy and denotes the importance of the objectives of the body so empowered, in the present instance it is remarkable more for the politeness of and caution demanded of the Registrar than of any substantive power of investigation. In any event, the Registrar is going to need information even to go to a circuit judge to get a warrant. Undoubtedly a legitimate consideration for the Registrar will be communications that he

62. Cl. 16 of the original Bill.
63. Schedule 4, para. 2.

receives from individual data subjects — but will he be able to rely on these alone? He may, of course, ask a data user to comment on allegations that have been made to him but the user is not obliged to answer his questions — the only time that he is at the renewal of registration. It might well be legitimate to refuse renewal on the basis that he had insufficient information because the user has not answered allegations from data subjects that have been put to him and therefore the Registrar could not be satisfied that the user is unlikely to contravene the data protection principles [64].

In respect of the Registrar's other powers, however, it remains to be seen whether allegations by data subjects which have not led the Registrar to apply for a warrant to search for evidence could alone be sufficient to satisfy him of a breach or continued breach of the data protection principles. Presumably such allegations would be sufficient to justify a circuit judge issuing a warrant but if the Registrar cannot issue enforcement and other notices without first obtaining one then the enforcement machinery is going to be very slow indeed. This is, however, probably what the Home Office intends as there has been much play of the need for the Registrar to negotiate and to be flexible, for there to be give and take with the data user. Certainly, if the Registrar is going to have to negotiate from this relative position of weakness, the data user will not feel stampeded into implementing the data protection principles in a hurry. On the other hand, if it were accepted that a refusal by a data user to answer an allegation by a data subject could justify the Registrar being satisfied then there would be scope for a more assertive policy of enforcement. This was the approach the Home Officer Minister thought he would take — if the answer to a complaint is unacceptable then the Registrar will threaten to serve an enforcement notice — but there is clearly going to be scope for disagreement about what is unacceptable and thus resort to judicial review [65]. If the data user were to enter into discussions, providing evidence against the allegation then the Registrar might find it more difficult to be satisfied unless he was prepared and was able to convince a circuit judge to give him a warrant to search for evidence in the user's premises.

It is possible that action by the Registrar will always be prompted by communications from data subjects, but given that many of them will not be aware of the files kept on them it is even more unlikely that they will be

64. S. 7(2) (c). A clause imposing a duty on the data user to furnish information required by the Registrar was considered to threaten the privilege against self-incrimination; House of Commons Standing Committee H, *Data Protection Bill*, Twenty-fifth Sitting, 26 April 1984, cols. 850–854.

65. House of Commons Standing Committee H, *Data Protection Bill*, First Sitting, 19 April 1983, col. 17.

aware of the abuses that might be occurring. It will be important for the Registrar, therefore, to act on his own initiative and indeed he is under a duty to so perform his functions so as to promote the observance of the data protection principles[66]. It must be open to him therefore to investigate possible abuses without complaints but he still lacks any coercive powers of investigation. Negotiations and discussions with data users may yield some useful information but it is doubtful whether it will be sufficient in many cases. Whether it would be permissible to employ « undercover » operatives in the manner of investigative journalists as a way of becoming satisfied remains to be seen.

The investigation of individual cases is likely to be a major source of information for the Registrar but there was no specific provision relating to this in either of the Bills introduced into parliament. Although the government always accepted that the Registrar would actually investigate complaints by individuals, it was perhaps understandable that, in view of the limited staff with which he would be provided, there was a great reluctance to put him under any duty to dose[67]. Proposed amendments to include such a duty were defeated, but, sensing the pressure for some hind of duty, the government moved and had accepted the clause that is now section 36(2)[68]. This allows the Registrar to consider complaints about breaches of the Act and requires him to do so « if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected ». Of course the object of an investigation will not be a remedy for the particular complainant but the more general observance of the data protection principles, but the damage or distress to a data subject is a relevant consideration. A more general comment about the Registrar's investigations is that given the information about individuals being harmed which may be discovered by the Registrar, it is regrettable that the proceedings for an enforcement notice, etc. cannot at the same time provide compensation for those data subjects who have already been proved to have suffered loss. There would, however, still have to be a separate remedy for other data subjects similarly affected but whose injury was not discovered untill the enforcement proceedings.

Another matter on which the provisions of the Act offer little guidance is the actual obligation of disclosure imposed on the Registrar with respect to the data user before he takes enforcement action against him. This is an important concern given the way in which the CRE's activities have been

66. S. 36.

67. House of Commons Standing Committee H, *Data Protection Bill*, First Sitting, 19 April 1983, cols. 16-17.

68. H.C. Debs., 5 June 1984, cols. 235-236.

hampered by procedural requirements that had not been fully understood until the intervention of the courts. In the *Data Protection Act* there are none of the detailed preconditions to be found in the *Race Relations Act* but that doesn't mean that natural justice requirements are not relevant. All the decisions of the Registrar (whether refusal or non-renewal of registration or enforcement or deregistration) will have a serious effect on the livelihood of the data user; it will make his activities henceforth a criminal offence unless he takes the appropriate action and even that may require expense. We know that he has to have reasons for his decision — to be able to justify his satisfaction — and that he has to give them to the data and given that in general the decisions of the Registrar are suspended pending an appeal, it could be argued that this is all that the Registrar needs to do; the whole matter can then be argued out at the Tribunal. However, an appeal with natural justice is rarely a substitute for an initial decision in breach of the principles of natural justice [69] and the Registrar's decision, albeit suspended, is still likely to have an impact on the data user, if only to discourage people dealing with him. The Registrar is going to be a person of distinction and his decisions will therefore be treated with the appropriate respect; the stain on the data user's character if nothing else could be formidable. Moreover, if the Registrar is only to act if satisfied, how can he be satisfied unless he has also heard the data user's side? If there is then a duty of disclosure, then the Registrar may have to reveal at least the substance of complaints by data subjects and it may be difficult for the data user to have an opportunity to rebut them without knowing the details of the case. If, therefore, the Registrar acts without giving the data user an opportunity to explain, he is likely to find his decisions being challenged in an application for judicial review by the data user.

3. The Scope for Judicial Review of the Registrar's Decisions

Judicial review might also be resorted to by the data user to challenge decisions of the Registrar on other grounds also, for example, that the reasons given could not justify the conclusion that there has been or is likely to be a breach of the data protection principles or that the steps required to be taken in an enforcement notice or in a transfer prohibition notice are perhaps unreasonable or go further than is necessary to secure compliance with the data protection principles. These complaints by a data user could, of course, equally be ventilated through the appeal system on the basis that the decision is not in accordance with the law. But although in some areas the Divisional Court might be reluctant to interfere where there is also a

69. *Ridge* v. *Baldwin*, [1964] A.C. 40.

right of appeal, it has already stated in relation to non-discrimination notices served by the CRE that it would be prepared to grant judicial review of such a notice if it were satisfied that as a matter of law the notice should never have been served and there was no dispute on the facts even though there had not yet been an appeal to an industrial tribunal [70] and it is probable that a similar approach would be taken with respect to decisions and notices emanating from the Registrar.

Data subjects may also be interested in challenging the decisions of the Registrar not only because his powers cover matters for which there are no civil remedies or at least they are uncertain, but also because an investigation by the Registrar could in some cases be an essential preliminary to a civil action by the data subject himself. However it is unlikely that data subjects would always be able to compel the Registrar to take action against a particular data user or even to investigate the data subject's complaint. The only duty expressly imposed on the Registrar is to investigate those complaints « which appear to him to raise a matter of substance and to have been made without undue delay by a person directly affected [71] ; otherwise he is not required to act even where he is satisfied that there is or is likely to be a breach of the data protection principles by the particular data user. The subjective wording of the terms in which the duty to investigate is laid upon the Registrar will undoubtedly leave him some discretion about which complaint he should actually investigate. Nevertheless, case-law defining « *a matter of substance* », « *undue delay* » and « *a person directly affected* » (which in most, it not all, cases must be a data subject suffering damage as a result of a disregard of the data protection principles) can be expected and the Registrar's discretion will not be open-ended. Even in those cases where section 36(2) does not impose a duty on the Registrar, successful challenges to the exercise of his powers, or more likely his failure to exercise them, are not out of the question. Certainly if the Registrar adopts policies about when he will and when he will not investigate individual cases, he may find his refusals to do so in particular cases open to the challenge that he had failed to exercise his discretion — although given the size of his staff, and the terms of section 36(2) there is likely to be some judicial sympathy for some kind of policy restricting the number of complaints he takes on board. Nevertheless, there can be no doubt that, given that his function is to be guardian of the data subject, individual data subjects would have a sufficient interest to challenge any refusal to investigate, based on a policy that is too restrictive. More problematical, however, is perhaps the situation where the data subject's complaint has been investigated and the Registrar is satisfied that

70. *R. v. Commission for Racial Equality, ex p. Westminster City Council*, [1984] I.R.L.R. 230.
71. S. 36(2).

there has been or is likely to be a contravention of the data protection principles. That state of satisfaction does not mean he has to act but enforcement action in the long term may be of more value to data subjects than pursuing their civil remedies and section 36(2) implicity recognizes this by the obligation to notify a complainant of « any action which he proposes to take » having investigated a complaint. The Registrar's discretion exists to allow him flexibility; the possibility of securing change by negotiation. Should and could his hand be forced by the data subjects who are not prepared to accept this gentlemanly approach to remedying breaches of the data protection principles? It is at least arguable that if the Registrar is satisfied of a breach or likely breach, then there will be cases where failure to take enforcement action does reflect a failure to properly exercise his discretion — after all relevant factors for all his powers are the damage or distress that may have been caused to data subjects and as far as, for example, the deregistration power is concerned, it may well be a flagrant case of closing one's mind if the Registrar persists in negotiation when there has been no effort at all to comply with an enforcement notice and prosecution has not led to any change of behaviour.

If the Registrar's decisions are challenged in this way through judicial review, it is possible that allegations of breaches of the data protection principles will be considered in three or even four different fora. Thus there could be appeals by the data user against enforcement action to the Tribunal; civil proceedings brought by the data subject; criminal proceedings against the data user; and applications for judicial review instigated by the data subject and/or the data user. This situation is possibly overcomplex and may prove to be an unnecessary hindrance to the Registrar's work, particularly as the increased use of computerisation means that its volume will grow rather than diminish.