IN THE DATA PROTECTION TRIBUNAL

BETWEEN:

EQUIFAX EUROPE LIMITED

Appellant

and

THE DATA PROTECTION REGISTRAR

Respondent

(DA/90 25/49/7)

APPEAL DECISION

Members of the Tribunal: Aubrey L Diamond (Deputy Chairman), Alex Lawrence and Victor Ross

Introduction

1. This is the third case we have heard involving a credit reference agency. A credit reference agency is a company which has created a large database which includes information about the financial position of individuals. A customer of the agency who is considering whether to grant credit to an applicant can obtain information from the database to assist him in making the credit decision.

2. This case resembles the earlier cases in some respects, and like them is an appeal from an enforcement notice served by the Data Protection Registrar, in identical terms in each case. But it differs fundamentally from the earlier cases in that there is virtually no dispute as to the facts, nor as to fairness or unfairness, nor as to the exercise of any discretion. Argument has centred on two particular provisions in the Act, and it is submitted on behalf of the appellant that these provisions, or either of them, preclude the Registrar from serving an enforcement notice.

Formal matters

3. Equifax Europe Limited was formerly known as Westcot Data Limited, the name against which the enforcement notice was served. It is a company which supplies credit reference (and other services which currently include tracing, credit scoring and associated systems) to its customers. The company is a credit reference agency, as defined by section 145(8) of the Consumer Credit Act 1974, and is licensed as such under that Act. It is also registered under the Data Protection Act 1984 as a data user who holds personal data and as a computer bureau. Its register entry number E0021120 contains a description of the personal data which it holds for purpose PO35 Credit Reference – the provision of information relating to the financial status of individuals or organisations on behalf of other organisations.

4. On 28 August 1990 the Registrar served on Westcot Data Limited an enforcement notice under section 10 of the Data Protection Act. After the enforcement notice was served Westcot Data Limited, on 12 February 1991, submitted an application to alter their register entry by adding a new purpose, PO58 Crime Prevention and Prosecution of Offenders. It was not argued by the Registrar that since this was not a registered purpose at the date the

enforcement notice was served it should not be taken into account. As far as we are concerned the enforcement notice speaks for the future, and it seems that we should have regard to the position as it is today.

5. On 24 September 1990 the Registrar received a notice of appeal under section 13 of the Act. An amended notice of appeal was served on 26 April 1991 by Equifax Europe Limited, to which the appellant company had changed its name on 11 March 1991. The appeal by Equifax Europe Limited ("Equifax") was heard by this tribunal from 28 to 30 May 1991. Equifax was represented by Mr Simon Chalton, a consultant with Messrs Dibb Lupton Broomhead and Prior of Leeds. The Registrar was represented by Mr Henry Carr and Mr Mark Vanhegan, instructed by Mrs Rosemary Jay, legal adviser to the Registrar. We heard evidence from seven witnesses. Written proofs of the evidence of each witness, and of one further witness who was unable to attend on account of ill health, were exchanged by the parties and made available to the tribunal.

6. The essence of the dispute relates to the way in which Equifax responds to the requests it receives from its customers for information for use for credit reference purposes and to the extraction from Equifax's database for supply to its customers of information which is not specifically about the person who has applied for credit and about whom credit reference information is being sought.

<u>The CCN decision</u>

7. On 25 February 1991 the tribunal had issued its decision in relation to an appeal by CCN Systems Limited and CCN Credit Systems Limited ("CCN") against enforcement notices served by the Registrar in like terms to that served in the present case. There was naturally some reference in the present hearing to the decision in the earlier case ("the CCN decision"). We are not of course in any way bound by the CCN decision, and in the present appeal completely new legal arguments have been raised. However, the facts in the CCN decision resemble those in the present case, and an example we gave in the CCN case would also be relevant here.

<u>Third party information</u>

8. As a credit reference agency, Equifax receives from its customers, who are mainly if not entirely providers of credit, requests for information about an individual who has applied for credit. The essence of the dispute – and this is agreed by both parties – relates to the extraction from Equifax's database for supply to its customers of certain types of what is called third party information, that is to say, information about persons other than the individual who is seeking credit and who is the subject of the inquiry.

9. The example we gave in the CCN decision was of a Mr Jones (the names are fictitious), a chartered accountant, who sold his house in 1985 to a Mr Watson. In 1988 Mr Jones applied to a building society for a cheque guarantee card. His application was rejected. Exercising his rights under the Consumer Credit Act 1974 he applied to CCN for a copy of his file. This revealed that in 1987 – two years after Mr Jones sold the house – a county court judgment had been entered against Mr Watson, the purchaser of the house. The only link between Mr Jones and Mr Watson was that they were respectively vendor and purchaser of a house a few years earlier. Put in another way, the only link between them was that they had at different times lived at the same address.

10. This comes about from the fact that some credit reference agencies search, not against names, but against addresses, and extract from their database all information about all persons recorded at that address. In the CCN decision we considered CCN's argument as to the predictive value of this "third party information" and found that "The evidence we heard leaves us in no doubt that third party information is of value to a grantor of credit. It has predictive value. It cannot of course predict whether the applicant for credit will or will not pay, but added to the other information that is available it does help the credit grantor to classify applicants so as to establish an approximation of the percentage risk of default".

11. The evidence we heard from Equifax was that when an individual seeking credit ("the applicant") approached one of Equifax's customers, the customer was not invited to submit the applicant's name to Equifax. The only information asked for was the applicant's address, including previous addresses if he had been at his current address for less than a specified period. Information was thus extracted from Equifax's database showing details about all individuals at those addresses, whether the applicant for credit or not. The customer would only supply the applicant's name to Equifax if difficulty was experienced in finding the correct address.

12. Most of the issues of fact which were argued in the earlier cases did not arise in the instant case. We were handed the following document: "The following facts are admitted by Equifax:-

> (1) That as a result of the correct operation of the Equifax System financial information has been and will be extracted about persons who have no financial link as a matter of fact with the applicant for credit ('unrelated third party information').
>
> (2) That, in cases where the score of the applicant for credit is on the borderline for acceptance, the inclusion of unrelated third party information has caused and may in the future cause refusal of the application for credit.
>
> (3) That as a result of such refusals persons have suffered and will suffer distress.
>
> (4) That all of the findings in paragraphs 32-37 of the CCN decision are correct. [This refers to our findings as to the predictive value of third party information summarised in paragraph 10 above].
>
> "The following proposition of law is accepted by Equifax:-

That as Equifax rely upon the exemption in Section 28(4) of the Act, the burden of demonstrating that they are within the exemption is on Equifax".

We were told that these admissions were not intended to prejudice Equifax's right to argue points of law on appeal.

<u>The Registrar's duties and powers</u>

13. Various provisions in the Data Protection Act 1984 are relevant to the action taken by the Registrar.

14. Set out in Part I of Schedule 1 to the Act are eight "data protection principles". The subject of dispute in these proceedings is the first principle, which reads as follows:

> 1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

15. The principle an be re-written in two parts:

> (a) The information to be contained in personal data shall be obtained fairly and lawfully.
>
> (b) Personal data shall be processed fairly and lawfully.

No issue was raised in the various credit reference agency proceedings relating to the obtaining of information, nor was it suggested that the processing of personal data was carried out unlawfully. The cases were concerned entirely with that part of the principle that can be reduced to: "Personal data shall be processed fairly".

16. A number of rules of interpretation of some of the principles will be found in Part II of Schedule 1. Those relating to the first principle are concerned solely with that part of the principle that deals with the obtaining of information, and are therefore not of relevance to this decision. However, some of the expressions to be found in the first principle are defined in section 1 of the Act, and will be referred to later (paragraph 43).

17. Section 36(1) of the 1984 Act states that "It shall be the duty of the Registrar so to perform his functions under this Act as to promote the observance of the data protection principles by data users and persons carrying on computer bureaux". Subsection (2) of the same section goes on as follows:

> (2) The Registrar may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected …..

Pursuant to this duty the Registrar considered the complaints he had received relating to the use of third party information.

18. We will describe in the next paragraph the action taken by the Registrar in considering the complaints. For the moment we will complete the reference to the Registrar's statutory powers. Section 10 deals with enforcement notices; the relevant subsections are as follows:

> (1) If the Registrar is satisfied that a registered person has contravened or is contravening any of the data protection principles he may serve him with a notice ("an enforcement notice") requiring him to take, within such time as is specified in the notice, such steps as are so specified for complying with the principle or principles in question.
>
> (2) In deciding whether to serve an enforcement notice the Registrar shall consider whether the contravention has caused or is likely to cause any person damage or distress.
>
> (9) Any person who fails to comply with an enforcement notice shall be guilty of an offence; but it shall be a defence for a person charged with an offence under this subsection to prove that he exercised all due diligence to comply with the notice in question.

It remains to say that sections 13 and 14 of the Act, and Schedule 3, relate to appeals to this Tribunal. Paragraph 4 of Schedule 3 empowers the Home Secretary to make rules of procedure, and we are accordingly governed by the Data Protection Tribunal Rules 1985, S.I. 1985 No. 1568. Rule 19 provides that "In any proceedings before the Tribunal it shall be for the Registrar to satisfy the Tribunal that the disputed decision should be upheld".

The Registrar's action

19. Over a period of years the Registrar, Mr Eric Howe CBE, had discussions with the credit industry. He had apparently made progress to some extent. On 17 July 1990 the Industry Forum on Data Protection issued a press release headed "Credit Industry to drop Use of some Third Party Information". The first paragraph read as follows:

> "Britain's major credit organisation have advised the Data Protection Registrar that they have requested credit reference agencies not to provide other surname non-concurrent information after 31 July next year. This means that credit grantors should be given information only about people who live, or who have lived, at the same address at the same time as the applicant".

However, nothing came of this initiative. The Registrar did not think it went far enough, and he issued the enforcement notice in this case on 28 August 1990. We were told that no steps were taken to implement the proposal by the credit industry.

The enforcement notice

20. The operative words of the enforcement notice read as follows:

> …. the Registrar hereby gives notice that in exercise of his powers under Section 10 of the Data Protection Act 1984 he requires Westcot Data Limited (now Equifax Europe Limited) to ensure whether by amendments to any relevant processing system or otherwise:-
>
> that from the 31st day of July 1991 personal data relating to the financial status of individuals ceases to be processed by reference to the current or previous address or addresses of the subject of the search whereby there is extracted in addition to information about the subject of the search any information about any other individual who has been recorded as residing at any time at the same or similar current or previous address or addresses as the subject of the search.

Equifax's database

21. To complete the factual background it is necessary to describe the way in which the information obtained by Equifax is stored on computer and extracted. Before the enforcement notice was served a statement describing the system of processing operated by Westcot Data Limited, as Equifax was then known, was agreed between officers of the Registrar and Westcot Data Limited. The following passages are based on the agreed statement, but references to Equifax have been inserted.

22. In order to provide its customers with information which will assist them in assessing the creditworthiness of individuals, Equifax stores on computer the following categories of information:

Electoral Registration Information. This comprises the information contained in the official electoral rolls which are revised annually and contain the names and addresses of all persons who are entitled to vote in elections in the United Kingdom and the Republic of Ireland. The information for a particular address is retained for a rolling six-year period.

Court Judgments. Details of those court judgments that are kept on public registers are obtained by Equifax. They cover England and Wales (county courts), Northern Ireland (county courts), Scotland and the Republic of Ireland. These are kept on Equifax's files for six years.

Bankruptcies and Related Matters. Details of bankruptcies are obtained from publicly available sources; details of undischarged bankrupts are retained indefinitely, those of discharged bankrupts for six years. Related matters include bills of sale and winding up orders.

Scottish Valuation Roll. There is a list, open to the public, of the valuation for rating purposes of all rateable properties in Scotland.

Previous searches. Details of searches are maintained for a maximum period of two years.

Insight. Customers who participate in the shared information "Insight" service submit regular updates of their consumer credit accounts to Equifax. The information recorded includes the type of lender, the type of account, the start, settlement and write off dates, the outstanding balance, the amount of monthly payment due, the payment history for the last twelve months and any derogatory status information over the last six years. This information is available only to those customers of Equifax who participate in Insight.

CIFAS (Credit Industry Fraud Avoidance Scheme). Members of this service (the major credit grantors) supply information on individuals who have been identified as fraudulent. Only members of CIFAS have access to this information. These details are retained by Equifax for three months.

Westrace. Westrace is a service provided for customers which tracks the movement of a person to assist customers in tracing. The Westrace file is created using the electoral roll, names and addresses from the telephone directory and client information.

Postal Address File (PAF). Equifax obtains this from the Post Office. It contains all postal addresses in the United Kingdom. It is updated in line with amendments to the PAF made by the Post Office.

Telephone Directory File. Equifax is currently entering details of all personal telephone numbers from British Telecom directories on to their credit reference database. This information is not yet being supplied to customers.

Closed User Groups. Under its registration as a computer bureau Equifax maintains a number of closed user groups on behalf of its clients where access to restricted data is given to members of the closed group via Equifax's search mechanisms.

23. The agreed statement includes a description of the structure of Equifax's credit reference database. The whole of the database is a single database and is based on the Postal Address File. To that file is added the detail from the various sources described above. Where there is an exact match of the address the details are added automatically, otherwise the address details will be considered individually by one of approximately 200 persons employed by Equifax to deal with address matching. Names of individuals are added to the database exactly as they are captured.

Search techniques

24. The information is supplied by Equifax to its customers in response to searches made by them. Searches may be made in a number of different ways:

> Post, Telephone or Telex. The customer supplies his account number, password and the appropriate details of the address of the individual in whom it is interested. These words are underlined because they assumed significance in the arguments referred to below. The search is conducted by Equifax's staff and the result is passed back to the customer by telephone, post or telex.
>
> Remote terminals. Remote terminals at customers' premises access the Equifax computer. The customer keys in his account number, password and appropriate details of the address of the individual in whom it is interested. These details are automatically processed by the Equifax computer and the result is transmitted back to the customer's screen or printer.
>
> Computer to computer links. Equifax has established direct links between its computer and the mainframe computers of its larger customers. The customer's computer communicates directly with programs on Equifax's computer which in turn integrates the Equifax database. The communication would usually be in the course of processing a credit application made by the individual to the customer and the information obtained from the Equifax computer may be used together with other information obtained by the customer from the individual in an automated credit scoring system operated by the customer.
>
> Batch mode. The customer supplies Equifax with the account number, password and details of the addresses of the individuals in whom it is interested on magnetic tape. The searches are conducted by Equifax's staff and the result passed back to the customer on magnetic tape.

25. Equifax provides different levels of search, covering specified items of information, and customers can select which they require. The common feature of all these searches is that the essential key to locating the information sought is by address. The searches will provide details of all the individuals, falling within the scope of the search, recorded as living at the address searched at any time. Any decision as to whether or not to grant credit to an individual is entirely a matter for the customer.

The legal arguments

26. We are now in a position to describe the arguments put to us by Mr Chalton on behalf of Equifax to justify his claim that the Registrar has no power to issue an enforcement notice against Equifax. One of these arguments is based on section 28(4) of the Act and can be

described as the “crime exemption”, the other is based on section1(7) of the Act and can be described as the “no processing” argument. We deal with the crime exemption first.

The crime exemption

27. Part IV of the Act, sections 26 to 35, contains a number of exemptions from various requirements of the Data Protection Act. Part IV opens with a preliminary section, section 26, subsection (1) of which provides as follows:

> 26(1) References in any provision of Part II or III of this Act to personal data do not include references to data which by virtue of this Part of this Act are exempt from that provision.

The Registrar’s power to serve an enforcement notice is contained in Part II of the Act. (We can add that subsection (2) of section 26 defines “the subject access provisions” and subsection (3) defines “the non-disclosure provisions”).

28. The succeeding sections of the Act set out a number of exemptions: s.27, National security; s.28, Crime and taxation; s.29, Health and social work; s.30, Regulation of financial services etc; s.31, Judicial appointments and legal professional privilege; s.32, Payrolls and accounts; s.33, Domestic or other limited purposes; s.34, Other exemptions; and s.35, Examination marks. It is section 28 with which we are concerned.

29. We set out section 28 in full, though the argument centred on subsection (4) and paragraphs (a) and (b) of subsection (1):

> 28(1) Personal 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.
>
> (2) Personal data which –
>
> (a) are held for the purpose of discharging statutory functions; and
> (b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1) above,
>
> are exempt from the subject access provisions to the same extent as personal data held for any of the purposes mentioned in that subsection.
>
> (3) Personal data are exempt from the non-disclosure provisions in any case in which –
>
> (a) the disclosure is for any of the purposes mentioned in subsection (1) above; and

(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection,

and in the proceedings against any person for contravening a provision mentioned in section 26(3)(a) above it shall be a defence to prove that he had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters.

(4) Personal data are exempt from the provisions of Part II of this Act conferring powers on the Registrar, to the extent to which they are exercisable by reference to the first data protection principle, in any case in which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in subsection (1) above.

30. The relevance of subsection (4) of section 28 is said to be this: although the function of a credit reference agency is generally seen to be the provision of information relating to the financial status of persons who have applied for credit, there is a further function, namely, the prevention of crime. This is because persons applying for credit may commit fraud, and the searches performed by the credit reference agency may help to prevent or detect fraud. We were told that the last – minute addition of purpose PO58 (crime prevention and the prosecution of offenders) (see paragraph 5 above) was not a belated ruse thought up by the appellant's legal advisers when preparing the appeal to the tribunal but the rectification of an oversight, the completion of a registration that should have been made from the start.

31. We were given several examples of alleged fraud which were said to have been detected by the address-based searches conducted by Equifax. Although we were not convinced that all of the examples were in fact examples of criminal fraud rather than innocent mistakes or misunderstandings, there is no need to go into detail here. We of course accept that some persons seek credit dishonestly, with no intention of repaying, and that fraudulent names and addresses may be used.

32. The Credit Industry Fraud Avoidance System ("CIFAS") was conceived by the Consumer Credit Trade Association in 1988 as an information exchange between licensed credit grantors and licensed credit reference agencies to facilitate the prevention of fraud and the dissemination of information on suspected fraud to its members. The preamble to CIFAS's rules states that the information is supplied solely for the prevention of fraudulent obtaining of credit or hire facilities and for associated law enforcement purposes. We heard evidence from Mr Alan C Hilton, the chief executive and company secretary of CIFAS. He estimated that in 1990 the CIFAS information had led to the identification of about 7,000 frauds, but said that they had no information on convictions or prosecutions, nor on frauds identified by non-members.

33. CIFAS deals with three main categories of suspected fraud. These may be summarised shortly as follows (1) False name, true address. Here "true address" does not necessarily mean the true address of the individual seeking credit under a false name. This category includes the so-called "empty house" fraud, where the address given is an empty house, usually one up for sale, where access can be obtained to collect mail and where address-based searches will provide information, if any, about the genuine former occupants. (2) Impersonation. The impersonation may be of a real or a fictitious person; typically the fraudulent person will pretend to be the person identified by stolen documents, such as driving licence or credit cards, in his possession. (3) True name, true address but false personal information. These cases include suppressing the fact of unemployment or falsely

stating the type of employment or level of income. It was clear from the evidence we heard that address-based searches do not necessarily bring all these categories of fraud to light. Other categories of fraud, such as mortgage fraud, are not recorded.

34. The evidence we heard emphasised that although there may be a significant number of fraudulent credit seekers, and although substantial sums may be lost by fraud (though it is not easy to distinguish between the honest defaulter and the dishonest), criminals form a tiny proportion of applicants for credit. Equifax alone process between fifteen and twenty million searches a year, and the director of Equifax who gave evidence told us, very fairly, that the vast majority of applicants for credit were not fraudulent. Mr V R Ware, a leading representative of the credit industry, confirmed the statement that "Most applications for credit are honestly made" and added that the credit industry exists because most of the population are honest.

35. Mr Chalton's argument is based fairly and squarely on the wording of section 28(4) of the Act. That subsection exempts personal data from the provisions of Part II of the Act that confer powers on the Registrar to the extent to which those powers are exercisable by reference to the first data protection principle. Those powers include section 10, which empowers the Registrar to serve an enforcement notice, and the enforcement notice in this case was based on an alleged breach of the first principle. Accordingly the Registrar has no power to serve the enforcement notice "In any case in which the application of those provisions to the data would be likely to prejudice" the prevention or detection of crime or the apprehension or prosecution of offenders. It is these last words we must now turn to.

36. Although most applicants for credit are honest, some are not. When an application for credit is received, the credit grantor does not know if the applicant is one of the honest majority or of the small dishonest minority. A search extracting details of information, particularly but not only adverse information, about all persons at the applicant's address, whatever their name, may, it was argued, help to identify cases of possible fraud. To identify as many suspicious cases as possible – for example, a large number of credit applications from the same address, all in different names but all based on variations of the same surname and initials – such an address-based search must be made in respect of each applicant for credit, even though there is no reason to suspect fraud. If such searches were restricted to cases where fraud was suspected for other reasons, some cases of fraud or suspected fraud might not be exposed. Therefore the enforcement notice, preventing most address-based searches, would, it was said, be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. Moreover, the present system adopted by Equifax no doubt exercises a deterrent effect on some persons who might be tempted to submit fraudulent applications for credit if there were no risk, or a diminished risk, of being detected.

37. We may follow on from Mr Chalton's careful argument in this way. If it is said that the universal making of address-based searches would be unfair to all the honest applicants for credit, this is not a matter that the Registrar can take into account. If the prevention of crime is prejudiced, considerations of fairness or unfairness do not enter the equation. It may be recalled that in the CCN case one of the factors we were urged to consider, and did consider, in weighing the balance of fairness was the need to prevent or limit fraudulent applications. We felt this could not justify the wholesale extraction of third party information in all cases. But in that case our attention was not drawn to section 28(4). In the light of that provision, argues Mr Chalton, the Registrar (and accordingly the tribunal) cannot take account of the fact that this would be unfair to the mass of honest applicants. If the exemption conferred by s.28(4) applies, the first principle has no application, and the Registrar cannot protect the mass of honest applicants from unfair – or, indeed, unlawful –

processing. The enforcement notice cannot be served, and the tribunal cannot uphold or vary it.

38. Mr Carr's response to that argument is to focus on the phrase "in any case" in section 28(4). Personal data are exempt from the provisions referred to "in any case in which the application of those provisions to the data would be likely to prejudice" the prevention or detection of crime or the apprehension of offenders. It seems to us that the words taken as a whole – "in any case in which the application of those provisions to the data" – make it plain that the exemption applies only in particular cases where we can talk about "the data", that is to say the personal data to which we may or may not apply the provisions.

39. Both parties drew attention to other exemptions in Part IV of the 1984 Act, and several other uses of the expression "in any case in which" may be referred to. For example, section 27(1) is an example of a blanket exemption in the interests of national security which is not limited to particular cases, in contrast with section 27(3) which uses the words "in any case" and where subsection (4) makes it clear that subsection (3) is talking about particular cases. Again, section 34(8) provides an exemption from the non-disclosure provisions to prevent injury: the exemption applies "in any case in which the disclosure is urgently required for preventing injury or other damage to the health of any person or persons". Mr Chalton took this to provide a blanket exemption, Mr Carr a limited exemption that went no further than the need to prevent injury in the particular case.

40. Consider subsection (4) in relation to the case of an honest application. Would the application of the Registrar's power to require Equifax not to conduct address-based searches producing certain third party information be likely to prejudice the prevention of crime? Since there is no crime, and no possibility of crime, in that case, the answer must be, not in that case. Would the application of the Registrar's power be likely to prejudice the detection of crime? A fortiori, since no crime has been or will be committed, the answer must be, not in that case. Would the application of the Registrar's power be likely to prejudice the apprehension of offenders? Again, there are no "offenders" and there will be no prejudice to their apprehension in that case. Finally, would the application of the Registrar's power be likely to prejudice the prosecution of offenders? Again, for the same reason the answer must be, not in that case.

41. It is clear that in any case where fraud is attempted the Registrar's notice would be likely to prejudice the prevention of crime. In any such case, therefore, the personal data are exempt from the relevant provisions of Part II of the Act and Equifax are free to process data untrammelled by the notice. But in our judgment section 28(4) does not prevent the Registrar from serving such an order in relation to all the cases – the vast majority – where no crime is, or is going to be, committed. The phraseology is "would be likely to prejudice" the matters referred to, not "might conceivably prejudice" those matters. We think it unlikely that Parliament would, as a side-wind from the provision in the Act intended to exempt some part of police computer operations, have wished to exempt virtually the whole of credit reference activities from the obligation to process fairly and lawfully.

42. Having rejected Equifax's argument based on the crime exemption, we now turn to the other argument.

<u>The "no-processing" argument</u>

43. The "non-processing" argument rests on section 1(7) of the Act. It will be recalled that the essential part of the first data protection principle in this case, extracted from the

words in Schedule 1, reads: “personal data shall be processed fairly”. The meaning of “processed” is to be derived from section 1(7):

> “‘Processing’, in relation to data, means amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of those operations by reference to the data subject”.

“Personal data” is defined in section 1(3) as follows:

> “‘Processing data’ means data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user) …..”

44. In the CCN decision we identified the relevant activity of processing as “extracting the information constituting the data”, but no argument was directed to the closing words of subsection (7). Mr Chalton now argues that in the present case personal data is not processed, and hence the first principle, which imposes standards for the processing of personal data, has no application. This proposition is based on the definition of processing just cited. We have personal data, such as information relating to named individuals concerned with matters such as court judgments or credit agreements. That information is extracted from the database for the purpose of credit reference. But processing, according to the last words of the definition, means extracting the information <u>by reference to the data subject</u>, and according to Mr Chalton that is not how Equifax extracts data. It extracts data by reference to address, not by reference to name, even though the sole purpose of the extraction is to enable a credit grantor to decide whether to grant credit to an individual. It is of course that very activity, extraction by an address-based search rather than by name search, which produces details of entries relating to all persons at the address whether or not they are, or are connected with, the applicant for credit, that the Registrar objects to as being unfair. Mr Chalton contrasted the phrase “by reference to” with the different phrase “with regard to” used elsewhere in the Act.

45. What did Parliament mean when it used the words “by reference to”? As a definition of “processing”, it would seem that the passage is quite adequate without the addition of the last phrase: processing means amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data.

46. Why, then, did Parliament add the words “and, in the case of personal data, means performing any of those operations by reference to the data subject”. (We should add that “Data subject” means an individual who is the subject of personal data”, so that both the applicant for credit, if there is any data about him on the database, and the other persons whose details are extracted, are all data subjects, though not perhaps “the” data subject). Both Mr Carr and Mr Chalton agreed that the purpose of the added words was to limit the scope of application of the Act, to relieve the burden of supervision imposed on the Registrar, and to reduce the cost of compliance with the Act. But they disagreed on how those words were to be interpreted. As we have seen, Mr Chalton equated the phrase to a description of how the data user accessed the data, whether by name or in some other way. Mr Carr, on the hand, would have regard to the intention and purpose of the processing.

47. We found two examples given by Mr Chalton helpful. He instanced the Driver and Vehicle Licensing Centre computer in Swansea. It is, he said, possible to access the database by reference to the vehicle number; this, he said, would not be processing by reference to data

subjects even if the computer extracted a list of past and present keepers of the vehicle. One might, he said, be interested in the vehicle itself, such as the date it was manufactured.

48. His other example was the Land Registry computer. One could, he said, access the computer's database either by reference to the names of individuals, such as registered owners, or by reference to title number – in other words, by reference to the land. The first means of access would involve processing, the second, according to Mr Chalton, would not.

49. We find this particular example helpful for this reason. Mr Chalton is looking at the phrase "by reference to the data subject" as linked to the mode of input into the computer system in order to conduct an operation such as amending data or extracting information. But it is difficult to believe that Parliament, or the draftsman, was looking at the issue through a computer-operator's eyes. What Parliament had in mind, we think, is the difference between approaching the database to conduct operations that had nothing to do with the data subject, and operations that focussed on the data subject. Thus using the Land Registry's computer to change the boundaries of a plot of land, or perhaps to extract a copy of a restrictive covenant, would in no way concern the individual identity or attributes of a data subject, and need not attract the control over processing. On the other hand, using the computer to extract the name of a data subject, whether the computer was approached by typing in the name of the data subject or by retrieving his name in some other way, would constitute processing.

50. If we are right in this, it seems to us not to matter whether the search on Equifax's database was initiated by typing in the name of the subject of the enquiry or typing in the description of a piece of land associated with the subject of the enquiry. In both cases the object of the exercise is to learn something about individuals, not about the land. The data is processed in a way linked to the data subject, and hence by reference to the data subject. (For another use of "by reference to" where it does not mean the way the computer is operated see section 28(4)). Equifax emphasised that it did not in most cases even know the name of the individual seeking credit, as if this confirmed that the extraction could not be by reference to the data subject. But Equifax is a credit reference agency, one of its registered purposes is "the provision of information relating to the financial status of individuals" and it knows perfectly well that its customers have in mind particular individuals with whom it is contemplating entering into credit transactions (see for example paragraph 24 above). We therefore find that the extraction of information constituting personal data by Equifax's address-based search is performed by reference to the data subject and so constitutes processing.

51. Various other points were drawn to our attention in connection with the interpretation of these two subsections. For example, reference was made to the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. It was pointed out that the final words of section 1(7) do not appear to have any counterpart in the Convention, and that the exemption in section 28(4) appears in a more restricted form. In the Convention the British first data protection principle is to be found in paragraph a of Article 5. Article 9, paragraph 1, states that no exception to the provisions of Article 5 shall be allowed except within the limits defined in Article 9. Then paragraph 2 of Article 9 provides as follows:

> "2. Derogation from the provisions of Article ….. 5 …. of this convention shall be allowed when such derogation is provided for by the law of the Party (ie, Contracting State) and constitutes a necessary measure in a democratic society in the interests of:

a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences …..”

There is a principle that Parliament is not lightly to be assumed to enact legislation in breach of the United Kingdom’s international obligations. Thus it might be said if section 28(4) is not a necessary measure in a democratic society in the interests of protecting (perhaps in the sense of promoting or not inhibiting) the suppression of criminal offences, this fact (or opinion) may help a court to resolve an ambiguity. But here we are concerned with a specific provision that Parliament has chosen to enact, and our conclusion is that it is tolerably clear in meaning. Similarly, Parliament has enacted the words at the end of section 1(7) and we do not think there is an ambiguity requiring the application of the principle we have mentioned.

52. Mr Chalton drew our attention to several other matters. On the basis that breach of the enforcement notice leads to penal sanctions, he asked us to interpret the Act in favour of the liberty of the subject – the strict construction of criminal statutes. We have borne this principle in mind, but finding the Act tolerably clear we do not think we need to rely on this presumption in this case. He also referred us to a number of cases, and in particular to the two we now mention. In Black-Clawson International Ltd -v- Papierwerke Waldhof-Aschaffenburg AG [1975] 1 All E.R. 810 he referred to a passage of Lord Diplock at p836 about certainty in the law. “The acceptance of the rule of law as a constitutional principle”, said Lord Diplock in the passage to which we believe Mr Chalton was referring, “requires that a citizen, before committing himself to any course of action, should be able to know in advance what are the legal consequences that will flow from it. Where those consequences are regulated by a statute the source of that knowledge is what the statute says. In construing it the court must give effect to what the words of the statute would be reasonably understood to mean by those whose conduct it regulates. That any or all of the individual members of the two Houses of Parliament that passed it may have thought the words bore a different meaning cannot affect the matter. Parliament, under our constitution, is sovereign only in respect of what it expresses by the words used in the legislation it has passed”. He went on to explain how this principle did not prevent a court from referring to an official report of a government committee in case of ambiguity. That might have been relevant here had either party made reference, for example, to the Lindop Report of the Committee on Data Protection, but as neither did so we have not referred to it.

53. The other case we were referred to by Mr Chalton was R -v- Cuthbertson [1980] 2 All E.R. 401, again to a passage, at p403, of Lord Diplock. This case was also concerned with the use of extraneous aids to interpret a statute, which Lord Diplock thought unnecessary in the particular case. The words in Mr Chalton’s mind, we presume, were “The words of the section, in my view, speak for themselves clearly, without resort to extraneous aids”. As we say, we have not needed to resort to external aids in this case.

Decision

54. This virtually completes what we have to decide arising from the arguments on the matters in dispute in this case. We can quickly summarise our other conclusions. Equifax admit that as a result of the correct operation of their system financial information is extracted about persons who have no financial link with the applicant for credit. In our judgment this processing of personal data is unfair within the first data protection principle. In coming to this decision we have carefully weighed the advantages and disadvantages on both sides. We believe in the benefits of reliable credit reference and credit scoring systems, notably in relation to their ability to restrain over-commitment by debtors or prospective debtors. This we believe to be for the benefit of debtors, creditors and the community in

general. We are also conscious of the role that the extraction of third party information may play in reducing the risk of fraudulent applications. Nevertheless, we hold that the unfairness to credit applicants of the extraction of such information outweighs the benefits and that the Registrar is justified in serving an enforcement notice.

Form of enforcement notice

55. The reasons we gave in the CCN and Infolink cases for our finding that the Registrar's enforcement notice is wider than is necessary to secure compliance with the first data protection principle apply equally in this case. The Registrar is well familiar with our views, and Mr Carr addressed us on the drafting of the enforcement notice at the hearing in this case. Mr Chalton, who has had copies of our earlier decisions, did not take the opportunity to address us on the drafting. We would not wish to exclude him from the possibility of arguing this matter before us if he wishes.

56. In the Infolink decision we announced that we proposed to exercise our power under section 14(1) of the Act to substitute for the enforcement notice served by the Registrar one drafted in accordance with the findings we made in that case. We promulgated the main part of our decision and announced that there would be a resumed hearing (which the parties in the Infolink case had requested) to hear representations on the terms of the enforcement notice. We think a similar adjournment would be convenient in this case, and the hearing is accordingly adjourned to a date to be arranged for this purpose.

Time for compliance

57. The Registrar stipulated in his enforcement notice dated 28 August 1990 that compliance must take effect by 31 July 1991. Only if this appeal were not determined before 31 July would section 10(6) of the Act extend the time for compliance, but it appears that Equifax has not yet taken steps to comply with the Registrar's notice. Since we are altering the Registrar's notice, it would be appropriate to give consideration to a new period of time for compliance.

58. Taking into account what was said at the hearing, it would be appropriate to allow further time. The date for compliance should be 1 January 1993.

Conclusion

59. For the reasons set out above this appeal will be allowed in part and an enforcement notice in the terms to be set out after the next hearing will be substituted for that served by the Registrar.

60. No application was made for costs and in accordance with Rule 24 of the Data Protection Tribunal Rules 1985 we make no order as to costs.

28 June 1991 Chairman

IN THE DATA PROTECTION TRIBUNAL

BETWEEN:

EQUIFAX EUROPE LIMITED

Appellant

and

THE DATA PROTECTION REGISTRAR

Respondent

APPEAL DECISION – CONCLUSION

Members of the Tribunal: Aubrey L Diamond (Deputy Chairman), Alex Lawrence and Victor Ross

1. On 28 June 1991 we issued the first part of our decision in this case, containing all our findings of fact and the reasons for the decision. We adjourned the hearing to a date when we could hear representations on the terms of the enforcement notice which we proposed to substitute under section 14(1) of the Data Protection Act 1984 for that served by the Data Protection Registrar on 29 August 1990. This document contains the concluding part of our decision.

2. The adjourned hearing was held on 12 February 1992. We heard submissions by counsel and solicitors as to the form of the enforcement notice, and also as to the date on which it should take effect. The Registrar's notice was to take effect on 31 July 1991, but in view of the time taken before the hearing of this appeal we thought at the first hearing that the revised form of enforcement notice should take effect on 1 January 1993. At the adjourned hearing on 12 February 1992 we were asked by Mr Chalton, representing the appellant, to reconsider that date, having regard to the time that it would take to make the necessary alterations to the appellant's programs, the date of the adjourned hearing and the delay after the first part of our decision before the appellant would have the definitive text of the enforcement notice. We have reconsidered the date, and think that in the interests of justice it is necessary to give more time than we envisaged last June. The enforcement notice set out below accordingly operates from 31 July 1993.

3. In the light of the parties' submissions we now conclude that the enforcement notice to implement our findings should issue in the following form:

(1) That, subject to paragraph (2) below, from 31 July 1993 Equifax Europe Limited ("Equifax") shall cease to extract personal data relating to the financial status of individuals by any extraction program whereby (i) such personal data is extracted by reference to the current or previous address or addresses of the subject of the search ("the subject") and (ii) there is extracted, in addition to information about the subject, any financial information about any other individual who has been recorded as residing at any time at the same or similar, current or previous, address or addresses as the subject.

(2) Subject to paragraph (3) below, nothing in this notice shall prevent the extraction of information about any other individual, recorded as residing at the same present or previous address as the subject concurrently with the subject, who –

(a) (i) has the same surname, and forenames or initials where these are recorded, as the subject, or

(ii) has a name sufficiently similar to that of the subject for it to be reasonable to believe that he or she is the subject, or

(b) (i) has the same surname as the subject, or

(ii) has a surname sufficiently similar to that of the subject for it to be reasonable to believe that it is the same surname,

and where in either case it is reasonable to believe that he or she has been living as a member of the same family as the subject in a single household, or

(c) does not have the same surname as the subject but in respect of whom, on the basis of information obtained before extraction, it is reasonable to believe

(i) is the subject or

(ii) has been living as a member of the same family as the subject in a single household.

(3) In paragraph (2) above –

sub-paragraphs (a) and (c)(i) shall not apply where there is information in the possession of Equifax from which it is reasonable to believe that the individual is not the subject;

sub-paragraphs (b) and (c)(ii) shall not apply where there is information in the possession of Equifax from which it is reasonable to believe that there is no financial connection between the individual and the subject.

Aubrey L Diamond
Chairman
28 February 1992

GH000544/DC