IN THE DATA PROTECTION TRIBUNAL

BETWEEEN:

INFOLINK LIMITED

Appellant

and

THE DATA PROTECTION REGISTRAR

Respondent

(DA/90 25/49/6)

APPEAL DECISION

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

Introduction

1. Infolink Limited ("Infolink") 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. The company provides credit reference and marketing information, credit scoring systems and debt collection services to its customers.

2. Infolink is registered under the Data Protection Act 1984 as a data user who holds personal data. Its register entry (number B11421064) contains a description of the purpose for which it holds personal data as purpose P035 Credit Reference – the provision of information relating to the financial status of individuals or organisations on behalf of other organisations.

3. On 28 August 1990 the Data Protection Registrar ("the Registrar") served on Infolink an enforcement notice under section 10 of the Data Protection Act.

4. On 21 September Infolink served a notice of appeal under section 13 of the Act. With the leave of the chairman the notice of appeal was subsequently amended. The appeal was heard by the tribunal from 15 to 19 April 199. The appellant was represented by Mr Nicholas Pumfrey QC and Mr Richard Arnold, instructed by Booth & Blackwell. The Registrar was represented by Mr Henry Carr and Mr Mark Vanhegan, instructed by Mrs Rosemary Jay, legal adviser to the Registrar. We heard oral evidence on oath from six witnesses. Written proofs of the evidence of each witness, and of one other, were exchanged by the parties and made available to the tribunal.

The CCN decision

5. On 25 December 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 the 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 have had the benefit of argument in the present appeal raising new and different points to those made in the CCN case. Moreover the facts in the present case do not in every

respect correspond to those in the CCN case. However, in correspondence both parties made admissions relating to some of the matters which we decided in the CCN decision and to that extent the earlier decision was not in issue in the present case.

Third party information

6. As a credit reference agency, Infolink 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 Infolink'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.

7. In the CCN decision we gave an example, using fictitious names, based on a complaint received by the Registrar. We repeat the substance of it here, keeping the references to CCN, because Infolink has, by its solicitors, agreed that such a factual situation could occur as a result of their extraction system, though they say that the statistical likelihood of it occurring is minute.

8. The example was based on this situation. In 1985 Mr Simon Jones, a chartered account, sold his house to a Mr J Watson. In 1988 Mr Jones applied to a building society for a cheque guarantee card. He was refused a card. A debtor or prospective debtor is entitled under section 157 of the Consumer Credit Act 1974 to make a request in writing to the creditor or prospective creditor for the name and address of any credit reference agency from which the creditor has applied for information about the applicant's financial standing. Mr Jones was informed by the Building Society that a credit reference had been sought from CCN. Mr Jones applied to CCN under section 158 of the Consumer Credit Act 1974 for a copy of his file. Among the information supplied was an entry showing a judgment awarded in 1987 against Mr Watson. 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 it another way, the only link between them was that they had at different times lived at the same address. Mr Jones was distressed by this incident.

9. Section 159 of the Consumer Credit Act entitles a consumer who considers that an entry in his file is incorrect to ask the credit reference agency either to remove the entry from the file or amend it. CCN refused to remove the entry relating to the judgment but agreed to add a notice of correction stating that it did not refer to Mr Jones. They believed it would not have been right to remove the entry since it was an accurate record of the fact of the judgment against Mr Watson. But it appears that there would be nothing to prevent the same judgment surfacing in any future search against Mr Jones, albeit with the notice of correction appended to it. If there were to be other judgments against Mr Watson they too would presumably surface, but without any notice of correction. Infolink accepted that these comments would equally apply to their system.

10. In accepting that such a situation could arise in their own case, Infolink made the point that one would not know whether "Mr Jones" and "Mr Watson" were the same or different persons, a matter we return to later (paragraph 30, below). It is necessary to say that the extraction of information relating to persons other than the applicant for credit is not an aberration. It is the deliberate policy of Infolink to conduct certain searches in such a way that information which may in fact relate to third parties is extracted, notably where that information is in the public domain, such as county court judgments. As

Infolink's evidence showed, such information is required by their customers, the grantors of credit.

11. Like CCN, Infolink receives a number of requests under section 158 of the Consumer Credit Act from credit applicants for "a copy of the file relating to him kept by the agency". It was explained to us that as a result of advice received from the Office of Fair Trading it is the practice of Infolink when receiving such a request to supply a copy of all the information which it would (or might) supply to a customer even if this includes information not relating to the applicant. In other words, the applicant will receive a copy of any third party information that has been (or might have been) supplied to the credit grantor. Not unnaturally, when an applicant who has been refused credit receives a copy of his "file" which shows no adverse information about himself but adverse information – typically records of one or more county court judgments – about others persons he jumps to the conclusion that the third party information was the reason credit was denied. This has resulted in the Registrar receiving a number of complaints about Infolink. We say "jumps to the conclusion" because it is not always clear what the reason for rejection was, or that there was a single reason; for example, one of the complaints shown to us in the present case was in regard to the refusal of credit to an individual where adverse information about others was supplied but where, in addition, the applicant for credit was himself unemployed at the time he sought a loan for the purpose of buying a second-hand car. We do not know the full facts of that particular case.

The Registrar's duties and powers

12. As a result of the receipt of complaints, the Registrar took action. Various provisions in the Data Protection Act 1984 are relevant.

13. 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.

14. The principle can 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 these proceedings relating to the obtaining of information, or was it suggested that the processing of personal data was carried out unlawfully. This case, like the CCN case, was concerned entirely with that part of the principle that can be reduced to: "Personal data shall be processed fairly". As far as these cases are concerned this is the essence of the first principle.

15. 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 essence of the first

principle are defined in section 1 of the Act, and will be referred to later (paragraphs 53 and 54, below).

16. 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 – for we think that a matter of substance was raised – the Registrar considered the complaints relating to the use of third party information.

17. 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

18. Over a period of years the Registrar, Mr Eric Howe CBE, had discussions with the credit industry in general and Infolink in particular. Being unable to obtain the changes in data processing that he sought, on 28 August 1990 he issued the enforcement notice in this case. As will appear, after the service of the enforcement notice Infolink changed some parts of its system so as to meet some of the Registrar's objections, but a residue remains which is the subject of this decision.

The enforcement notices

19. Counsel likened enforcement notices to injunctions. The operative words 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 Infolink 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.

20. Annexed to the enforcement notice was a statement of the Registrar's reasons for his conclusion that he was satisfied that Infolink had contravened the first data protection principle. This included the following passages:

> "On a search about an applicant for credit, the …. system of processing extracts (for supply to Infolink's customers) address-based information relating not only to the applicant, but also to other individuals who have been recorded as residing at the same or similar current or previous addresses as the applicant".
>
> "The …. system of processing has extracted information about third parties which has accordingly been supplied to Infolink's customers but which does not relate in a material way to the ability to meet the terms of the credit for which the applicant for credit is being assessed ("irrelevant information"). Members of the public, who have been refused credit as a result of such irrelevant information, have complained to the Registrar".
>
> "Principle 1 of the Data Protection Principles requires inter alia that data …. shall be extracted by reference to the individual who is the subject of such data in a fair manner".
>
> "By operating a system which extracts information by reference to the current or previous addresses of the subject of the search whereby irrelevant information is extracted in addition to information about the subject of the search, Infolink are unfairly processing data in contravention of the First Data Protection Principle".

Infolink's database

21. In order to explain how what we have called third party information arises, it is necessary to describe the way in which the information obtained by Infolink is stored and extracted. It is of course stored as data on computer. A statement describing the system of processing was agreed between the Registrar and Infolink, and what follows is based on this statement and the evidence we heard. Changes were made to the system after the agreed statement was prepared, the most recent changes being within the two weeks before the appeal hearing, in April 1991.

22. To provide its customers with information on the creditworthiness of individuals, Infolink stores on computer the categories of information described below. Headings (a) to (i) all come from sources accessible to the public, and may be described as "public information", while headings (j) to (n) come from private sources and may be described as "private information". By using the term "public information" we do not mean that the public has access to Infolink's files – these are of course private and available only to

Infolink's customers – but rather that the information is to be found in public documents or registers as well as on Infolink's database.

(1) Public information:

(a) Electoral Registration Information. This comprises the electoral roles which are updated annually and contains the names and addresses of all persons who are entitled to vote in elections in the United Kingdom (approximately 42,000,000 names at 23,000,000 addresses). The electoral registers are public documents.

(b) Scottish Valuation Roll. This is a list of the valuation for rating purposes of all rateable properties in Scotland. The rolls are produced by regional councils in Scotland and the councils are by law obliged to make the information available to the public. Up to 1989 it was updated annually, but this may not continue due to the introduction of the community charge. The details provided are the names of the occupier and proprietor, the type of property and the rateable value.

(c) County Court Judgments in England and Wales. Details of county court judgments and satisfied judgments in England and Wales are obtained by Infolink from the register operated by Registry Trust Ltd which is open to public inspection. These details are kept on Infolink's files for six years. Infolink also obtains information in respect of judgments which have been set aside and removes the details from its files.

(d) County Court Judgments in Northern Ireland. Details of county court judgments in Northern Ireland are obtained by Infolink from Stubbs Gazette. Infolink retains these details on its files for six years.

(e) Scottish Decrees. Details of Scottish decrees are obtained by Infolink from the register of Scottish Decrees which is maintained by Registry Trust Ltd. Decrees can be cancelled and, additionally, details of satisfactions can be added to the database on receipt of satisfactory evidence either by Registry Trust Ltd or direct from the affected consumer. Infolink retains these details on its files for six years.

(f) County Court Judgments (Channel Islands). Details of county court judgments from the Channel Islands are obtained by Infolink from Stubbs Gazette. They are retained on Infolink's files for six years.

(g) Bankruptcy and Relates Matters. This information is obtained from publicly available sources including Stubbs Gazette and the London Gazette. Bankruptcy information includes records of bankruptcy orders, voluntary arrangements and administration orders. Bankruptcy and administration orders are retained on Infolink's files for fifteen years, and voluntary arrangements for six years.

(h) Bills of Sale. This information is obtained from publicly available sources including Dunn & Bradstreet Gazette. The satisfaction of bills of sale is registered when this information is published. Info link retains these details for six years.

(i) Postal Address File. Infolink obtains this from the Post Office. It contains the name or number of the house, the name and type of street, the post town or district and the postcode of every address known to the Post Office.

(2) Private information:

(j) Default Information. The information consists of details supplied to Infolink by its customers of credit transactions where debtors have defaulted. These details are retained on file for three years. Customers are warned by Infolink only to supply this sort of information in clear-cut cases. They should not notify a default where a debtor is disputing his liability to pay. If the customer subsequently notifies Infolink that the default has been satisfied, this fact will be added to the record; if the customer notifies that the default was registered in error or should be removed for some other reason, all references to the default on the file will be cancelled.

(k) Credit Transactions. This information consists of details supplied to Infolink by its customers of new credit transactions. They include details of the type of agreement (eg fixed term or revolving credit), the date of the agreement, and the amount and number of repayments or the agreed credit limit. Details of fixed term agreements are held for up to six years, and details of open-ended agreements such as budget accounts and resolving credit are held indefinitely.

(l) Previous Searches. A record is kept, for six months, of the fact that a customer has searched against the name and address of an individual. It is also a requirement of the Office of Fair Trading that a record of enquiring customers be kept over a six-month period so that those customers can be informed of any notice of correction that is placed on the file in respect of an individual.

(m) Payment Profile. Customers who participate in the Payment Profile Service submit regular updates of their current consumer credit accounts to Infolink. As well as such information as the date, amount and period of the loan, there is included the outstanding balance, the payment history for the past twelve months, and the date of the last up-date of the file; these last three items are not available to all customers of Infolink, but only to those who participate in the Payment Profile Service. Some bankers currently supply default information as part of the Payment Profile Service; these details are held for six years. Other information is to be kept for two years after completion of the account or after the last up-date.

(n) Credit Industry Fraud Avoidance Scheme (CIFAS). Infolink receives details of individuals appearing on the files of CIFAS. The details provided by the members of CIFAS (the major credit grantors) are the name and address, the type of fraud, the case reference number, and the supply date. These details are retained on file for a period of six months and are only made available to those customers of Infolink who are members of CIFAS.

Data capture

23. Infolink maintain two separate databases: the Voters' Roll (the electoral register, (a) above) and the Credit Register (most of the rest of the information listed above).

24. Adding information to the Credit Register database is a two stage process. First, the given address undergoes a process of validation which includes an attempt to confirm the given postcode (or apply a correct postcode) by using the Postal Address File. Addresses which fail the validation, or for which a postcode cannot be applied automatically, are sent for manual consideration. In most cases a correction or a reformatting of the address results in it being validated and loaded with or without a postcode. Secondly, the data is loaded as a new record or is added to an existing record where the name and address match. To be considered a match, the address must be the same and the surname, first name and initial must be identical, and there must be no conflict in the sex implied by the title. Name data is recorded as received. There is no general minimum level of detail required for it to be added to the database. For instance, the standard format of Payment Profile information only requires surname and initials to be provided, although full forenames are requested. In the case of county court judgments the surname alone is sufficient.

Search techniques

25. The information is supplied by Infolink to its customers in response to searches made by them. The customer supplies Infolink with the appropriate details of name and current and previous addresses of the individual in whom it is interested. Infolink recommends that any previous addresses within the six years prior to the search should be obtained by the customer from the individual so that all the information available can be obtained. Customers may search by post, telephone or telex, or they may have a remote terminal on their own premises through which they can access the Infolink computer which automatically processes the details, the result being transmitted back to the customer's screen or printer.

26. Some of the Infolink's larger customers have established direct links between their main frame computers and Infolink's computer. The customer's computer is programmed to interrogate the Infolink database automatically by reference to the appropriate name and address details. This is usually done in the course of processing a credit application made by the individual to the customer, and the information obtained from Infolink may be used, together with other information obtained by the customer from the individual, in an automated credit scoring system. Such a credit scoring system may be operated by the customer, or it may be operated by Infolink on behalf of the customer.

27. Infolink provides different levels of search, and customers can select the level of information which meets their requirements. What follows is based on the agreed statement and is subject to the later change. Customers may undertake one or more of the following types of search:

    (a) Voters' roll search: customers will receive details of the names of all persons currently registered on the electoral register at the current and previous matching addresses. Where the individual is not traced at the address supplied, other information will be supplied on electors registered at similar addresses where a similarly named individual is registered or at dissimilar addresses where an individual with a very similar name is registered.

(b) County court judgment and bankruptcy and related matters: such a search will produce county court judgment and bankruptcy information which has been registered against one or more individuals, whatever their names, at the current and any previous addresses supplied by the customer. When such information is reported to customers it is classified as either "Possible" or "Other Info" (other information). We explain how these terms are used below (paragraphs 28 and 29).

(c) Customer search: Infolink is able to provide a customer with the data of searches made by any of Infolink's customers within the previous six months in respect of an identical or similar name and an identical or similar address together with an indicator of the kind of organisation which made the search (eg finance, house, bank, retailer).

(d) Default credit transaction and payment profile information: all customers of Infolink may carry out a search of customer-provided default information (excluding bank defaults) and credit transaction information (including some Payment Profile details) held on its credit reference database. Only members of Payment Profile (see paragraph 20, heading (m), above) who provide full Payment Profile details are entitled to see all Payment Profile information and bank defaults. The individuals about whom such information will be provided are those where the name recorded is identical or similar and the address recorded is identical or similar to that supplied by the customer making the search. Where there is no similarity in the name, Infolink will not supply the information even though it is recorded in respect of an identical or similar address. Subject to this, when such information is reported to customers it is classified as either "Possible" or "Other Info" (other information). We explain how these terms are used below (paragraphs 28 and 29).

(e) PACE searches: Infolink offers its customers the possibility of asking for a search where, even if known to the customer, the full name of the subject of the search is not required by Infolink. The so-called PACE search ("Postcode Access Customer Enquiry") may be either an "all information" search or a "public information only" search. In the former, where a search is made of both public and private information, it is necessary to enter the first five letters of the individual's surname (with no forenames or initials) together with the postcode and also the house number or the first three letters of the house name. Information will then be provided by Infolink about individuals in respect of whom the first five letters of the surname match the five letters supplied by the customer and where the postcode also matches. For house names, the first three letters must also match precisely. Where the customer supplies a house number, this must be identical or similar to that appearing in the database; similar numbers would for example be B1 and 1A or 1B. If the same house number appears more than once in the area covered by the postcode, which may happen, the PACE search is aborted and the customer is advised to search using the full address. Where the customer asks for a "public information only" search, which does not report default, credit transaction or payment profile information, Infolink asks for postcode and house number or house name (first three letters) only, and supplies details of all public information found recorded at the address or addresses found which match. The customer may however supply the first five letters of the

surname, in which case the information supplied will be limited to individuals whose surnames match the letters supplied.

28. In the last paragraph we referred to the classification by Infolink of some of the information which it provided to its customers. To be classed as "Possible" the names must match exactly and the address must be considered a very good match with the search details supplied by Infolink's customer. The name "marches exactly" when all three elements are surname, first name and second initial. There must be no conflict in the sex implied by the titles, if given. The address is considered to be a "very good match" when the post town and the street name are the same and the house name and/or number are character for character matches if they present on both the addresses being compared. It does not matter if there are differences in other parts of the address such as the district or postcode.

29. The "Other Info" (other information) which is provided will be details where the name and address recorded by Infolink is similar to that supplied by the customer or the address is identical or similar but the name is not that given by the customer. If this other information is being provided by Infolink staff and not by computer link it will be qualified in the following ways: where the names and address are similar, it will be qualified by the words "we cannot say if identical"; if the address is identical or similar but the name is not, the information will be recorded under the heading "we also note the following in respect of the address shown". According to the Managing Director of Infolink, their customers do not all deal with this other information in the same way; some will use it, and some will not. Those who use it were likely, he thought, to be at the higher risk end of the market.

30. It will be noted that there is no provision for a return showing an "exact match", no doubt because Infolink would say that it is not possible to say from the name and address alone whether the two names relate to the same person or not. Even where the names are given in full and are accurate, it must be said that there may be problems in searching for names. For example, names are not unique, and there may be two or more persons with completely identical names at the same address (they may be related, but this is not necessarily the case). Written evidence was presented to us of a research project carried out for the Registrar on the instructions of the Central Office of Information. This showed that 8.06% of all households on the electoral roll (excluding single person households) contained two or more members with the same surname and first initial, and 0.9% contained two or more members with the same surname and the same first name. Moreover, names may not be fully recorded in the database; a county court, for instance, may have no more information about the name of a defendant than was provided by the plaintiff in instituting proceedings, so that the judgment may be recorded simply against a surname and gender. Some persons use two different names, such as a married woman who retains her maiden name for professional purposes, or a person who changes a name to commit fraud. The customer who searches may not be sure of the correct name of the applicant for credit; this may occur where the applicant has not written legibly and the customer does not wish to go back to the applicant for more information. One frequently meets spelling discrepancies in names; Infolink's evidence was that in their experience public sources of information are less reliable than private sources, and that the more often a name is transcribed, the more chance there is of error creeping in.

31. There are also difficulties in identifying addresses. Words like Road and Street, Avenue and Lane, are not infrequently confused, making it difficult to distinguish between, for example, Acacia Avenue and Acacia Road. There may be two streets of the same name

in the same post town, and without the postcode it may be impossible to distinguish them. District names are unreliable as, for example, Fulham merges into Chelsea.

The matters in dispute

32. Of the five types of search headed (a) to (e) in paragraph 27 above, only two are now the subject of dispute between the parties having regard in part to the changes made by Infolink to their system. As to paragraph 27 (d), the search of the "private information" on the database, the search places great weight on the name of the subject of the search and genuinely seeks only to extract information about that person. The Registrar no longer thinks it necessary to pursue the enforcement notice in relation to such searches and agreed before us that Infolink effectively complies with the notice for these searches of private information.

33. Paragraph 27 (b) details with the search on Infolink's database of public information relating to financial status. Here it is still Infolink's practice to extract the details of any entry found at any of the addresses searched, irrespective of the name to be found on the entry. In other words, the name of the subject of the search carries no weight in the search process if an exact match of the address is found. Infolink will also extract information on entries relating to other addresses if the program regards them as "similar"; here the name is taken into account, but only to the extent that entries will not be extracted unless the name is "similar" within the parameters laid down by the program. The Registrar seeks to uphold the enforcement notice in respect of such searches.

34. Paragraph 27 (e) describes the so-called PACE searches. If the customer requires a PACE search of public information only, he need not supply the name of the subject of the search, but only the postcode and the house number (or first three letters of the house name). Details of the public information at the address will then be extracted. If he wishes, the customer may also supply the first five letters of the surname of the subject of the search, and then the details extracted will be limited to those where the five letters of the surname match. Where the customer asks for a full information search, the first five letters of the surname must be supplied in addition to the postcode and house number. Thus in PACE searches, either no name is supplied or only part of the name is supplied (of course, if the whole surname is five letters or less, the whole surname will be supplied, but in all cases without forenames or initials). The Registrar maintains his objection to both kinds of PACE search, an seeks to uphold the enforcement notice in this respect.

The granting of credit

35. According to the agreed statement, any decision as to whether or not to grant credit to an individual is entirely a matter for the customer. Infolink supplies the information to its customers to use in making that decision. It does not offer advice or express an opinion about the creditworthiness of an individual.

Credit scoring

36. In the CCN decision we described CCN's automated scoring system. We did not hear detailed evidence of Infolink's scoring system, but before the hearing Infolink agreed that it provided automated scoring on behalf of customers and did not seek to qualify the relevant passages in the CCN decision. Accordingly we think it appropriate to

incorporate at this point the relevant passages from the CCN decision, unaltered, as an illustration of how credit scoring works.

37. We said in the earlier decision: The information supplied by CCN to its customers may be in the same form in which it is held on CCN's files, but instead of supplying "raw data" arrangements can be made for CCN automatically to apply the customer's credit rules, CCN notifying the customer of the result as "accept", "reject" or "second opinion needed". Decisions of this type can be based on a policy, such as "reject all applicant sunder 18" or "second opinion for persons not on the voters' roll", or on a credit score.

39. Under the credit score system, a credit scorecard is developed for the customer, allocating points to different items of information, such as the marital status of the credit applicant, the time he has been in his present employment and at his present address, and whether he has a telephone. The information on CNN's files, including third party information, is allocated points, and the decision is made on the total points value or credit score.

39. The credit score can be arrived at by "manual" calculation, or it can be performed automatically. Automation has a number of advantages, including speed, accuracy and confidentiality. In addition the computerised data derived from application forms can be used to monitor the operation of the credit scoring system.

40. CCN provides an automated application processing service to its customers known as "Autoscore", which is integrated with CCN's scorecard development and credit referencing services. Its Autoscore customers communicate with CCN by way of computer terminals which are linked to CCN's computer.

41. It is important to describe how the Autoscore system operates. The customer's terminal operator sends the name and address of the applicant for credit. The computer searches the electoral register file and the postal address file and the address located on those files is displayed on the customer's terminal. The operator confirms that the address shown is correct, and the remaining files are then searched, creating a "credit search record" containing the data, including third party data, retrieved from CCN's files. This record is not displayed to the operator, who is asked to input the relevant items taken from the application form, forming a new "application record". The computer then sends the credit decision ("accept", "reject" or "second opinion needed") which is displayed on the customer's terminal. Each Autoscore system is individually created for a particular customer and incorporates that customer's lending criteria. We were told that although the customer's lending criteria operate on CCN's computer, CCN acts only on behalf of the customer, who makes his own lending decisions.

The extraction of third party information

42. In paragraphs 33 and 34 above we identified the matters which are still in dispute between the parties. To the extent that a search is made without reference to a name at all, as is possible in the case of PACE searches of public information, or that no match with the name supplied is required, as with other searches of public information, the search leads to the extraction of all names found at the target address and it is inherently likely to extract information about "third parties" – individuals other than the individual known to Infolink's customer with whom it is contemplating some business transaction. These individuals may be members of the applicant's family and share the same surname and, possibly, initials or forenames, or members of the family with different surnames, or persons living with the applicant for credit, or friends, or tenants or lodgers, or estranges

spouses. They may have financial links with the applicant for credit, as is sometimes the case with spouses and children, but they may well be completely financially independent of the applicant. However, they may have nothing whatever to do with the applicant for credit, but simply be persons who have at some time lived at the same address as the applicant, at different times – "non-concurrent" – as in the example of Simon Jones we gave in paragraph 8 above.

43. As we have noted, in PACE searches of private information the customer is required to supply the first five letters of the surname of the subject of the search (with no forenames or initials), and this is also an option open to the customer in searching public information. In these cases the name does play a role in the extraction process, because only information relating to persons where the letters supplied match will be extracted. The question we have to consider is whether this should be regarded as much the same as address-only extraction, or whether it is a genuine attempt to extract information relating to the subject of the search alone.

44. Mr Pumfrey, appearing for Infolink, emphasised how small the problem was, since PACE accounted for only about one percent of Infolink's business. Having regard to the fact that Infolink conducts about thirty million searches a year, however, it seems to us that even the one percent represents a very large number of searches – in the region of three hundred thousand searches a year. He asked whether there was an appreciable chance that the search might show a county court judgment against the wrong person. Given the number of county court judgments alone featuring in Infolink's database, we think it follows from the evidence we have heard that there is an appreciable chance. Infolink's database retains county court judgments for six years, and Infolink's customers are asked to provide all the addresses where the subject of the search resided in the past six years. Mr Beer, Infolink's Systems Auditor, agreed that it was inevitable that in searches where the name was not the determining factor, county court judgments against previous occupants of the subject's current address and judgments against current occupants of previous addresses, among others, would be extracted. He told us that about two million judgments were added to the database each year, so that it would include about twelve million judgments at any one time.

45. Mr Pumfrey also pointed out that there were no complaints produced by the Registrar relating to PACE searches and no evidence of dissatisfaction with the result of a PACE search. Although we do not know how it was possible for the Registrar to identify whether a complaint relates to a PACE search or not, we acknowledge that the onus is on the Registrar and agree that no evidence identifying PACE searches as supplying third party information was produced. Nevertheless, section 10(2) of the 1984 Act does not require the Registrar to find that there has been any actual case of a person suffering distress before he may issue an enforcement notice.

46. Since Infolink does not require the customer to supply any name when making a PACE search against public information, in our judgment this is a clear example of a type of search likely to extract third party information and where no steps at all are taken to limit or exclude the extraction of third party information. We find that the chance of this happening is such that it would have been wrong for the Registrar to have ignored the question.

47. There is the other kind of PACE search where the customer chooses to, or is required to, supply the first five letters of the surname of the subject of the search. In our judgment the omission of any forename or initials would clearly lead to the chance of confusion

with other persons bearing the same surname, but the matter goes further than that. Many names are more than five letters long, and for these the system adopted accepts that information about persons with different surnames cannot be eliminated from the process of extraction. We do not agree with Mr Pumfrey that there is no appreciable chance of information about the wrong person being extracted. An example given by the tribunal drew attention to the number of names ending with the suffix "-son", such as Williams and Williamson, where the five-letter method would be incapable of distinguishing between the different names with and without the suffix. There are of course many other examples.

48. In our view these searches are designed in such a way that they will produce third party information in many cases. We think this view is supported by the letter from Mr Brian Bailey, the Managing Director of Infolink, to the Registrar, dated 26 January 1988, to which our attention was drawn. In this letter Mr Bailey referred to the fact that some competitors operated on an address match only basis, stated that this had left Infolink at a commercial disadvantage, and told the Registrar that it was to rectify this that Infolink had introduced PACE searches to search for public information on a postcode basis. It is clear they were introduced so as to supply Infolink's customers with third party information.

49. There was some discussion before us as to the value of third party information. As we said in the CCN decision, we are 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.

50. In correspondence Infolink accepted a number of the points relating to third party information which we made in the CCN decision. In particular, they agreed that there is no identifiable causal link between information which does in fact relate to a person unconnected with the applicant (ie who is not a member of the same economic unit) and default by the applicant. Surprisingly, this lack of link does not impair the predictive value of the information. Although Infolink did not accept our finding that the value of third party information arises where the details known about the applicant for credit are not adequate, they accepted that information which may in fact relate to the third parties is useful in such circumstances.

51. In the CCN decision we mentioned the different views of what was relevant taken by the parties. CCN used the word to mean "relevant to the question whether the credit applicant was a member of a group or class if persons of whom a certain percentage would be likely to default". In this sense we accepted that third party information was to some extent relevant. The word was used by the Registrar to mean "relating to the individual applicant for credit". In this sense third party information may or may not be relevant, and even if it is agreed to be relevant in the first sense it will often be irrelevant in this second sense. Infolink accepted our definition of "relevant" (we assume this means our analysis of the meanings), and in addition contended that information was "relevant" if it might in fact relate to the applicant for credit although it apparently did not, with allowances being made for (i) the quality of the data being searched and (ii) the precision achievable with the search algorithm being employed. For our part, we accept that information is relevant if it does in fact relate to the applicant, whether this fact is known or not.

52. Infolink's witnesses were curiously reluctant to admit that an application for credit might be rejected because of third party information, but in the end the Managing Director of Infolink agreed that this might happen. In our judgment the presence of third party information can lead to an applicant being refused credit.

The Registrar's case

53. The essence of the Registrar's case is that extracting address-based information produces, and is designed to produce, irrelevant information in the sense in which the Registrar uses that word, and that this is unfair to the individual credit applicant. The legal basis of the Registrar's action is his finding that the extraction of third party information is unfair processing and therefore in breach of the first data protection principle, the essence of which, for present purposes, is: "Personal data shall be processed fairly".

54. "Personal data" is defined in section 1(3) of the Data Protection Act as "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), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual". By section 1(2), "data" means "information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose". It was not argued before us that the information relating to or alleged to be relevant to an applicant for credit, retrieved from the database by Infolink for supply to their customers, was not personal data, but argument did centre on the rest of the first principle: "processed" and "fairly". It is necessary to look at these terms in order to decide this appeal.

Processing

55. The word "processing" is defined in section 1(7) of the Data Protection Act as follows:

> "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".

56. There was no real dispute that the crucial part of the definition in the present case was "extracting the information constituting the data", but there was disagreement as to what precisely was involved in extracting information. One view was that this meant that the computer was operated so as to produce one of three things: information in the form of sheet of paper; information revealed on a screen; or information – perhaps data would be a better word – fed into a scoring program. Mr Pumfrey did not accept that this amounted to the extraction of information. He argued that extraction does not take place until the information was used for its purpose, and asked whether extraction took place at a stage when the information extracted was seen by no human being and had no objective effect. He used two striking metaphors: until the information was put to use it had no reality, it was an unopened book; and he likened extraction without use to someone shouting in an empty room – you could not say that he had said anything if no-one had hard it. Information, he said, is something that informs, and it does not inform until it is used by the credit grantor for the purpose of granting credit.

57. In our view, the metaphors equally support a contrary argument. An unopened book contains as much, and the same, information as the same book opened, and we are in the

realm of metaphysics if we deny that someone has spoken because no-one has heard. We believe that it is perfectly possible to say that information is extracted at a stage before a human being looks at the screen of the video display unit or the sheet of paper and, as far as credit scoring is concerned, the information extracted is used without any human being seeing it. We are plainly concerned, in the definition in section 1(7) of the Act, with the "performing [of] operations" by a machine, and extracting for present purposes leads to what is produced by the machine at the end of the extraction process.

58. Mr Pumfrey suggested at one point that his argument might resemble the argument in the CCN case that extraction could not be fair or unfair but, being an automatic process, was value free. In the CCN case counsel for CCN argued that the representation on a screen of paper of what existed in the database could not be unfair unless, perhaps, it was false. Without adopting the identical argument, which we had rejected in the CCN decision, Mr Pumfrey argued that extraction could only be unfair if it involved a breach of privacy. This was put by Infolink in the notice of appeal as follows: "The Registrar ought to have held that the applicant's personal data is only unfairly processed if it processed in some manner which involves a breach of the applicant's privacy (eg by disclosure of his race or political opinion or sexual orientation); and that the inclusion of information concerning third parties is incapable of amounting to a breach of the applicant's privacy".

59. Mr Pumfrey gave us an example based on a number of suppositions. Suppose the database records of a person's race or religion. Suppose, he said, the lender, Infolink's customer, will not lend to persons of a particular race or religion. Suppose the credit scoring facility is programmed automatically to reject persons of the particular race or religion. In this case, a person would be rejected by the program without any disclosure to anyone. This, he suggested, was an example of unfair processing: the extraction of data would be unfair because on no reasonable view could that information be treated as relevant to the registered purpose. But where the information might be relevant, one could not conclude that its extraction was unfair. We were told that this example made it clear why the definition of processing included extraction, namely to catch this short of "invasion of privacy" case.

60. We do not find this argument convincing. The example may indeed be one of unfair processing, but we see no reason to think tat invasion of the data subjects privacy, if that is what the example is about, is the only type of unfair extraction.. There is no indication in the Act that is the case, and there is no reason to think that Parliament had just one example of unfair extraction in mind. There may be many ways in which information can be extracted unfairly. As we explained in the CCN decision, in our view the program instructing the machine what to extract can be unfair if it is deliberately designed to extract certain information for the registered purpose. The unfairness lies in the instructions to extract, for the purposes of credit reference (the provision of information relating to the financial status of an individual), material irrelevant to the individual who is the subject of the credit reference. We use the word irrelevant here not in the sense of having no predictive value in the aggregate but as referring to a person whose activities are not related to the creditworthiness of the subject of the reference. (in his example, Mr Pumfrey said that the extraction of information in his example did in fact relate to the subject of the search, and we can imagine a credit reference agency arguing that such information was relevant because it was predicative).

61. We find that the extraction of information about persons other than the subject of the search is the result of Infolink's deliberate policy of searching for information by reference to addresses, and not by names, as is done in searches for public information, or

by reference to addresses where inadequate information on names is used, as is done in PACE searches, whether for public or private information.

Fairness

62. We now come to the question whether the processing that we have described may be said to be unfair. In our CCN decision we referred to the argument that fairness involved "a balancing of competing interests, so that in judging whether processing was fair we should set against any possible unfairness to the individual the advantages gained by other individuals, the benefits to the grantors of credit, and the public welfare".

63 We said in that case that we were "very conscious of the benefits of reliable credit reference and credit scoring systems in preventing over-commitment by debtors, a measure very much for their benefit and that of the community, and in ensuring a well-managed credit system for the benefit and that of the community, and in ensuring a well-managed credit system for the benefit of potentially sound debtors and of the credit and supply industries". We also found that the purpose of the Data Protection Act "is to protect the rights of the individual about whom data is obtained, stored, processed or supplied, rather than those of the data user. The Act was the result of concerns about the use of computer data, concerns voiced in Parliament and in the reports of a number of representative official committees and widely held throughout Europe (hence the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data opened for signature on 28 January 1981 referred to in sections 37 and 41 of the Act)". We might also have noted Mr Carr's argument that in a number of its provisions the Act expressly takes account of the public interest, as in sections 27 to 34 and section 12(4), though we do not think that means that no consideration may be given to the public interest elsewhere.

64. In the CCN case we came to the conclusion that "in deciding whether the processing we have described is fair we must give the first and paramount consideration to the interests of the applicant for credit – the 'data subject' in the Act's terms". We added that we were not ignoring the consequences for the credit industry of a finding of unfairness, and that we sympathised with their problems. Later we added the following: "although we have concluded that fairness is to be judged primarily by reference to the data subject, we have taken account of the interests of CCN and of their customers, the credit industry, in considering whether the Registrar has exercised his discretion properly".

65. In the present case, Mr Pumfrey referred to our ruling in the CCN case that we must give the first and paramount consideration to the interests of the applicant for credit. He took this to mean that the applicant's interests prevailed over all other interests and argued that if this was intended by the Act it would not have introduced the concept of fairness at all. We do not think this adequately sums up our finding in the earlier case. We do not think "paramount" bears the meaning that it is the only consideration, but rather the most important single consideration. In other words, we are to weigh the various considerations, and do so, but are entitled to give more weight to the interests of the individual about whom the credit reference enquiry is being made.

66. Mr Pumfrey made a number of other points. He argued that since information such as county court judgments is made public, it is the policy of the Government (he used the expression "public policy") that such information should be publicly available, and that Infolink advances this public policy by making the information accessible. We certainly accept that there is a public interest in having access to records of county court

and other judgments and other public information, and we do not quarrel with the making of public information available to Infolink's customers. Objection is taken to a much narrower activity: the alleged unfairness of extracting information for the purposes of credit reference about third parties not financially linked with the individual seeking credit.

67. Mr Pumfrey went on to argue that since Infolink's customers could themselves search public records, for example of county court judgments, it would not be said that the extraction of such public information could be unfair. We do not agree with this. Collecting all the public information on Infolink's database admittedly serves the public purpose of making the information accessible, but it is unrealistic to suggest that Infolink's customers might have been able to spend the time to research the public files to discover, not only information about the individual in whom they are interested ("the subject of the search"), but also about other individuals whose only feature is the sharing of an address with the subject of the search. This use of computers to extract a large body of information which may or may not be relevant is one of the activities the Act is, in our view, intended to regulate.

68. Mr Pumfrey took the point that the credit industry was regulated by the Office of Fair Trading under the Consumer Credit Act, and suggest that it was for the Office of Fair Trading to put an end to reliance on third party information, not the Data Protection Registrar. This is an interesting point, but does not concern us. It emerged clearly from Infolink's own evidence that the use of third party information is directly related t the ease of extraction of such information by reason of the use of computers. The Registrar has found a contravention of one of the data protection principles, and has taken action under the Data Protection Act. It is that action that is the subject of the present appeal.

69. Counsel went on to draw attention to the fact that under section 10(1) of the Act the Registrar may serve an enforcement notice only if he is satisfied that Infolink has contravened or is contravening the relevant data protection principle. The Registrar, he said, must demonstrate as a minimum that it is more likely than not that a class of individuals will have its data processed unfairly. This was in contrast with what was said to be the Registrar's argument that processing must be fair in relation to each individual. If it is necessary for us to do so we find clearly that the risk of unfair processing, to which we return shortly, exists for all individuals in respect of whom a search for public information or a PACE search is made by Infolink, potentially a very large number of persons, and if there is unfairness the Registrar had good reason to be satisfied that there was a contravention of the first principle. Infolink's policy of searching so as to supply details of all public information entries against the same address, past or present, whether the name is the same or similar or not, is designed to extract information about complete strangers. The same comments apply to PACE searches. We reject Mr Pumfrey's argument that the contravention, if there is one, must be regarded as de minimis.

70. In presenting his case, the Registrar gave the tribunal information about fourteen of the complaints he had received against Infolink, as he said, and mentioned seven more complaints, details of which had not been supplied to Infolink but the files in respect of which were, he said, available for Infolink's inspection. As to the additional seven complaints, these were criticised by Mr Pumfrey as hearsay upon hearsay upon hearsay. Although Rule 18 (1) of the Data Protection Tribunal Rules 1985 says that we "may receive in evidence any document or information notwithstanding that such document or information would be inadmissible in a court of law", we have not relied upon these

seven complaints. As to the fourteen complaints, various criticisms were made of them by Infolink including in at least one case the allegation that the search complained of had not been carried out by Infolink and must have been carried out by another company. We think that some of the criticisms are justified, but even if all fourteen complaints are disregarded we do not think that that destroys the Registrar's case. The Registrar is in effect instructed to consider complaints in exercising his discretion by section 10(2) of the Act:

> "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".

As we have already said, we do not think this provision debars the Registrar from serving an enforcement notice even if there is no actual case of a person suffering distress. Whether or not any of the fourteen cases presented to us survived Infolink's attack, we find that having regard to the way in which Infolink admittedly conducts searches they may be regarded as illustrations of the sort of thing that is inherently likely to happen, and which we are satisfied will have happened on more than fourteen occasions. For this reason we have not described each of the complaints presented in detail.

71. None of the complaints would lead us to find that the contravention had caused damage to anyone, but several of the complaints showed at least the possibility of distress. Mr Pumfrey made the point that the evidence showed that most of the distress was caused by the belief that credit had been refused as a result of the use of third party information rather than of its extraction. This is undoubtedly true, but it could be said that that is a natural consequence of the extraction.

72. Following on from the points just referred to, Mr Pumfrey argued that it was not possible, looking at the way that Infolink works, to say that there was a contravention of the first principle. It might be possible to gather a group of persons whose data had been unfairly processed, and the common element in those cases might be the subject matter of an enforcement notice. But the Registrar had identified a method of processing that might or might not be fair, so there was here no evidence of contravention. The onus is on the Registrar to justify the enforcement notice, and he had not even started to distinguish in a satisfactory way why some cases were fair and others unfair. It will be clear from the findings we have already made that we do not accept this argument. While we do not seek to uphold the enforcement notice in the terms in which it was served by the Registrar, we find that the evidence clearly shows that Infolink's methods involve a contravention of the first data protection principle.

73. The evidence in this case, notwithstanding the arguments presented by Mr Pumfrey, has brought us to the conclusion that it is unfair for a credit reference agency so to program the extraction of information as to search for information about all persons associated with a given address or addresses notwithstanding that those persons may have no links with the individual the subject of the enquiry or may have no financial relationship with that individual. We believe this to be so even if the customer has requested address-based information and notwithstanding what is said to be its predictive value.

The Registrar's discretion

74. We have found that contravention's of the first principle are involved. But this does not mean that we take the view that the enforcement notice is justified in its entirety. The

Registrar is not bound to serve an enforcement notice but has a discretion, and we consider that he should have exercised this discretion differently. A major part of Mr Pumfrey's argument was designed to show that that Registrar's enforcement notice was defective or too wide. In our view there is a need to distinguish between different sets of circumstances in a way that is not to be found in the enforcement notice, and to this extent we find that the terms of the enforcement notice must be varied. This we propose to do by exercising our power under section 14(1) of the Ac to substitute such other notice as could have served by the Registrar.

75. The purpose of an enforcement notice is set out in section 10(1) of the Data Protection Act. It is a notice requiring a registered person to take such steps as are specified in the notice for complying with the principle in question, in this case the first principle. The enforcement notice served by the Registrar, cited in paragraph 19 above, in our view goes beyond what is needed to bring Infolink's procedures into line with the requirement to process fairly. Although we think that it is unfair to extract information by reference to addresses indiscriminately, we do not take the view that every extraction of third party information is intrinsically unfair, and this is why we believe that the Registrar should have exercised his discretion differently.

76. Mr Pumfrey made a number of criticisms of the terms of the enforcement notice served by the Registrar. Many of these we accept: indeed, several of them mirrored points we had ourselves taken in the CCN decision. For example, he pointed out that even a search based on name and address might be said to be processed by reference to the address and, given the difficulties as to searching by name (see paragraph 30 above), was bound to catch persons of the same or similar name to that of the subject. This was the sort of point we had in mind when we attempted to vary the Registrar's enforcement notice in the CCN case. On several occasions he made the point that it was meaningless to talk about "the subject of the search" because names were not adequate identifiers. This we do not accept: we think everyone understands the "the subject of the search" is the person with whom the credit grantor or supplier intends to contract with; we do of course agree that where at the same address it may be impossible to tell which is the subject of the search. It is a valid criticism of the Registrar's enforcement notice that it fails to recognise that a search may extract the very name of the subject of the search and yet refer to another individual, apparently a breach of the enforcement notice leading to possible criminal liability under section 10(9) of the Data Protection Act (subject to the defence set out in that subsection).

77. In the CCN case we said that "The present search procedures are unfair, but if they were revised so as only to retrieve information about persons who were reasonably believed to be closely financially linked with the subject of the search we would not have found them to be unfair". We now think it is possible to explain this finding in more detail. We also said in that case that "We appreciate that the Registrar takes the view that all address-based searches are likely to produce irrelevant (in his sense) third party information, but we do not believe that that is necessarily so. It is not for us to devise a method of extracting information that would confine itself to the relevant (in the Registrar's sense), but having seen the expertise possessed by CCN we would not wish to rule out the possibility that, perhaps on the basis of requiring their customers to obtain more information from applicants for credit where this is feasible, and by extracting by reference to names as well as by addresses, they may be able to do so. If they cannot do so, our version of the enforcement notice would no doubt have the same practical effect as the Registrar's; but if they can devise an appropriate extraction program they will be able to utilise that amount of third party information the extraction of which would not be

unfair. We therefore do not rule out address-based searches, provided some means is devised of limiting the information thereby extracted to that relating to relevant (in the Registrar's sense) persons".

78. The fundamental difficulty with the Registrar's enforcement notice is that it not only inhibits address-based searches producing third party information, it could also make it impossible to frame a search designed to produce information about the subject of the search (see paragraph 76 above) only. For example, two persons named Robert Jones live at the same address at the same time (we may even assume they are father and son). Neither Infolink nor their customer may know this. A search against Robert Jones at the address is, at least in part, address-based. The search may turn up information – judgments, perhaps, or credit agreements – against either or both persons. If it turns up information about the subject of the search only, the enforcement notice has been complied with. If it turns up information about both persons, or about the other Robert Jones, the Registrar's enforcement notice has been contravened. We think the enforcement notice must be qualified so as not to prevent such a search.

79. A related situation is where the forenames of the subject of the search are not known but only his or her initials and sex.. Here a search is more likely to turn up a different person, but this again would be an unavoidable by-product of an attempt to find entries about the subject of the search and should not involve a breach of the notice. A further variation, which cannot be ruled out, is where only the surname and sex of the subject of the search is known; here it is even more likely that a search designed to find information about the subject of the search would turn up information about third parties, and no breach of the notice should be caused as a result. In none of these cases, or the following cases, should information be extracted save in respect of an address at a time when the subject of the search resided there.

80. The next question is in connection with persons sharing the surname of the subject of the search and living at the same address at the same time. Here we believe that a program designed to extract information about the persons with the same surname should be permitted, since it would be a reasonable inference that they were living as members of the family of the subject of the search in a single household unless there were any facts known to Infolink to counter such an inference. For example, the existence of a correction giving notice that there was no connection between the two persons should prevent information about the person other than the subject of the search from being extracted. In our CCN decision we concluded that it would not be unfair to extract information about such persons, a view now, we think, partly supported by research conducted by the Policy Studies Institute and funded jointly by the Registrar and the Industry Forum on Data Protection. The Institute summarised the findings of the research as providing "fairly clear evidence that there is an association between the repayment records of husbands and wives; [that] this link is large enough to be taken seriously as a potential predictor of default, but accounts for only a small proportion of all arrears; [and that] there is a much weaker, if any, link between members of a household other than husbands and wives". Our judgment that it would not be unfair to extract information about persons with the same name in the same household at the same time was not based on the predictive value of the information but rather on what we saw would be widely recognised as fairness, a view we still hold. We recognised that this view would not be universally held, but felt that a judgment could not be made until the information was available, and that extraction was therefore not unfair.

81. Members of the same household do not necessarily share the same surname. One can think of many reasons for this. A wife may not have adopted her husband's name. The couple may not be married. Married daughters may live at home. Whatever the reason, the fairness identified in the preceding paragraph would apply equally where the names differed, but the point of difference is that no assumptions or inferences can be drawn from the names. To constitute fair extraction, therefore, we think that there must be some additional information, information arising before the extraction takes place. We put it more fully in the CCN decision, as follows: "On the other hand, it would not be fair to produce a program which automatically extracted, for the purpose of credit reference, information about persons with different surnames, whether or not living at the same address. It might be argued that such information could relate to the subject, using a different name whether for legitimate or fraudulent purposes, or to another person with a different name but a member of the subject's immediate family or household and financially linked, such as a spouse who uses a different name, or a person living with the subject though not formally married, or a married daughter or son-in-law or other in-laws. There are doubtless other possibilities as well. Although any of these situations could exist, we do not consider that an automatic extraction program made as a matter of routine would be fair. If sufficient facts were known, such extraction might well be fair, but if it is desired to extract such material it would not be as a result of an address-based search made as a matter of routine but as the result of a deliberate decision, based on the particular facts, to search for and extract such information".

Form of enforcement notice

82. We propose 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 have made. It will be convenient, after this part of the decision is made available to the parties, to contravene a further hearing to hear representations by the parties on the terms of the enforcement notice, and the hearing is accordingly adjourned to a date to be arranged for this purpose.

Time for compliance

83. 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 to time for compliance, but it appears that Infolink 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.

8. Taking into account the evidence we heard as to the time necessary for creating new computer programs and scorecards, it would be appropriate to allow sufficient time for the work to be done. A period of between 18 months and two years should be adequate, and accordingly the date for compliance should be 1 January 1993.

Conclusion

85. 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.

86. 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.

Chairman

31 May 1991

IN THE DATA PROTECTION TRIBUNAL

BETWEEEN:

INFOLINK 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 6 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 19 February 1992. We heard submissions by counsel 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 19 February 1992 we were asked by Mr Pumfrey, leading counsel for the appellant, to reconsider that date, having regard to the date of the adjourned hearing, the delay after the first part of our decision before Infolink Ltd would have the definite text of the enforcement notice and the unfairness of prescribing different dates for competing companies. We have reconsidered the date, and think that in the interests of justice it is necessary to give more time than we envisaged last May. 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 Infolink Limited 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 of 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 Infolink Ltd 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 Infolink Ltd 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