Employment and Privacy: A Problem for Our Time

M. Newman
G. Marks de Chabris

ABSTRACT. The employment application form is a major source of information about candidates for many companies. It is also a potential source of infringement by the company upon the privacy of the individual. Although September 1984 saw the passing into law of the Data Protection Act, the U.K. has not been in the forefront of civil rights where employees and personal information are concerned. During an extended interview with members of a personnel department of a major company, several issues relating to privacy issues were revealed and these are discussed in the paper. Although these interviews were carried out before the new law came into effect, they do show that this and many similar organisations may experience problems over compliance. This is particularly likely in the computerisation of personnel records and employees' access to their personal information.

Privacy and employment

Terms such as 'privacy', 'data protection' and 'individual rights' have been brought to the fore and into everyday conversation by the expansion in the civil rights movements seen in many Western countries, including the United Kingdom. Resulting from this movement has been the demand that personal information collected about an individual by governments and other organisations should be presented through the implementation of legally or voluntarily binding privacy principles. Schein (1976) identified three factors which have made a special contribution to the emergence of this movement, namely:

1. advancing computer technology;
2. the uncertainty of an individual's legal position and protection of his privacy;
3. the new views which have emerged on privacy.

Many writers (for example, Westin, 1979; Hoffman, 1973; Sieghart, 1976) have become interested in privacy issues because of a growing concern about the almost daily technological advancements in computer science and because of greater public awareness of the impact of this technology, following such publications as George Orwell's *1984*, and Vance Packard's *Naked Society*. While the costs of introducing and implementing a computer system are continually decreasing, rapid advancements are simultaneously being made in the quantities of data which can be held and the speed at which this information can be processed. Westin and Baker (1972) attribute the growing interest in this subject to human fear: fear of what data is recorded and fear of how it is used.

Throughout one's life, knowledge and records about individual members of society are being assimilated and collected. As governments accept an increasing role in social responsibility, so the types and quantities of data collected have had to be modified in order to assist the system in its proper administration. Industry has a personal interest in discovering more not only about its markets, products and consumers, but also about the factors used in production, including its personnel. Through the use of personality tests and other screening procedures, which disclose increasing amounts of data about employees, it is possible to exert a greater

Michael Newman is Lecturer in Accountancy at the University of Manchester and Visiting Assistant Professor at the University of Connecticut. He has been awarded a grant by the Economic and Social Research Council, U.K. for his project 'The Introduction of Information Systems into Organisations', 1985/87. He is one of the authors of Accountants' Roles in Industrial Organizations and Access to Information. *He has also published several articles.*

Gloriana Marks de Chabris is Junior Accountant at Price Water House (Accountants).

Journal of Business Ethics **6** (1987) 153–163.

control over the process of selection and, hence, the make-up of the labour force. Additionally, individuals reveal personal information almost unnoticingly to private organisations such as building societies, credit bureaux, banks etc., many of which utilise computer systems for recording and storing such data.

An early concept of privacy was that the individual had the ability to prevent information about himself being collected or abstracted by others. This view has, over time, been amended and extended to encompass the individual's control over the dissemination and use of personal data, that is, the confidentiality with which such data is treated. For an organisation to operate efficiently and effectively within this society, it is essential that various pieces of personal data be collected. Furthermore, as in the case of the census, there may be legal sanctions to enforce compliance. The new focal point is, instead, how best to protect and safeguard the right of the individual against unwarranted use or unauthorised access (OECD, 1976). As Miller echoes, "the basic attribute of an effective right to privacy is the individual's ability to control the circulation of information relating to him" (1976: 25). Thus information is considered personal property to be used in the manner selected by the individuals and where its misuse is the violation of this right.

It is this modern view of 'privacy', coupled with the growing uneasiness as to the legal rights of the individual and the rapid advancements being made in computing, that has kindled the move to protect the rights of individuals to privacy. In an employment context, the emphasis is upon:

1. What information the organisation collects about its employees? Is the individual aware of the assessment and the mechanisms used?
2. How such material is used; legitimately as intended, or illegitimately?
3. Who has access to such data (both within the organisation and outside)?

However, there is an initial problem to be examined, that of defining the term 'privacy'.

Definitions of privacy must be somewhat culturally dependent. Therefore, the pattern of legislation or voluntary protection followed by one government may be entirely unsuitable for the problems of employees' rights faced in another country. Kovach (1976) notes that when first introduced, photographic equipment and communications by telephone and telegraph were seen as invading the privacy of the individual in a similar way in which personality, intelligence, and polygraph tests are currently viewed. As society changes, so there is a change in the problems it faces.

'Privacy', 'citizen's rights' and 'individual rights' form part of the set of terms used to describe the entire field of private personal information; its use, collection, and distribution. Writers frequently neglect to define what they perceive 'privacy' to mean and use the term in a variety of contexts, each of which may have a different meaning. "Privacy", Margulis (1977) states, "like many abstract concepts in common speech suffers from definitional ambiguity and vagueness". Indeed Wolfe and Laufer (1974) in their study of 'The Concept of Privacy in Childhood and Adolescence' found thirty nine different yet distinct meanings which were attributable to the term 'privacy'. Of these, the four which predominated were:

1. controlling access to information;
2. being alone;
3. controlling access to space;
4. no one bothering me.

A sample of the range of definitions frequently found in the literature on this topic, vary from merely considering the control an individual can exercise over information about himself, to broader definitions, as advocated by Schein (1976) encompassing wider aspects, such as the attitudes of the employee and job applicant to selection and assessment procedures and how these are seen to impinge upon the privacy of the employee.

However, not all data is as private or sensitive as some. Therefore, in defining the term "employee's rights" different people will regard different pieces of information as being personal and interpretations of what is understood by "private information" will be equally as varied. For example, medical details may be more private to some than for others and the employee's perception of the sensitivity of this data will affect his reaction to the methods used by an organisation for handling such data. These differences are important considerations which should be taken into account in using such terms or when trying to extract a definition.

A further distinction to be drawn before dis-

cussing privacy in depth is introduced by Sieghart (1976) in his book *Privacy and Computers*, differentiating between the need for privacy and the right to privacy. Realising the need serves to clarify why the right to privacy has been the cause of such a debate. The Justice Report explained that:

> Man is a social animal. No human being can exist for long in total isolation from all others. Yet we also have a need to withdraw from others to a greater or less extent at different times of our lives . . .

The quest and need for privacy is a natural one, exhibited not only in man, but found as well in many animals as part of the biological and social processes upon which animal existence depends. This view is restricted by Klopfer and Rubenstein, who examine the fundamental biological basis of privacy and note that: "The degree of character of the privacy an organisation attains must represent a compromise between competing forces . . ." (1977: 54). This reflects the conflict between the individual's need for privacy and the organisation's quest for greater disclosure. For the employee, the desire to influence the collection, use and dissemination of his personal information is largely rooted in human nature. For the employers, their requirements to accumulate data not only about their employees, but concerning all parts with which they interact, are an attempt to control the organisation's environment.

One of the great fears which arises from the 'secrecy' of personnel files, is that these mistakes may be recorded in a mechanical fashion and recalled out of context. Employees fear that they may be 'labelled' throughout their working career by one particular instance which may have occurred many years previously or many jobs previously and that their rate and path of advancement has been hindered by this single incriminating factor. Arguments of this kind have been offered in proposing that employees be allowed the chance to examine the files maintained on them, to contest the information contained within them, and have this data amended.

The need for privacy is, therefore, more than merely the biological necessity of "the need to be left alone". It extends further to include the freedom to keep the past from interfering with the future and the ability of the individual to control the destination of confidential communications (Rothman and Mosmann, 1976). In contrast to the need for privacy, the right to privacy is the right of the individual to decide for himself how much of himself (his personal life and its details) he will share with others.

People, by necessity, desire privacy in varying amounts and at various times in their lives. Hence, the debate in Western countries is no longer whether such a need exists but rather, to what extent people (employees) should be entitled to choose the degree of privacy they wish to exercise in their lives, while competing forces (employers; governments) try to prevent them from practising such a choice. This dispute necessitates the use of value judgements, complementing the standards and norms set by society and in line with other methods for resolving disputes adopted in legal, philosophical or political debates.

Advances in data processing technology have focussed attention more sharply on the privacy issue. Besides a growing awareness that the computerisation of an organisation's personnel system may facilitate the extension and addition of forms of data collection and storage, the employee has also become concerned that inaccurate, incomplete and out-of-date material will be collected and used in decisions. If the individual is unaware of the existence of such records and cannot, therefore, check or verify their contents, he may suffer, financially as well as psychologically. Furthermore, unless the systems of data storage are known to be secure, adverse behavioural reactions may ensue and the individual employee be tempted to supply misleading or incomplete information.

Automation of personal data can have other implications for privacy as, for example, it affords the facility for collecting together a number of independent pieces of information, which together will have a greater impact than each piece individually. Niblett claims that employees and the general public are concerned with the : "ability of the computer to reorganise a large quantity of information (each element of which is separately harmless) into a new quality of information, which may reveal more than he wishes to be known" (1971: 21). The widespread use of computers and the ever increasing knowledge of programming techniques could mean a greater risk of unauthorised transmission or access. Consequently, organisations have had to consider different security needs

depending on whether information is dispensed over a number of locations or located in a central databank, access to which can be simultaneously obtained from a number of remote terminals.

However, it is clear that computers are not the villains per se, and that equally damaging information can be found in manual files. What the advancing rate of computer technology does do is bring the possibility of information being more easily available in large quantity to those with the skills to obtain it. Nevertheless, there are a number of advantages in favour of maintaining records in this form which should be used in assessing a system of this kind (see, for example, Westin and Baker, 1972). Even from the earliest start of the civil liberties movement, the uncertainty of the legal protection afforded to the individual has been apparent. It is a moot point as to the amount of legal or voluntary regulation needed to protect data privacy and whether such legal protection can be given, should be given, or is even feasible. The stance adopted by particular governments has varied considerably between countries (Sieghart, 1976).

The case study

The organisation selected for the case study is the largest subsidiary of a worldwide corporation operating in 120 countries and employing over 50000 people in more than 1000 offices. In the United Kingdom, it has been established for over eighty years and has six manufacturing centres and fifty offices with 6000 staff.

One of the primary reasons for choosing this company was that its main business is the recording and processing of data. Therefore, it might be expected that:

1. The organisation, because of the nature of its business, would be aware of the privacy issues related to employment.
2. For reasons of self-interest and the promotion of its product, the corporation might have devised certain safeguards for the privacy of personal data in a similar fashion to the steps taken by IBM. These have been well publicised through journal articles such as Cary (1976) which drew attention to IBM's own personnel system and the way in which personal information was treated. Defining a formal policy of this kind satisfied both the employee and pressure groups, but more especially, provided beneficial publicity for the company's business and social relationship.
3. Because a large part of the operations of the selected firm deals directly with computers, the organisation might have automated its personal records.

The results of this study highlight, firstly, what privacy issues were involved at various points in the employment data lifecycle and then, what factors have influenced this company's privacy and data protection practices.

One of the main functions of this study was to follow through the capture, maintenance and disposal stages within the data lifecycle and to discover the potential threat these may pose for privacy. The company had recently changed the format of the application it used, a move which generally received an unfavourable reception. Whereas the previous form had been suited more specifically to the U.K. labour market and management or graduate entry, the newer form was more general and had been imposed upon the company by the American parent in order to provide uniformity at the application level.

In addition to asking the more usual questions, a considerable amount of detail on, as earlier defined, 'sensitive data' was requested upon this new form. The first two sections asked for general and personal information, including: "height and weight"; "do you own your own home?"; "do you own your own automobile? If so, specify make and year". The rationale, for example, for asking the last question was that if a candidate were applying for the position of a sales representative in the U.S.A., he would not be supplied with a company car, whereas in the U.K. he would. Therefore, the company might want some indication of the individual's mobility before hiring him, although in this instance, it might be more applicable to enquire whether the candidate held a driving licence. There may be other similar reasons why such data is required prior to an individual commencing employment with the organisation. However, irrespective of whether such details are used in employment decisions, their availability at

this initial stage could be perceived as a way of discriminating against certain individuals.

Other enquiries made upon the application form reflect the competitive nature of the industry or the high security of its operations:

"Have you applied to (company's name) before?"

"Are you a former (company's name) employee?"

"Have you ever been convicted of a felony?"

"Do you have any relatives in the business machines industry?"

When questioned about the uses of such information, a representative from the personnel department described how the company previously had formally discouraged the employment of an individual whose spouse worked for a competitor or within an allied sector of the industry. This policy has since been relaxed and although the form has not been modified, little emphasis is placed upon the response to these questions.

Some of the questions asked did not appear to have much connection to the employment decision but the mere practice of asking such questions could infringe upon an employee's privacy:

"Do any members of your immediate family own their own business?"

"Have you any outside business interests?"

"Have you ever been in, or petitioned for, bankruptcy?"

"Are you entirely dependent on your salary? Specify other income."

"Specify total monthly expenses and salary required."

Other sections of this new form did not fulfill the information needs of the U.K. personnel departments as, for example, little space was given for the candidate to supply details of his educational background compared to the previous format. Although equal space was allotted to "language skills" and "geographic area knowledge and travel", little attention was paid to either category in the selection procedures and the latter was described as "irrelevant" and "an embarrassment even to ask". However, in South American countries, fluency in a variety of languages could be a very important aspect of the employment decision and this new application form sought to achieve a compromise between the requirements of a number of countries.

In the section concerning previous employment, a candidate was asked to indicate his earnings and other forms of compensation and to "give specific reasons for leaving or wishing to leave. Do not merely say 'resigned', 'better position', 'disagreement', 'still employed', etc". While requesting this additional information could eliminate a degree of misinterpretation many of the reasons for terminating employment are highly personal.

The information disclosed on the application about the company was quite limited. At no point in the form did it state that its contents were private and confidential or how the individual's details would be used, issues that have been discussed in the literature. A member of personnel said that, within the U.K. this department had devoted its energies rather to changing the application form to rid it of irrelevant details, than to providing the applicant with data of how the form was to be used. An applicant's attention would automatically be directed, by the use of bold type, to ensuring that every question had been answered and to appreciating that a misrepresentation of facts would be sufficient cause for dismissal. This disincentive was a means of ensuring the accuracy of data. If the applicant is successful, his application form becomes the basis of a manual personnel file maintained about him. If he is not, it would immediately be disposed of, or held for a further six months if another suitable vacancy was thought to be likely to arise shortly.

References are asked from the employee when he is called for an interview. It was estimated that seventy-five per cent of the total personal information the company holds in an employee's record comes from the applicant directly. Other inputs into the file during the course of one's employment would be, for example, training reports, performance appraisals, salary changes and security checks. The company stressed that they do not use investigative or credit agencies or make use of such information sources as the Economic League. Education and employment details were checked for accuracy and any discrepancies, but no independent verification was made of offences.

Performance appraisals are another way in which the company collects information about its employees. These are conducted on staff members at yearly intervals and most of the performance sheet is completed as a running account during the appraisal session between an employee and his supervisor. The

top of the form reproduces a number of the individual's personal details (marital status, children's ages, etc.) and asks for other data including most recent job, date employed, and current position and location. The appraisal period, therefore, provides a formal mechanism for verifying the accuracy of some parts of the personnel record. There is, however, no established policy to ensure the accuracy of other data not listed on the form and the burden is upon the employee to notify personnel of a change of circumstance, for example, a change of address or a new skill acquisition. The appraisal discusses the individual's projects and achievements, formal training received and performance in these courses. The manager and employee will also have to assess a comprehensive range of management traits or attributes in the light of the employee's effectiveness and skill. These characteristics cover such aspects as knowledge of assignment and operations, ability to complete assignments, determination and establishment of realistic forecasts, effectiveness of communication, abilities in training and developing personnel, and willingness to accept responsibility. The reporting is completely open and its results are signed by the individual and his manager.

However, the final quarter of the form is completed without the individual because the nature of these details could easily be misunderstood by the employee. The layout of the form means the employee, nevertheless, will be aware of the type of questions his supervisor is required to answer, namely, planned assignments for the individual for the next six/twelve months, recommendations about his future development and promotion, relocation factors and comments subsequent to the post-rating conference. It is quite possible that without a rigorously specified structure to the questions asked, a considerable element of subjectivity could enter into an individual's appraisal without his knowing it or being able to lodge a protest against it. However, the alternative, which would be to eliminate the subjectivity which accompanies open-ended questions, would remove a valuable management planning tool. The organisation does not publicise the extent of information it collects and uses but the personnel department believes employees are aware of the information being held about them.

Information about the employee is collected throughout his career with the organisation and even just prior to terminating his employment, an exit interview is conducted. Through this medium, the employee's opinion of the organisation as an employer is questioned and this information is used by the personnel department to recognise trends and whether the company need alter its policies, if, for example, staff are leaving for reasons of salary or conditions. At this final interview the employer records where the employee is going and conducts a final appraisal of his ability. Together with a few personal details, these are maintained separately on a manual record in the personnel department and can be used to trace all employees' details up to twenty years ago. The individual's records are held in the head office for ten years in their entirety before being taken to a warehouse, where they may be stored indefinitely. Although this means personnel are able to verify data about previous employees and answer any enquiries, it also means the organisation may be storing some potentially highly sensitive information, the demand for which is minimal.

One method of ensuring the accuracy of personal information would be to allow the employee access to his own record, a method employed by the 1984 Data Protection Act for computer files. This serves a two-fold purpose in that it not only relieves employees' fears about what type of data is being recorded on them, but also improves the quality of decisions made, by providing those responsible for such decisions with accurate and complete data. This organisation did not encourage the employee to make requests to see his file and within the past four years, no individuals had requested to see his own personnel record. The reason direct access had not been encouraged was that these records contained a certain amount of information divulged in confidence, for example, references, and it would be a breach of this relationship if the individual was permitted to see such data. This is not an uncommon practice in companies and even in the 'model' policies adopted by IBM to protect data and employee privacy, certain information (e.g. planning forecasts) has highly restricted access (Cary, 1976). Information recorded manually is not covered by the 1984 Data Protection Act.

The confidentiality with which personal details are kept may depend upon which parties the organisation allows to see an employee's record. An employee's file is held by his manager in the local

branch and a copy of its written contents, such as test and training results, duplicated by the company's personnel department. There is nevertheless, no mechanism for preventing the branch manager from keeping personal notes or recording verbal entries into the individual's file, without the knowledge of the main office. Although not quantified, the impression given by a member of personnel was that such instances were not entirely rare (see also Newman, 1985). A second manager would not be permitted to access the contents of an employee's file solely on the grounds of the rank he holds within the organisation. After all, the personnel department stressed it was not a "lending library" and would therefore question the manager's motive and not permit full access.

A company's policy on disclosure to third parties can infringe on employees' privacy. In this case, no details about an employee would be given over the telephone except to the police if their investigations had a direct bearing upon the employee/employer relationship as in the case of internal theft. Most inquiries would be answered in writing where there had been a written request by the employee to furnish these details. The exceptions are building societies whose call would be returned after the identity of the inquirer had been verified. Even in this case, the company would not disclose any new information but only confirm the details that were already possessed (e.g. when the employee had been employed, in what position, when he left his employment etc.). Requests for information from other employers about previous or departing employees were usually made in the form of a questionnaire rather than a general, and highly subjective, open-ended inquiry.

The U.S. parent company appeared to play a dominant role in determining the U.K. subsidiary's policies on privacy and data protection. The parent determines to a large extent what information is collected about the individual as both the application forms and the assessment forms were American. Although currently using a manual personnel system, the company plans to automate it by the next year. However, before this is done, the computerised personnel system is to be introduced in the Japanese and French subsidiaries of the organisation. It would be expected that there are significant differences between countries which require the collection and use of different information about employees by national personnel departments. For example, the stereotyped image of a Japanese company is that it is much more paternalistic than an American company. That other differences exist between British and American companies is shown by the unusual U.S. application form. In the U.K., the selling side of this organisation was not unionised and hence policies on privacy would not be influenced by trade union negotiations. Unions might have a more significant part in bargaining for their members on privacy issues in the manufacturing side of the company. Once a year, the eight largest manufacturers within this industry meet and exchange information on salaries and benefit levels. Employee privacy and data protection does not, however, appear to have been discussed and even though the personnel department maintained informal contacts with other organisations, the company was not specifically aware of practices within the industry for protecting personal data.

More significant, however, may be the impact which professional standards, established for example by the Institute of Personnel Management, have upon its members and, in turn, upon the confidentiality with which data about an employee is handled. One task of the personnel department within this company was to keep the subsidiary abreast of recent legislation, government reports and White Papers. Because of the nature of its business, the company would have been especially aware and interested in the outcome of the Government Paper 'Computers and Privacy' and the impact which such reports on data protection could have upon its industry. It is questionable whether any of these have had much influence upon the policies the company adopts on data protection, especially given that one member of Personnel did not know whether such reports were kept up-to-date.

Surprisingly, although the entity operates in the computer industry, computer technology has, as yet, only had a minimal effect upon personal data and personnel practices. Presently, the only section of the personnel function which is automated is payroll although, as previously stated, personnel records will be automated using a system developed at the international group level. Only objective facts, such as training, nationality and education, will be held in computerised form. Sensitive information by and

large, will still be in a manual format. The main impact foreseen of such technology in personnel, is that the computer will speed up and increase the ability of the department to cope with informational requests made by management. Some of these demands include:

(1) An inquiry about a job position.
A certain department may have a vacancy for an employee with a certain specified level of training. The personnel department can, with a computer, use such information to help fill this assignment. In a similar way, the same procedure can be used to establish a basis for and hasten the process of selecting a job candidate. As a result, this increases the need for the company to have accurate, complete and verifiable information about applicants and present employees.

(2) Turnover analysis, manpower reports by location and category, quarterly studies of the calibre of labour, source and qualifications of new recruits.
These are examples of some of the corporate requirements for data at both the national and international level. Computerising these records could improve the department's ability to supply aggregate statistics for the organisation and for use in planning.

(3) Plans concerning the career paths of certain individuals, progression analysis.
The personnel department will be able to record and follow the progress of these individuals in greater detail. The personnel department will also find the computer a great advantage in the compilation of statistics required by the Government helping to complete, for example, the Industry Training Board Returns.

The company recognised that additional security measures will be necessary to protect personal information from unauthorised access. It is the feeling of the department that following a change in the actual design of the office occupied by personnel to a more open-plan layout, the facilities for storing records were no longer as secure as they had been. Nevertheless, this by no means implies that such records were insecurely kept, for there is a complex system of physical security surrounding the department. By introducing a computer, the company will be able to incorporate a number of software deterrents into their security system in, for example, the use of passwords, encryption, differential access, audit logs, etc.

The computerised personnel system the organisation will introduce is highly generalised in order to meet a number of legal requirements in different countries, as, in some subsidiaries, salary is the most highly controversial piece of data. At the same time, it will be important to adopt and modify this all-embracing information system to suit particular information needs within countries. Moreover, because of the expense involved in doing this, the company is introducing the system firstly into minor subsidiaries so that any mistakes are made on a smaller scale.

Employment and privacy: a problem for today

Data capture

The case study showed that more information was collected than necessary for the employment decision. Once collected this information was often included as part of the employee's personnel record even though its relevance was doubtful. It is considered that other data necessary prior to engaging an employee, was asked prematurely upon the initial application form. Besides slowing the selection procedure, this may be an unwarranted procedure at this stage or an indication of a discriminatory policy used by the organisation.

Employers do not appear to be asking for much information about the applicant's family. Any such cases were in order to meet specifications required by government contracts and to satisfy other governmental needs. Details about the applicant's spouse and children are still regularly requested.

The government is a major factor in determining what other data are collected by an employer. Details of disability number, National Insurance number, marital status, etc. are required to assist the government in administering both systems of social security and of taxation. However, the time at which such data is acquired will be largely determined by the particular organisation and its recruitment policies. Some information, for example, as to whether the applicant is a houseowner, was found to

be stored by the organisation even after it had become redundant.

The application form did not specify that the information furnished would be treated as private and confidential. Neither did it say how the forms were to be used or what would happen to the details of the unsuccessful candidate. Where adequate data protection procedures exist, stating these policies explicitly would emphasise the confidentiality with which personal information is treated within the employee-organisation relationship. In turn, the individual is more likely to supply more complete and accurate information, thus improving the quality of the inputs into later decision-making.

The results from the case study do not support the idea that blacklists, intelligence tests, hearsay or other subjective sources of data (e.g. the Economic League) are widely used in employment decisions. Nevertheless, this should be considered in the light of:

1. Submissions to the Lindop Committee by the London Personal Finance Associations, a trade association representing consumer credit organisations, which revealed that employers sometimes disclosed information from personnel records related to the credit-worthiness, salary, benefits, etc. of their employees.
2. The Economic League, financed by the subscriptions of nearly five thousand member organisations, provides information on alleged subversions from its control register of political and trade union activists (Hewitt, 1979).
3. Employers might not readily admit to the use of such subjective information sources or be aware when such sources are used by any of its staff. Management studies of informal sources of information have shown that they are widely used (Newman, 1985).

Data maintenance and use

The uses and requirements for information should determine what personal details the organisation collects about the individual and what is contained as part of his personal record. Some information may be factual while other information may be subjective. A first step towards data privacy and formulating a policy on access, would be to make the distinction between data which are factual, and data which are subjective, unverified assertions. Further interviews with a number of firms admitting graduates found that management files were being kept independently and separately from personnel records and seemingly without much concern from the personnel department who felt unable to check this practice, irrespective of its threat to employees. If employees do not even know of the existence of these essentially "secret files", let alone their contents, there will be no method to ensure accuracy or take steps for redress of grievance if such notes are found to contain defamatory material.

In addition, the confidentiality of personal data is directly affected by which parties within the organisation are allowed access to an employee's file. Rank and seniority should not and do not automatically form the basis for "carte blanche" access to personal records. To ensure internal policies are adhered to, codes of practice mirroring the recommendations of bodies such as the Institute of Personnel Management, should be established where not already present. Further, evidence from this research and previous findings reinforced the belief that unauthorised access to data by third party outsiders can be obtained.

Data disposal

Employee data is also threatened, it was found, by the measures used by an organisation to remove personal information no longer necessary or relevant. The burden for adequate disposal should be upon the collectors and users of the data (employer) to avert incidents such as the example where highly confidential medical files were found on a tip (Guardian, 2 September 1981).

When data is stored in a computer data-bank, its disposal is complete erasure. The computer also avoids the problem of having to use a separate mechanism (incinerator, shredder) to dispose of personal data. In line with the results of the Canadian Task Force (1972) and Westin and Baker (1972) the results in the case study showed that when personnel files had been computerised, the most highly

sensitive details were still held in the company's manual files.

Trade unions

Unions have not brought great pressure upon employers on behalf of their members. However, from the TUC submissions to the Lindop Committee and the guidelines established by APEX, we are of the opinion that data protection will become a topic of increasing importance in collective bargaining and union negotiations and that the 'spill-over' effect would impact upon non-unionised industries.

Industry norms

Surprisingly, this variable did not significantly influence the privacy policies among competing organisations. Moreover, because such competitive pressures are intangible, analyses of these and extrapolation of any results beyond the limitations of a single organisation and a division within it, may not be feasible.

International pressures

It was interesting and almost unexpected the extent to which policies established overseas by a parent corporation were reflected in the practices of a subsidiary. Two conclusions are drawn from this:

1. To effectively regulate multinational corporations for data protection requires a mutually agreed international position being defined on the problems of privacy by such bodies as the OECD.
2. To avoid the dangers of "data havens" the country of origin may need to take into consideration that operations of some corporations span many countries not all of which have similar levels of data protection. Further legislation might be extended to cover both the manual as well as computerised record-keeping practices of organisations. The current Data Protection Act (1984) makes just this distinction.

Technology

The case study and further interviews found the incidence of computerised personnel systems is far smaller in the U.K. than in the U.S.A. from where the majority of the literature is derived. This result is reiterated by the listings of forms of computer systems in operation, in recent editions of "computer survey". Although conclusions as to the impact of technology upon privacy policies are still somewhat limited, the following results are drawn from this paper:

1. Introducing a computer system requires increased and different types of security measures which can secure the system more than was possible with a manual system but centralises the information into a store or 'target'.
2. Sensitive details about an individual are most likely to be held in manual files.
3. The change from a manual to automated record-keeping information system is often a time for reviewing and formalising corporate policies of access and privacy.

Government

The study did not attempt to quantify the impact the government has had to date upon data collection and privacy policies. Nevertheless, we believe the impact of governmental bodies must be discussed as privacy legislation is a highly political subject with information a type of power (Forrester, 1967). The National Computer Centre in a recent survey, found organisations using computers for data storage were overwhelmingly in favour of legislation. Without legislation, British companies may be at a disadvantage compared to their Western counterparts as the U.K. stands virtually alone in Europe without laws or regulations to determine whether a certain employment practice is an acceptable use of personal information stored in a manual or automated record system. It is not clear that the 1984 Act will impress our continental neighbours in this respect. Government intervention could redefine the individual's legal position for data protection and ensure the costs of such protection are fairly distributed. Recent guidelines issued by the OECD on data privacy

recommended that computerised personal information should only flow freely between countries if both countries have some form of data privacy legislation. This has resulted in Sweden's refusal to allow certain types of data to be sent to the U.K. because of the weak rules here.

Professional agencies, whose members are in contact with highly sensitive data, are providing further pressure upon the government. The British Medical Association has requested legislation to control private information held in computerised record systems since 1980. Whatever stance the government adopts on this matter will directly influence a company's policies on privacy and data protection. The government already determines a considerable amount of the information an employer collects from employees and some of the uses (e.g. taxation, government statistics). Therefore, although the conclusions were not drawn from the research, the impact of this variable has been considered in depth.

Bibliography

APEX: 1981, *Guidelines for Members.*

Canadian Task Force: 1972, *Privacy and Computers: A Report by the Department of Communication and Department of Justice*, Goverment of Canada.

Cary, F. T.: 1976, 'IBM's Guidelines to Employee Privacy', *Harvard Business Review*, Sept-Oct 1976.

Forrester, J. W.: 1965, 'A New Corporate Design', *Industrial Management Review* **7** (1), pp. 5—17, Fall 1965.

Hewitt, P: 1979, *Computers, Records and the Right to Privacy*, National Council for Civil Liberties.

Hoffman, L. J. (ed.): 1973, *Security and Privacy in Computer Systems*, Los Angeles: Melville Publishing Co.

Kovach, K. A.: 1976, 'A Retrospective Look at the Privacy and Freedom of Information Acts', *Labour Law Journal*, September, pp. 548—564.

Klopfer, P. H. and Rubenstein, D. I.: 1977, 'The Concept of Privacy and Its Biological Basis', *Journal of Social Issues* **33** (3), pp. 52—65.

Margulis, S. T.: 1977, 'Conceptions of Privacy: Current Status and Next Steps', *Journal of Social Issues* **33** (3), pp. 5—21.

Miller, D. B.: 1976, 'Privacy: A Key Issue between Employees and Managers', *University of Michigan Business Review*, January, pp. 7—12.

Newman, M: 1985, 'Access to Information: Strategies for Prevention and Promotion', *Journal of Management Studies* **22** (2), pp. 193—212.

Niblett, G. B. F.: 1971, 'Digital Information and the Privacy Problem', *OECD Informatics Studies*, No. 2.

OECD: 1976, 'Policy Issues in Data Protection and Privacy', *Informatics Studies*, OECD.

Rothman, S. and Mosmann, C.: 1976, *Computers and Society*, Chicago: Science Research Associates.

Schein, V. E.: 1976, 'Privacy and Personnel: A Time for Action', *Personnel Journal*, December, pp. 604—615.

Sieghart, P.: 1976, *Privacy and Computers*, London: Latimer.

Westin, A. F.: 1976, 'The Problem of Employee Privacy Still Troubles Management', *Fortune*, June 4.

Westin, A. F. and Baker, H. B.: 1972, *Databanks in a Free Society: Computers, Record-keeping and Privacy*, New York: Quadrangle Books.

Wolfe, M. and Laufer, R. S.: 1974, 'The Concept of Privacy in Childhood and Adolescence', in D. H. Carson (ed.), *Man-Environment Interactions: Evaluations and Application*, Washington D.C.: Environmental Design Research Association.

Department of Accounting and Finance,
University of Manchester,
Manchester M13 9PL,
U.K.