The U.K. privacy white paper 1975

by A. S. DOUGLAS
The London School of Economics and Political Science
London, England

ABSTRACT

It is now some years since the formation of the Younger Committee, set up to study the question of Privacy and its protection as it related to the private sector. The Committee published its report in 1972. Shortly after the Younger Committee was set up, an interdepartmental working party was set up within central Government to study the problem as it related to the public sector. This working party's report has now been issued along with a Government White Paper, which makes specific proposals for action in the computer field. In the meantime other countries, including the U.S., have taken significant steps in the direction of defining Privacy and introducing data protection procedures.

INTRODUCTION

The White Paper has been promised for some eighteen months, but there have been successive delays and it has long been an open secret that disagreements over its content have existed in official circles. The final version issued owes a great deal to Alex Lyon, the Minister of State at the Home Office, who sat on the Younger Committee and whose minority report is incorporated in the report of that Committee's findings. The White Paper was drafted by a lawyer, Mr. Paul Sieghart, who spent considerable time in wide-ranging consultation beforehand under the aegis of the Home Office and no little time in subsequent amendment to take account of comments and objections!

In discussing the various reports and the White Paper it is essential to distinguish clearly between Privacy, Confidentiality and Security. These three concepts are often confused. However, there are important differences involved, not only in the topics covered, but also in the attitudes to which they can and should be adopted by the professional community, and in the acceptability of those attitudes to the general public. For a brief but clear statement of what is involved see "The Application of Computer Technology for Development." The question is discussed at more length in the Younger Report and elsewhere.

WHAT IS MEANT BY 'PRIVACY'

It is sufficient here to point out that Privacy concerns the rights of an individual, personal or corporate, to enjoy protection from unwarranted and unauthorised intrusion into his affairs. It is not related in any specific way to computers.

It is a social phenomenon and depends critically on public opinion. In a democracy it is clearly a political matter, to be dealt with by our elected representatives —under the (hopefully!) watchful eye of the electorate. It defines what is to be protected, not how this is to be done.

Every professional is a citizen also. In that capacity he has a right to speak on privacy, but only on the same basis as every other citizen—his professional status confers no special virtue on any pronouncements he may make. However, in regard to the legal definition of what is to be protected, or to the methods of protection of data regarded as private, professionals in whose area the matter lies may speak as experts and carry an appropriate degree of authority. This authority carries with it a responsibility to explain the nature of any problems involved—in language laymen can understand—and to warn of the probable results of abuse, misuse or omission of safeguards. It is in this spirit, I shall approach the rest of this paper.

CONFIDENTIALITY

Confidential material is data entrusted to an individual, corporation or agency, whether local, national or international, the possession of which imposes a duty on that agency to protect it from disclosure except as authorised by the protocols under which it may be collected. It may include, but is not limited to data about individuals. The protocols creating confidential status for data may be statutes, contracts or customs recognized by the Courts or by common consent. The protocols sometimes conflict with other protocols, when the individuals involved may well be placed in an invidious position. A journalist asked to reveal his sources when these are connected with criminals, for example, may feel that he must preserve the anonymity
of the sources partly to preserve them from retribution and partly to ensure that he is able to use similar sources at a later date—yet his action could be deemed to conflict with the criminal law and place him in jeopardy as an accessory to a crime. In some cases the conflicts have been resolved by the Courts in favour of preserving confidentiality except in specified circumstances—e.g., the doctor-patient and solicitor-client relationships, where the preservation of confidentiality is generally acknowledged to be in the public interest unless criminal proceedings are involved.

The protection of confidential material is, of course, closely related to the preservation of privacy in respect of data about an individual. The security considerations are similar. But in the case of privacy the rules under which disclosure may be made are not necessarily well defined, if they are defined at all. Since there is no right to privacy defined in English law, rules of disclosure must currently rest solely on any protocols which may exist or be created by, e.g., contract. It is interesting to note that this is not so under the Code Napoléon, on which French law is based, in which the point is covered to some extent by the ‘droit de la personnalité’. (For a comparative study of the position under different laws, see Reference 6.) A political move is now afoot in the U.K. to cover this ‘open’ position by Statute. It will be interesting to study the White Paper which will in due course, no doubt, emerge.

It is fair to say that the White Paper on Privacy discussed here does not directly define Privacy or Confidentiality but primarily addresses itself to the question of Security. However, there is one important point on which it is clear. This relates to the question of disclosure of the existence of data banks containing records concerning individuals. The White Paper proposes that disclosures should here be the rule (para 34 & 35) and that exemptions on grounds of national security would need a certificate from the Home Secretary (para 39).

SECURITY—SOME GENERAL REMARKS

There are two points to bear clearly in mind when examining any security system. The first is that there is no such thing as a perfectly secure system. In general, one gets the degree of protection one is prepared to pay for—and perfect protection has infinite cost. It is generally cheaper to design features into the system from the start than to add them later. The aim must be to ensure that penetration of the system costs at least as much as the possession of the data is worth to a penetrator, and to design the system so that penetration, if it occurs, is detected.

The second point is that the weakest link in any security system is the people involved in it. Almost all breaches of security involve the co-operation of someone inside the system. Thus the selection and control of personnel is a key issue in providing protection of data. Moreover, only those ‘inside’ a system are normally in a position to detect certain types of abuse, before these effect the public. Thus their cooperation is essential.

These points are implicitly recognised in the White Paper, and specific mention is made of the role that the British Computer Society could play in relation to any legislation which may follow from its provisions (para 43). But the mechanism involved has been left open for the present. We shall discuss this further below.

The essential elements of a security system must involve legislation, detection of breaches, and enforcement. The White Paper, whilst proposing legislation, is not definitive on the method to be used to detect breaches or by whom the law is to be enforced. However, one important aspect on which it is clear is that the mechanism of enforcement should apply equally to the public and private sector. The delay in prohibiting the Report of the Interdepartmental Working Party which completed its work in 1972, indicates that this view may not have been wholly shared by the official side. To understand this, it is perhaps necessary to review existing practices.

THE OFFICIAL SECRETS ACT, 1911

In the public sector, protection of data has been practised for many years, of course. Indeed, specific duties of protection are laid down in various statutes to preserve the interests of the individual. Cross-correlation of data relating to an individual has been controlled by a set of internal rules drawn up within the Civil Service. It is a fairly sophisticated code and takes account of the need to obtain valid statistics, whilst at the same time preserving the anonymity of the individuals whose records are used in those statistics. It is recognised that any such procedure can lead to a risk of disclosures about individuals, but there is insistence on this risk being minimised by the techniques employed. It is fair to say that a specific case of unauthorised disclosure has yet to be proved, although it is not difficult to 'manufacture' situations in which it could take place. To this extent existing protection is to be commended as being effective and sensible.

Enforcement of the rules is by administrative fiat. The unauthorised disclosure of data by an individual Civil Servant not covered by any other protocol is covered by the Official Secrets Act, under which every Government Servant who handles any confidential or private data operates. Signature of a declaration under the Act is not essential to its effect being binding on

* For some valuable comments on this aspect of matters see 'Report of a Working Party on Survey Research and Privacy' 1973, issued by Social & Community Planning Research, 16 Duncan Terrace, London N1 8BZ.
persons involved in handling such data, but helps to draw attention to its provisions. The Act is comprehensive and was drawn up with matters of national security in mind. There are thus “catch-all” clauses which can be extended to cover matters which might be considered to be secret only in a national emergency—and then only by the stretch of a very fertile imagination. It is, for example, possible to bring under the Act the important topic of whether and how often the grass is cut at a designated Government installation. Whilst one can undoubtedly construct an ingenious scenario in which such a matter is of crucial national importance, one can reasonably feel that, in normal circumstances, it is unlikely that this is of great concern to anyone—friend or foe—except perhaps an aspiring gardening contractor!

Use of the Act to support a case against reporters and others concerned with the Nigerian civil war led to some public concern a few years ago. There have been rumbles about its effect ever since, and a Departmental Committee set up in 1972 under the Chairmanship of Lord Franks recommended the repeal of Section 2 and its replacement by an Official Information Act. But any alteration is naturally met by an equal concern about the effects which could flow from its repeal and a general uncertainty as to what amendments are really needed.

There are, no doubt, those who deem the Act necessary in some form, as I do myself. Many of them, like me, feel that it is a somewhat blunt instrument as it now stands. It is administratively convenient, because it confers wide powers to impede the flow of information both inside and outside Government on senior civil servants when they deem it necessary. Whilst I have no reason to doubt the sincerity of their intentions in the public weal, nor can I point to specific instances of abuse related to computer matters, the system could all too readily be abused, and there is at least circumstantial evidence that it is, from time to time, used more to cover up incompetence than to protect what must be protected for the good of all. To this extent the present system could usefully be amended.

The White Paper, if implemented, must necessarily impinge on the working of the Act in so far as it relates to computer-supported data bases concerning records of individuals. Since non-disclosure on grounds of national security of the existence and nature of such a data base would require the certificate of the Home Secretary, if the provisions of the White Paper become law the provisions of the Act could then only be used if that exemption were to be granted. This implies a review procedure which is not necessary at the moment. Furthermore, the mechanisms for enforcement considered by the White Paper both imply that, if complaints are made concerning the effects of the existence or use of such a data base to the enforcing authority, that authority will need to know of the existence of such an exemption order, and could ask for it to be reviewed by the Home Secretary if it felt that exemption was being abused.

While there are those who would welcome the abolition of the Official Secrets Act or, at least, its substantial modification, it is incumbent upon them, in my view, to state how those of its provisions deemed essential to national security are then to be dealt with. For the most part, this has not been satisfactorily tackled by would-be amenders. Total abolitionists would not, I think, obtain a Parliamentary majority, and would undoubtedly be opposed by a majority of officials.

A partial answer might well evolve from the legislation proposed by the White Paper. Clearly the review mechanism introduced as described above would tend to reduce the unselective use of blanket security provisions, and a sensitive use of his powers by the Home Secretary could lead to greater openness overall, by insisting on a careful definition of what features of a system actually attract exemption, initially in relation to computer-based systems, but, in due course, by extensions to manual systems. It is to be hoped that this evolution will indeed take place.

ENFORCEMENT—THE PROPOSED DATA PROTECTION AUTHORITY

The White Paper describes two possible forms of enforcement agency, which it tends to contrast. The one with a tighter form of control would involve a process of licensing. The White Paper does not set out to determine whether this relates solely to the licensing of the organisation holding the data, the collection agency, the people involved, or all three. Nor is any specific mechanism proposed for ensuring the existence of a ‘responsible person’ in relation to the data, although this point is discussed at some length in the Younger Report. Any or all of these forms of control are possible under the suggested provisions, however.

The “alternative” seen by the White Paper envisages an agency which only reacts in response to a complaint of an abuse of the citizen’s rights by virtue of the existence or operation of a data base. The proposed Data Protection Authority in this case would act only to investigate such complaints and take action to remedy them where they proved to be justified.

An interim Data Protection Committee is being set up to make recommendations on the form the Data Protection Authority should eventually take. The terms of reference of this Committee are not spelled out in the White Paper directly, but, by implication, include advice on the legislation to be enacted. They will almost certainly be required to define, at least provisionally, some of the individual’s rights to privacy as well as spelling out the powers and duties of the Data Protection Authority. It is, perhaps, significant that Sir Kenneth Younger has been appointed the Chairman of this Committee. In the light of the work done by his
earlier Committee, we may expect that the definition of privacy will follow the lines of its Report, modified by any impact made by inclusion of public sector considerations.

COMMENTS ON ENFORCEMENT

The problem of enforcement is perhaps best seen in relation to a real-life situation, albeit a hypothetical one. U.K. firms are currently subject to a Pay Code, forbidding the paying of increases in wages in excess of a fixed figure each twelve months. It is true that this does not exactly have the full force of criminal law, but a breach is certainly punishable, if detected. In all firms which use their computer for payroll one or more programmers are authorised to see the figures paid out, although these are regarded as confidential. The programmers concerned are usually asked to sign papers drawing their attention to the confidential nature of their work and under law can be dismissed by their employer for a breach of such confidentiality.

Let us suppose that one such programmer notices a breach of the Pay Code in the course of his duties, what should he do? He can, of course, report it to his superior. However, more likely than not he will be told to forget it and reminded of his obligations relating to confidentiality. He can resign, but with present employment prospects, he might find that, at the least, inconvenient. A threat to resign in order to reinforce his report to his senior, is clearly a dangerous course, bordering on blackmail at worst, and almost certain to rebound on him in course. He can consult his professional Society—assuming he belongs to one. The Society can operate at a higher level than he is able to do, and stands some chance of getting the situation put right, but there is no way to avoid the finger pointing at a small number of people as containing the one responsible for the 'leak'. Naturally straight dismissal would be out of the question as the adverse publicity the Society would ensure would not be welcome. But it is difficult to see how some retribution could be avoided if the management were so minded. The least that would be likely would be a transfer to other work.

Clearly the dice are loaded against disclosure of the breach coming from anyone, however professional and public spirited, inside the system, unless they are on the point of resigning anyway. Moreover any tangible proof of their contention which could be produced by them would constitute theft of company property—all the more culpable if they took it with them on leaving.

The only possible counter to this seems to be to strengthen the 'outside' pressure on the individual professional to act according to a code of ethics and good practice and to protect him, if he does so, from reprimals by his employer. An enforcement authority would need to be equipped with wide licensing powers to do this, applicable equally to the conduct of operations and the personnel involved. It is also clearly practically desirable to have a named person to accept responsibility if things go wrong, who is empowered under the licensing procedure to enforce proper control even though this may not be in the direct interests of his employer. The parallel drawn in the Younger Report is to a mine safety officer, who is employed by the mine but has statutory powers and duties in respect of safety. The parallel is not exact, but illuminating.

It is, I think, clear that a 'complaints board', however strongly armed with investigative powers and sanctions on future action, would be unlikely to achieve a significant change in employee attitudes. But this is not to say that some complaints procedure is not desirable for a licensing authority. I do not myself see the White Paper proposals as strictly alternative. To an extent they are complementary. It is arguable, obviously, that it is possible to have a complaints handling procedure without licensing. However I do not think that, in practice, a licensing procedure will work smoothly without a complaints mechanism.

The British Computer Society, in addressing the Home Secretary on the subject, has come out firmly in support of a licensing authority (see Appendix). One form of such a system is already in operation in Sweden, under their Data Act.

COSTS

The White Paper refers specifically to costs, and it is clear that the Data Protection Committee, in making its recommendations, will need to justify them on a cost/benefit basis. The Swedish licensing system does not involve a large central staff—25 at present, I believe, and direct costs are covered by charging a licensing fee. Some of the factors involved in implementing recent legislation in the U.S. are set out in a recent Rand Corporation report. A similar study will be needed to assess the costs, both direct and indirect, incurred in implementing the alternatives proposed in the White Paper. Whilst, as in the Swedish system, central costs can be kept down and funded from license income, if this route is chosen, there are bound to be additional costs at each installation. This raises, in particular, the question of consultation of records by those about whom they are kept. Although the right to inspection is advocated in principle in the White Paper it is clear that the cost of this will need to be reviewed carefully and some arrangements set up that will enable the individual to be assured of the correctness of data held about him without either he himself, the data bank operator or the public purse being put to unreasonable expense. It is here that proper advance planning of the data base system for filing and retrieval in the light of security and accuracy requirements will have its most important role to play. A well planned system which satisfies a reasonable licensing requirement may well be little more expensive to construct and operate than one which does not.
Clearly, temporary measures may be necessary to deal with this problem. More study is certainly needed before costs can be determined.

So far as the licensing of personnel operating data banks is concerned, I have explained above why I believe it is important to 'control' the people involved as well as the organisation keeping the data bank. Here "control" can be assisted by the existence of a national professional body or bodies whose standards include a code of ethics and a code of good practice attuned to the needs of the situation. Whether or not the societies concerned maintain rigid restrictions on entry to qualified persons is perhaps less important than their members should accept the need for a degree of responsible discipline in their work. The Swedish Computer Society for example whilst subscribing to the latter concept has yet to embrace the former and may well never do so. But I have no doubt that its existence is of value in operating their Data Act.

The B.C.S. would not, I believe, wish to seek a monopoly under any licensing system, but would certainly seek to ensure that its membership at an appropriate level would carry with it automatically a license to practice at a licensed installation, and this would undoubtedly simplify and strengthen the implementation of a licensing scheme.

CONCLUSIONS

The White Paper has gone a considerable way in the direction pointed by the Younger Report, and, in particular, to satisfying the various concerns expressed by the British Computer Society in its submission to the Younger Committee, as developed subsequently by the Privacy and Public Welfare Committee of the Technical Board. As I have indicated, there are a number of matters still to be defined and worked on before an Act is finally introduced—indeed, more than I have had time to develop here. The various Committees of the B.C.S. within the Technical Board are already at work on these with a view to making a submission to the Data Protection Committee, with whose work they hope to be even more closely associated than they were with that of the Younger Committee. I am proud to be associated with this effort, which, I feel is helping to maintain in the U.K. the high standards of liberty and open Government for which we are renowned. I am also very grateful to the organisers of this Conference for giving me the opportunity to present this report to those who share our concern that computer systems should be used to the advantage and not to the detriment of individual liberty.

REFERENCES

4. The Application of Computer Technology for Development,
Second report of the Secretary-General, 1973 U.N. Sales No. E.73 II.A.12 para. 50, p. 73. See also First report of the Secretary-General 1971 U.N. Sales No. E.71.II.A.1 paras. 214-7, pp. 73-4.


7. Official Secrets Act 1911, available from H.M.S.O.


APPENDIX—BCS POLICY ON COMPUTERS AND PRIVACY

Preamble

The BCS has 22,000 members from all elements of the computing community, by whom it is guided and influenced. As such it is aware of the existing and potential impact of computing technology on the personal and economic lives of us all.

The BCS recognises that computing techniques have much to offer in improving the general quality of life of both the individual and the community. Computing technology is an asset of such power for assisting us to attain real wealth that it becomes essential for it to be used effectively.

Any source of power may be used or misused—the issue of privacy and computers is concerned with ensuring that control may be exercised in such a way as to avoid and prevent the misuse of personal data and in so doing also to encourage the beneficial use of such data.

Computing within our community has attained a stage at which legislative control is required as the White Paper of December 1975 acknowledges.

The policy

1. The policy of the BCS is to encourage the effective use of computing for the benefit of individuals and society and we believe that all regulatory measures to be introduced should reflect this positive attitude.

2. There is a need for legislation to control the use of personal data held on a computer.

3. The regulatory measures should apply to both the public and private sectors.

4. Regulation should be carried out by licensing.

5. Regulation should be associated with appropriate enforcement procedures.

6. The Regulatory measures should include a complaints and appeals mechanism available to organisations and the general public.

7. Regulation should involve the approval of the original purpose and any subsequent revisions thereto for which personal data is collected and processed.

8. The Licensing Authority should have the duty to disclose the existence and purpose of collections of personal data unless it is satisfied that substantial reasons exist to the contrary.

9. Regulatory measures should include the definition of the responsibilities and duties of individuals engaged in a licensed function affecting personal data, together with the authorisation of those individuals.

The Society believes it to be desirable that the Regulatory Authority should be wholly independent and preferably self-financed. However, although data processing costs are currently falling the expenses of the regulatory measures to be embodied should be arranged so as not to inhibit the wider exploitation of computers.