PRIVACY AND DATA BANKS

C.L. SOSKOLNE

Human Sciences Research Council

Résumé Le rapport entre la vie privée de l'individu d'une part, et les banques de documentation de l'autre ne semble pas apparent à première vue. L'auteur essaye de mettre en perspective les rapports existants entre ces deux concepts.

Avec un développement toujours croissant, dans le monde entier, des systèmes de documentation intégrée, les questions d'accès et les possibilités qui existent d'abuser de la documentation ainsi amassée ont été au premier rang des controverses publiques outre-mer.

Etant donné que la centralisation de la documentation est souhaitable et que l'établissement de systémes d'information éducative basés sur une centrale est imminent en Afrique du Sud, une analyse des tendances y afférent semble nécessaire.

Zusammenfassung Der Zusammenhang zwischen Privatheit einerseits und Datensammlung anderseits, ergibt sich nicht ohne weiteres. Es wird versucht die heutige Beziehung zwischen diesen beiden Begriffen klarzustellen.

Die weitverbreitete Verwirklichung integrierter Informationssysteme in der ganzen Welt wirft Fragen auf hinsichtlich des Zuganges zu diesen Informationen und der Möglichkeiten, die so gespeicherten Informationen zu missbrauchen, was im Ausland zu öffentlichen Debatten geführt hat.

Da die Datenzentralisierung immer erstrebenswerter wird und die Gründung zentraler erzieherischer Informationssysteme in Südafrika vor der Tür steht, erscheint eine Analyse verwandter Tendenzen erwünscht.

Opsomming Die verband tussen privaatheid aan die een kant en databanke aan die ander mag nie dadelik opval nie. 'n Poging word aangewend om huidige verhoudings tussen hierdie twee begrippe in perspektief te stel.

Met die uitgebreide implementering van geïntegreerde inligtingstelsels dwarsdeur die wêreld, het vrae ten opsigte van toegang tot en die moontlikheid van die misbruik van inligting wat op hierdie wyse bewaar word, in die openbare polemiek oorsee op die voorgrond getree.

Namate die sentralisasie van gegewens wensliker word en met die vestiging van sentraal geleë opvoedkundige inligtingstelsels in Suid-Afrika wat voor die deur staan, word 'n ontleding van verwante tendense wenslik geag.

Summary The connection between privacy on the one hand and data banks on the other may not be immediately apparent. An attempt is made to place in perspective existing relationships between these two concepts.

With the extensive implementation of integrated information systems throughout the world, questions of access to, and the possibility of abusing information so stored, have recently been in the forefront of public debate overseas.

As the centralisation of data becomes more desirable and with the imminent establishment of centrally based educational information systems in South Africa, an analysis of related trends is felt warranted.

INTRODUCTION : THE PERIOD 1968 TO 1973

"Constitutional problems of the greatest consequence will arise from the extensive and intensive individual enquiries necessary for educational research, from the collection of sets of data about individuals and from the availability of stored information and accessibility to it — for the simple reason that entirely novel instruments of state control can be fashioned from them."

HELLMUT BECKER[5]
1970

General world-wide concern over the subject of privacy had hardly existed to any significant degree before the matter began to come to a head in 1968. Experience had begun to show that storing data on individuals was open to abuse unless entrenched safeguards protected the individual. At that time (1968) the British Vice-Chancellor's Committee drew attention to its concern that if a computerised record were to be established for students, safeguards should be built into the scheme to ensure confidentiality with regard to the individual. The report of the Commission on Privacy in 1968 was an important contribution made by the Government Commission in the implementation of the British Universities' Statistical Record.

In Berlin in 1969 the constitutional principles of planning were being investigated because the "thorny relationships between democracy, science and planning are very important. Legal problems are of very great significance"[5] Hellmut Becker goes on to emphasise the importance of communicating research findings to the public in a comprehensible form and further expresses his concern by saying that "such communication allows the public to be clearly informed about educational policy relating to the future and not the past, and to co-operate with it. This means of communication is necessary if we are to bridge the gap between the moulding of the future by technocratic means and the authorisation for it by democratic means."

In October 1969, Harvard students protested against their university's participation in Project Cambridge*[4]. It was stated that the likelihood of misuse, both by self-serving politicians and by those who are duped by the

* Project Cambridge: An integrated computer facility allowing the behavioural scientist to manage and analyse data simply and to build behavioural models. This Massachusetts Institute for Technology data bank ran into fierce criticism because of its military and political implications.

computer mystique, made the project potentially highly dangerous.

In September 1970 the International Commission of Jurists was commissioned by Unesco to undertake a comparative study on the right to privacy[6]. The results of this comprehensive study were published in the second half of 1972.

The *Cambridge Review* of January 1971[9] recommends, as a solution to possible infringements of individual privacy, that legal and institutional provisions be introduced to encourage and supplement "electronic locks, guards and burglar alarms". There is also a need for organisational and professional ethical codes. Information system auditors are also suggested. By May 1971 a "Control of Personal Information Bill" was presented in the English House of Commons[9]. Chief provisions of the Bill include the establishment of a data bank inspectorate having clear-cut legal powers, and the right of each individual to control the collection, storage and use of personal information about himself. In May 1971 the Privacy Committee of the British Computer Society submitted its evidence to the Younger Committee in the form of a detailed report on computers and privacy[11].

In April 1971 *Minerva*[12] published an article by Laurence H. Tribe entitled: "Legal Frameworks for the Assessment and control of Technology". Tribe expresses his aim in writing as "to explore .... the question of how an enlightened society should use the legal process to influence the development and application of science-based technology."

The December 1971 issue of *Data Systems*[12] devoted a feature to the above problems entitled: "Software Security" and "How Safe Is Your System?".

In the January — March 1972 issue of *Information*[8] IBM points out that while it recognises its responsibility to its customers in providing them with technology for an effective security system, it leaves the matter of ethics — in gathering and disseminating information — to each customer. The Company will continue to offer its views on constructive legislation when they are requested by a government.

Under the title: "On the Question of Statistical Confidentiality", Fellegi[13], in the March 1972 issue of the *Journal of the American Statistical Association,* discusses the nature of the disclosure (violation of privacy) problem. The article also includes a possible approach to the development of automated mass production methods of checking for possible disclosure, and concludes by considering certain confidentiality issues related to different media of data dissemination.

In other countries such as Japan, Canada, France, Switzerland, Sweden, Mexico, Argentina, Venezuela and Brazil[6] individuals, professional and non-governmental organisations, governments and intergovernmental organisations have also at different times through this period expressed concern about privacy.

The literature (in particular 7.1) deals with the 'futuristic' concept of national information-bank systems which are defined "as systems for the integrated storage, processing and distribution of information which give relevant, comprehensible data on request, or by the selective dissemination of information for the making of all information-based judgements and decisions." This implies the co-ordination of or the ability to extract from a variety of 'more specialist' (integrated) data banks. If "it is accepted that data banks and data-bank systems are desirable, then care must be taken that no misuse is possible."

Clearly, the past approximately five-year period has seen the frequency of debate over data banks escalate into world-wide, national investigations with a full range of guide-lines, recommendations and actions ensuing.

The time now appears ripe to present an analysis of the situation in relation to South Africa's own needs, especially in view of the imminent motivations for centralisation and the resultant establishment of automated data banks.

THE ORIGINS OF THE PROBLEM

> "The ability of computers to process vast amounts of data rapidly and economically has made feasible programs and solutions which would not otherwise have been possible."
>
> N. DE B. KATZENBACH[8]
> 1972

Privacy has been a question of law for hundreds of years. Today, however, the whole question is magnified: the nature and scale of potential infringements of privacy is due mainly to the advent of the electronic computer. Information bases of a vastness hitherto unimaginable are operational today.

Today's industrial societies are paying their citizens through computers; bank statements and other official documents are most probably administered by computer. In this personal way, more and more people are realising that many intimate details of their lives are being stored in computerised data bases. The subject of privacy has thus been discovered by politicians in some countries as a subject worthy of debate.

The pace of technological advance in the computer world has more recently facilitated sophisticated technical crimes which can be directed against the broad spectrum of systems utilising data communications networks. This type of 'crime' or breach of security is today possibly as common as the violation of computer systems for criminal means. Accidental corruption of stored data is another problem to be guarded against, with as much care as is applied to system security.

Individual Data Systems (IDSs) are being employed with greater urgency in the fields of education research, not only at institutional administrative levels, but at state departmental levels too. As implied by the name, IDSs 'accumulate' information pertaining to individuals personally over a period of time. The essential purpose in the creation of IDS is for the production of both flow and stock (aggregated) statis-

tical data essential to modern research and planning needs. For this type of information, reports in error of up to, say, one per cent, would be tolerable. We thus have two theoretically possible states for the correctness of each record in such a data bank:

1 error-free records, and

2 erroneous records.

The over-riding problem, however, in debating computer security and its association with privacy and the need for ensuring error-free records or erroneous record tolerability, is clearly that whatever the situation or specifications on our data, individual records are, inevitably, accessible. The two major problems then are those of accessibility and the dangers of individual data (corrupted or otherwise) being made known to a third party.

PRIVACY AND THE RIGHT THERETO VIS à VIS COMPUTERS

> "Any Government could, if it wished, decide to use the centrally gathered information in ways that are not envisaged at the moment. In these circumstances no other body could do much about it."
>
> W. KIRKMAN[9]
> 1971

> "Legislation should be introduced to define the rights of the person whether an individual group or institution, with respect to the privacy of information relating to him, when held by others or handled by them."
>
> PRIVACY COMMITTEE[11]
> 1971

Privacy has been defined by A.F. Westin in his book *Privacy and Freedom* (1967) as the claim of people either individually or collectively to decide when, how, and to what extent information about themselves shall be passed on to others. In fact, what is private varies from day to day and setting to setting. Information, however, can be put to varied uses. On the subject of surveillance, Westin points out that one of its possible subdivisions is that of "data surveillance' which he defines as "the collection, exchange, and manipulation of documentary information about individuals and groups by data-processing machines (primarily computers) which, if enough detailed data are accumulated and collated, can produce such knowledge of an individual's or group's transactions that privacy may be seriously threatened."

The Unesco report[6] states: "As a method of storing information and making it available, computers are not only cheaper and more efficient than conventional methods such as books or files. They operate on an entirely different dimension and make possible the collection, collation and distribution of information on a scale hitherto unthinkable .... The benefits to mankind (from computers) are immense." It is plain that more and more personal data are to find their way into computer memories.

Whilst many of the private issues centre around errors arising in personal records dealing with credit systems and commercial systems in particular, related problems could equally apply to the activities of central and local government. The British Computer Society[11] sees "at least as great a danger to the privacy of the individual from the use of centralised government data banks as from those under the control of privately owned companies trading in information." Risks of personal injustice, invasion of privacy, and exposure to criminal pressure inevitably arise[9] in either case.

As quoted in *Information*[8], Winston Churchill, writing about man's need, and right, to be alone from time to time — in a word, about privacy, said: "The nature of man is a dual nature, ... For some purposes he must be a collectivist, for others he is, and he will for all time remain, an individualist ....." Another quote from the same source states Senator Sam J. Ervin Jr. as tritely saying: "Somewhere, a balance must be struck between the individual's desire to keep silent and the Government's need for information." This latter statement perhaps presents this problem most lucidly, for it implies both an acknowledgement of the value of computers to the people and the need for the people to compromise for the collective good.

The Unesco report[6] gives to Westin's 'data surveillance' concept real proportions: "With on-line multi-access systems, the information stored in a computer can be made available in a matter of seconds in the form in which it is required to users anywhere in the world, provided they are connected to the computer by a telephone line." It is estimated that within twenty years most recorded information will be on computers and more than half the telephone calls in the world will be communications to and from and between computers. Whilst this may indeed be so, the British Computer Society[11] remarks that "as with any new technology, there is as much fantasy as fact in the popular mind with regard to its nature."

"There are a number of ways in which computers can pose threats to the privacy of the individual, but the central one is the fact that they will make it possible for a person having access to the coded data on computers to bring together all the recorded information, often of a private and personal nature, about a particular person in a way that would never have been practical before" warns Unesco[6.1]. The British Computer Society does not believe that the "mere introduction of computers has a material effect on the nature of privacy." It does, however, support the view that the computer "does have an effect on the way in which intrusions into privacy and the unwarranted disclosure of sensitive information may be brought about." The British Computer Society goes on to say: "In fact, certain existing abuses become harder to control, while others can be more readily checked by taking suitable preventative measures. New hazards to privacy of the individual are introduced also, but it is the Society's view that, provided proper safeguards are built into them, computer-based data banks are, on the whole,

less dangerous to the privacy of the individual, group or institution than manual systems."

In G.B.F. Niblett's paper presented at the "Workshop on the Data Bank Society" in London, 1971[6], he reported that the ability of the computer extends to being able 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 an individual wishes to be known. A noteworthy point concerning this report is that the extent of this 'quality' may certainly be questionable if not controlled with the utmost vigilance. On the 'futuristic' concept of national information-bank systems, Müller and Kuhlman[7.2] warn that "if this is not to result in the individual's becoming transparent for data bank users, regulations must be formulated which will achieve data secrecy (protection of the individual's sphere of privacy). In matters of access to and assessment of individual data, it should follow that —

differing regulations governing access to data of differing degrees of 'privacy' will have to be drawn up;

standard regulations will have to be devised to outlaw the unauthorised storage of 'private' data on individuals and make it impossible for the aggregate of the data stored in regard to individuals to be integrated for the purposes of assessment."

The British Computer Society concludes: "Damage to the interests of an individual, group, or institution can occur as a result of intrusions into the privacy of confidential data about him held in a data bank. Damage can also occur due to the dissemination of incorrect data concerning him, particularly if the circulation of such data is clandestine. It is our view that .... legislation is required to establish his right to privacy, to ensure that his interests are protected so far as possible by instituting suitable controls over data bank operation, to provide legal remedies where damage to his interests occurs as a result of a breach of privacy, and to enable such remedies to be enforced."

ADMINISTRATIVE AND TECHNICAL SAFEGUARDS

> "There are no easy solutions to the perplexing problems of protecting privacy in our industrial society. If there were, there would obviously be no urgency in the issue. But .... the problems are being met head-on, not only by the people in the data processing industry itself but also by concerned private citizens, public officials, and authorities in the legal and technical fields. And some of the answers, however hard-won, are beginning to emerge."
>
> E.F. PIERCE[8]
> 1972

Some solutions to the privacy question have been suggested, legislation being one well-motivated solution. In principle, there are also a number of secondary ways in which the individual can be protected against the risk of violation of his privacy (disclosure). These lie in establishing good professional standards, building in technical safeguards and adopting secure administrative procedures. [6.1]

Attempts at a professional code for computer programmers are being made.

Data screening is one method which can be adopted in order to lessen the frequency of errors in storage.

Allowing the individual the right to inspect data stored on him has been suggested.

Programmed safeguards, coded dialling signals, 'locks', and burglar alarms[2] form only a first line of defence.

The formulation of strict ethical codes for the handling of data, backed by severe penalties for infringement, have been suggested as a supplementary form of safeguard.

Computers themselves must be safe from intruders as well as from the elements such as fire and water. Damaged or destroyed data banks can be an expense in terms not only of inconvenience to possibly millions of people, but also in terms of national economy and even security.

The threat of data-tapping via terminal communications also appears in the literature.

F.J.M. Laver[6.3] has compiled a list of administrative safeguards that can be regarded as a set of "model rules" for the operation of individualised data banks. There is no known code of this kind in force anywhere.[6.2]

Regulations governing access to data of differing degrees of 'privacy' will have to be compiled.[7.2]

Through their very nature, the secondary forms of safeguards tabled above are neither easy nor cheap to implement. Clearly then, a form of enforcement is necessary to ensure their adoption. Legal measures are thus considered of primary importance in the safeguarding of information stored in data banks.

Fellegi[13] presents a possible approach to the development of automated mass production methods of checking for disclosure of a 'direct' or 'residual' nature.

LEGAL SAFEGUARDS

> "Many countries have legislation which makes it an offence for public servants to disclose without authority confidential information acquired in the course of their official duties."
>
> UNESCO[6.2]
> 1972

Some of the dangers to individual privacy from the operation of data banks fall within the ambit of existing laws. This is clearly recognised in the above quotation from the Unesco report entitled: *The Protection Of Privacy* by the International Commission of Jurists.

Of primary importance in the protection of privacy are "legal and institutional provisions (which) must encourage and supplement these two kinds of (administrative and technical) safeguard"[9.1], including the possible establishment of data bank inspectorates and policy groups. Legal safeguards will be presented here based on their implementation in other countries and research into some aspects of the problem.

EXISTING SOUTH AFRICAN LEGAL REQUIREMENTS WITH REFERENCE TO DATA BANKS

Laws relating to the gathering, handling and disseminating of information, exist pertaining to the Population Register; statistics on agriculture and business in general; Population Census, Voters Roll; Income Tax; Register of Births, Marriages and Deaths; the Defence Register; Official Secrets, and Research Findings.

Common stipulations

Concerning the gathering, handling and dissemination of information, most of the current laws contain the following provisions:

(i) Registration and the making available of information are compulsory in all cases.

(ii) The nature of the information to be made known and the manner in which this must be done, is described.

(iii) Unauthorised dissemination of information is prohibited and offenders are punishable in terms of the law.

(iv) It is laid down whether and to what extent available information may be used as evidence in a court of law.

Compulsory registration or furnishing of information

In each of the laws referred to[10], registration or the furnishing of information is compulsory.

Dissemination of information

In most of the laws, it appears that there is not much prohibiting general disclosure of certain more general personal information such as, for example, a person's name, sex, age, home address, profession or occupation and identity number (cf. the Population Registration List and the Voters' Roll). It should also be noted that laws permitting the disclosing of these general personal details apply to the population as a whole. Where more personal details are concerned, the dissemination thereof is strictly forbidden (cf. Census Act[10.3] and Income Tax Act[10.2]). In most of the laws, the manner in which gathered data may be published, is laid down. The Statistics Act[10.5] and the Census Act[10.3] stipulate, for example, that the final publication of data must be approved by the minister concerned.

Unauthorised dissemination of information

Regulations forbidding the unauthorised dissemination of gathered information can probably be classified according to two categories:

(i) The unauthorised dissemination of information *by the institution* that gathered it. To prevent an occurrence of this nature, stipulations have been laid down as to the manner in which information may be made known and the nature of such information, as above.

(ii) The unauthorised dissemination of information *by the employees* of the institution. In the law, specific clauses preventing such publicity and penalties for offenders are laid down. The Income Tax Act[10.2] goes even further and requires an oath of secrecy from its employees. The personnel regulations or conditions of service of certain institutions also contain such clauses. The officials of the Department of Defence (including their administrative officers) are, for example, also bound by an oath of secrecy. Although a specific law or regulation does not provide for it, Article 17(m) of the Civil Service Law[10.4], which applies to all civil servants, states that an official is guilty of misconduct and liable in terms of the law to penalties if he, without the permission of his head of department, makes known information obtained in the course of his duties, except as required in the normal course of carrying out his duty.

Use of information as evidence in a court of law

All the relevant laws contain some provision or other concerning the use of available information as evidence in a court of law.

EXISTING FOREIGN LEGAL REQUIREMENTS WITH REFERENCE TO DATA BANKS

Legislation similar to that which is described as existing in South Africa (~~see section 5.1~~) serves many other countries. The Unesco survey details the position[6.2]: "There are provisions of this nature, for example, in the United Kingdom's Official Secrets Act of 1911 and in the Texas Management Act, 1970." Changes are, however, coming about. "Recent legislation establishing national data processing services in the U.K. imposes upon the officials of the Post Office operating the services an obligation of secrecy with penalties of up to two years' imprisonment for unauthorised disclosure. Paragraph 268 of the Federal German Penal Code, which came into force on September 1, 1969, provides for the protection of privacy in automated information systems. In the USA the Fair Credit Reporting Act of 1971 covers the activities of credit reporting agencies. It entitles an individual against whom an adverse report is made, to be told about it. He is entitled to examine the file maintained about him and to have errors corrected. The only country, however, which has introduced any comprehensive legislation dealing with data banks, is the Land Hessen of the Federal Republic of Germany"[6.4]

The Hessen Data Protection Act of 7 October 1970 is included as an appendix to this article[6.5] as a significant piece of legislation in this field. The Act imposes two kinds of protection on data banks:

Data must be handled so that they cannot be consulted or altered in any way by any unauthorised person;

Persons handling the data are to maintain secrecy subject to penal sanctions.

Two kinds of checks are also imposed:

(i) An effective enforcement and complaints procedure in the name of the Data Protection Commissioner is established.

(ii) The individual has the right to correct errors.

Unesco goes on to mention that the Union Internationale des Avocats has prepared for the Council of Europe a draft convention and model law on the right to privacy which deals with the question of data privacy, including data storage, theft or misuse, and the publication thereof [6.4]

Resolution 2450 (XXIII) of the General Assembly of the United Nations has triggered the preparation of reports at the intergovernmental level, the terms of which specify that "these studies may serve as a basis for drawing up appropriate standards for the protection of human rights and fundamental liberties." The report continues: "It is only through an international convention that sufficient legal protection is likely to be provided to ensure that technological devices do not operate to the detriment of legitimate human rights"[6.6].

Privacy has thus been flung into the arena of public debate overseas. The survey conducted by Unesco [6] is undoubtedly a direct result of this fact, and compares in its analysis the following ten countries: Mexico, Venezuela, Argentina, Brazil, Federal Republic of Germany, Sweden, France, Switzerland, United States of America, and the United Kingdom. The concept of privacy and its related implications for the individual in society are causing such concern that they are being analysed thoroughly. So much so, that the said Unesco survey covers the legal standing of related areas not only pertaining to data banks, but also the areas of, for example: "Search of the Person", "Listening and Recording Devices ('bugging')", and "Impact of Employment or Profession on Private Life", to mention but a few of the possible "Intrusions into Privacy".

SOME CONCLUDING STATEMENTS BY THE UNESCO AUTHORS ON PRIVACY [6.7]

The legal protection of privacy should consist of penal as well as civil remedies. The techniques of modern invasions of privacy are such that the ordinary individual has little chance of detecting and bringing to light attacks made on his privacy, even if he were able to do so. The resources of the state should be available to protect him.

It is not enough for the law to give protection only against invasions of privacy by private individuals or corporations. A large part of the electronic surveillance which invades privacy today is carried out by police and other government departments, organs and agencies. Effective administrative controls are required to see that these distasteful and disturbing methods are employed only in really serious cases where the public interest so requires, and it is suggested that the proper degree of restraint is unlikely to be achieved without judicial control of the use of these methods. Unauthorised surveillance by police or state officials should be a serious criminal offence, and evidence obtained by or through it should be inadmissible in any legal proceedings.

The latest and potentially the greatest threat to privacy is the recording, storing and dissemination of personal information by computers. This practice requires to be controlled by special legislation which should (inter alia) ensure —

(i) that the individual has the right to know what information is being collected and disseminated about him, and to have it corrected if it is erroneous;

(ii) that access to the information is strictly controlled;

(iii) that personal information is in general used only for the purpose for which it has been collected; and

(iv) that there is some authority of the nature of an "ombudsman" with the technical resources to see that the legislation is enforced, and with power to receive and investigate complaints.

SOUTH AFRICA IN RELATION TO WORLD TRENDS IN PRIVACY SAFEGUARDS

South Africa indeed conforms strongly to the international legal norm which makes it an offence for public servants to disclose without authority confidential information acquired in the course of their official duties.

The administering of such laws as do exist, has been exercised admirably by such departments as that of Internal Affairs, for instance. Experience in dealing with the gathering, handling and dissemination of information vis à vis the Population Register Act [10.1] has been had; for many years various internal precautions have ensured strict control in the prevention of any unauthorised person from gaining access to information.

The question of the handling of information in view of the advent of the computer and automated data banks has, however, not yet been debated at any public level. Nothing comparable to the work done overseas has been seen in South Africa. The desire to develop a research-oriented centralised student register based on the principle of IDS has met with some reluctance: concern over the safeguarding of the information that is, in fact, to form such a register. Such points as have been raised in other countries have also been raised in South Africa over at least the past two years. Reservations discussed were pertinent not only because it was at this time that most countries were feeling the possible dangers inherent in data banks to individuals, but also because it is plain that passing information on for use in a data bank would be an infringement of the confidence in which such information had initially been gleaned, namely for registration purposes. There is little question as to the benefits resulting from the establishment of such a data base, but at the same time, data safeguards must be entrenched.

From the experience of other countries, it is clear in the mind of the author that legislation in support of technical and administrative safeguards and the establishment of a policy group for particular registers are imperative to the safeguarding of individual data. Securing public support and hence the successful im-

plementation of centralised, integrated information systems are dependent on these initial procedures.

CONCLUSIONS

> "It has not been possible to extend this study to compare the way .... different legal professions operate in practice. It does not, of course, follow that there is more invasion of privacy in the countries with the least legal safeguards. Indeed, the contrary may be true; the need for legislation may not yet have been felt in these countries or not until recently."
>
> INTERNATIONAL COMMISSION OF JURISTS[6]
> 1972

Together with the establishment of centralised, automated information systems, there is an urgent call for data protection throughout the world.

Legal safeguards are of primary importance in reducing the possibility of dangers to individual privacy through the abuse of information stored in automated data banks.

Laws are required for the reinforcement of possible administrative and technical safeguard measures. These are considered as secondary to legislation in the safeguarding of information.

Whilst similar legislation concerning the gathering, handling and dissemination of information exists in most countries, the introduction of new legislation is apparent in many of these. With imminent calls for centralisation, the time in South Africa may indeed be right for due consideration of this subject.

REFERENCES

1. BARTRAM, P. Software security. *Data Systems* Dec., 1971. pp. 16-17.
2. BRAY, M. How safe is your system? *Data Systems* Dec., 1971. pp. 12-15.
3. British bill proposes data bank tribunal and inspectorate, *Communications of the ACM* 14(5), 1971.
4. HANLON, J. The implications of project Cambridge. *New Scientist and Science Journal* 25 Feb., 1971, pp. 421-423.
5. HELLMUT BECKER, H.C.H. Educational Research and planning in modern society. *Universitas* 13 (1), 1970. pp. 1-24.
6. INTERNATIONAL COMMISSION OF JURISTS. The protection of privacy. *International Social Science Journal* XXIV(3), Unesco, 1972.

6.1 Ibid. pp. 421-432.

6.2 Ibid. p. 430.

6.3 Ibid. pp. 418-421.

6.4 Ibid. pp. 430-431.

6.5 Ibid. pp. 580-583.

6.6 Ibid. p. 432.

6.7 Ibid. pp. 577-578.

7. MULLER, P.J. and KUHLMANN, H.H. Integrated information systems, social bookkeeping and privacy, *International Social Science Journal* XXIV(3), Unesco, 1972. pp. 584-602.

7.1 Ibid. p. 596.

7.2 Ibid. p. 597.

8. PIERCE, E.F. Privacy. *IBM Information* Jan-Mar., 1972. pp. 4-6.
9. ROSE, M. Data Banks, the technological dilemma and the 'ascetic option'. *Cambridge Review* 29 Jan., 1971. pp. 97-101.

9.1 Ibid. p. 100.

10. STATUTES OF THE REPUBLIC OF SOUTH AFRICA

10.1 *Population Registration Act* No. 30 of 1950 as amended. Sections 3, 8, 9, 12, 17, 18.

10.2 *Income Tax Act* No 58 of 1962 as amended. Sections 4, 8; Chapter III, Part I.

10.3 *Census Act* No 76 of 1957 as amended. Sections 11, 12, 13, 17.

10.4 *Civil Services Act* No 54 of 1957 as amended. Sections 17(m), 18.

10.5 *Statistics Act* No 73 of 1957 as amended. Sections 5, 8, 9, 15.

10.6 *Registration of Births, Marriages and Deaths Act* No 81 of 1963 as amended. Section 42, Chapters III, IV, VII.

10.7 *Defence Act* No 44 of 1957 as amended. Sections 63, 118.

10.8 *Official Secrets Act* No. 16 of 1956.

10.9 *Consolidation of the Voters' Roll Act* No 46 of 1946 as amended. Sections 9, 15, 21, 26.

10.10 *Human Sciences Research Council Act* No 23 of 1968. Section 11.

11. Submission of evidence to the Committee on Privacy, *The Computer Bulletin* 15(5), British Computer Society, 1971, pp. 169-176.
12. TRIBE, L.H. Legal frameworks for the assessment and control of technology, *Minerva* 9(2), 1971. pp. 243-255.
13. FELLEGI, I.P. On the question of statistical confidentiality, *Journal of the American Statistical Association* 67 (337), 1972, pp. 7-18.

APPENDIX

Data Protection Act[6.5]

State of Hessen
Federal Republic of Germany
7 October 1970

PART I: DATA PROTECTION

Section 1. Scope of data protection

Data protection shall cover all records prepared for purpose of automatic data processing, all stored data and the results of processing such records and data within the purview of the Land authorities and the public corporations, institutions and establishments under the jurisdiction of the Land.

Section 2. Meaning of data protection

The records, data and results covered by data protection shall be obtained, transmitted

and stored in such a way that they cannot be consulted, altered, extracted or destroyed by an unauthorized person. This shall be ensured by appropriate staff and technical arrangements.

Section 3. Data secrecy

1. Persons responsible for the preparation, transmission, storage or automatic processing of data shall be prohibited from communicating or making available to other persons any information concerning the records, data and results gained during the course of their duties and from enabling other persons to obtain such information except where authority exists by this virtue of the provisions of law or the consent of those entitled to exercise control over records, data and results.
2. The prohibition in Subsection 1 shall not apply if the procedures described therein are necessary for the administrative or technical operations involved in data processing.
3. The duty to maintain secrecy shall persist after the completion of the procedures referred to in Subsection 1.
4. The legal duty to provide information shall not be affected.

Section 4. Claim to data protection

1. If stored data are incorrect an aggrieved party may demand rectification.
2. Any person whose rights are infringed by unlawful access, alteration or destruction or by unlawful extraction (Section 2, first sentence) may require that such action be discontinued if there is danger of further infringement.

Section 5. Data banks and information systems

1. Records, data and results may be communicated for the constitution of data banks and information systems and for the statistical purposes of the establishments referred to in Section 1.
2. In the case of data banks and information systems it must be ensured that none of the establishments referred to may consult or extract records, data and results other than those to which it is entitled.
3. Data and stocks of data containing no individual details concerning natural or legal persons and permitting no such details to be inferred may be communicated and published when there is no legal prohibition against it nor any important public interest to prevent it. As a rule public interest shall not stand in the way of the Land Parliament's right to information (Section 6(1)).

Section 6. Right of Land Parliament and local representative bodies to information.

1. The Hessen data processing centre, local district computer centres and the Land authorities operating data-processing installations shall be bound to give the Land Parliament, the Prime Minister of the Land Parliament and the parliamentary parties such information from the stored data as they are entitled to receive, provided the requirements of Section 5, Subsection 3 are satisfied and processing programmes exist.
2. In respect of the Hessen data-processing centre, the relevant local district computer centre and other data-processing installations operated by Gemeinde and Landkreise, the right to information referred to in Subsection 1 shall be vested in district and local councils (Gemeindevertretungen and Kreistage) their political groups and appropriate bodies instituted by the corporations and establishments referred to in Section 1, each within its sphere of responsibility. Any application from the political groups shall be submitted through the Gemeinde authorities or the Kreis Council.
3. In case of doubt the decision of the controlling authority shall be final.

PART II: DATA PROTECTION COMMISSIONER

1. On the proposal of the Land Government, the Land Parliament shall appoint a data-protection commissioner.
2. The data-protection commissioner shall be a public official, under the terms of this Act. A public official in part-time employment, an official on leave or a retired official may be appointed to the office.
3. The data-protection commissioner shall be elected to hold office during the electoral life of the Land Parliament. After the expiration of this period he shall remain in office until the new elections. He shall be eligible for re-election. Before his term of office expires he cannot be dismissed except in circumstances which justify the dismissal of a public servant. He may resign at any time.
4. The remuneration of the data-protection commissioner shall be determined by contract.

Section 8. Freedom from direction

The data-protection commissioner shall be free from direction notwithstanding his obligations under Sections 10 and 12.

Section 9. Secrecy requirements

The data-protection commissioner shall be bound, even after the completion of his term of office, to maintain silence about the facts with which he may become acquainted during his official activities. This does not apply to communications made in the course of his duties or facts that are available to the public or which are not of sufficient importance to require any secrecy. He shall not, without prior authority, whether in a court of law or elsewhere, disclose facts which are subject to secrecy requirements. Such authority shall be given only by the Prime Minister.

Section 10. Duties

1. The data-protection commissioner shall ensure that the provisions of this Act and other regulations governing the confidential hand-

ling of information provided by citizens and of records relating to individual citizens are observed in the course of automatic data processing in the establishments referred to in Section 1. He shall inform the responsible control authorities of any infringements committed and shall initiate measures for improving data protection.

2. The data-protection commissioner shall observe the effects of automatic data processing on the operation and powers of decision of the establishments referred to in Section 1 and note whether they lead to any displacement in the distribution of powers among the Land's constitutional bodies, among local administrations and as between Land and local administration. He shall be entitled to initiate any measures he thinks fit to prevent such effects.

Section 11. Right of complaint

Every person shall be entitled to apply to the data-protection commissioner if he considers his rights to have been infringed by the automatic data processing referred to in Section 1.

Section 12. Investigations on behalf of the Land Parliament and local representative bodies

The Land Parliament, the President of the Land Parliament, the parliamentary parties and the representative bodies referred to in Section 6, Subsection 2 may require the data-protection commissioner to investigate the reasons for which requests for information are not met or not fully satisfied.

Section 13. Right to information

All the establishments referred to in Section 1 shall provide the data-protection commissioner with the information needed in the performance of his duties.

Section 14. Annual report

1. With effect from 31 March 1972 the data-protection commissioner shall submit a report on the results of his activity to the Land Parliament and the Prime Minister by 31 March each year.
2. The Prime Minister shall obtain the Land Government's opinion on the report and present this to the Land Parliament.
3. Interim reports may be submitted and shall be treated as laid down in Subsection 2.

Section 15. Assistance

1. Staff may be made available to the data-protection commissioner by the State Chancellery if required for the performance of his duties. Such staff shall be answerable to him.
2. For specific individual problems the data-protection commissioner may call upon the assistance of third parties.

PART III: FINAL PROVISIONS

Section 16. Offences

Whosoever intentionally or through negligence contrary to Section 3, contributes to making information covered by data protection available to unauthorized persons, shall commit an offence.

Section 17. Commencement

This Act shall come into force on the day it is promulgated. The constitutional rights of the Land Government shall be preserved.

The foregoing Act is hereby promulgated.

Wiesbaden, 7 October, 1970. Osswald
Prime Minister of Hessen