PAPER 5: LEGAL PROBLEMS OF STORAGE AND PROCESSING OF ELECTRONIC DATA

by
F. M. AUBURN
(read by J.A.B. O'Keefe)

Introduction

In the last five years much attention has been paid, throughout the world, to the legal problems connected with the large-scale utilisation of electronic data processing, and the matter has even reached the United Nations.[1] The resultant debate has often yielded more heat than light. On the one hand there is a fear of computers and their operators among the general public which is frequently reflected in newspaper articles.[2] On the other hand, it is argued that consideration of computerised information systems has no relevance in any discussion of privacy as "invasions of privacy are the result of misuses of the data retrieved and not a function of the storage medium."[3]

In this survey it will be suggested that the better view lies somewhere between the two extremes. Such legal problems arising from the misuse of computers cannot be separated from the wider problems of the right to privacy. But the particular questions connected with electronic data processing are clearly urgent, due to the large and increasing utilisation of computers in New Zealand. It is significant that a major role in discussion has been taken by computer professionals. Mr A.L.C. Humphreys, Managing director of I.C.L. recently stressed the need for computer societies to collaborate towards the framing of effective and practical legislation to protect the individual in the future environment of data banks.[4] The British Computer Society has established a Privacy Committee which has made detailed recommendations to the Younger Committee.[5] I.B.M.–U.K. has recently formally endorsed computer privacy legislation.[6] The growing concern within the industry is timely in view of the major investments that will be needed to develop viable technical systems to prevent misuse, and clear indications that the uninformed public is apt to regard the computer as a most dangerous machine.

Computer Use in New Zealand.

Computers are already used very extensively in New Zealand. In Auckland, for instance, the following companies and institutions had computers in use or on order in 1969: Air New Zealand, Alex Harvey, Auckland City Council, Auckland Electric Power Board, Auckland Harbour Board, Auckland Savings Bank, Automobile Association, Berlei (N.Z.), Bond and Bond, Burroughs (N.Z.), Computer Activities, Computer Systems, Consolidated Brick and Pipe, Databank System, Electronic Data Systems, Fletcher Computer Bureau, I.C.L. Centre, John W. Andrew, Johnson and Johnson, Joseph Lucas (N.Z.), J. Steel, Manukau City Council, Motor Specialities, Naval Research Laboratory, N.Z. Newspapers, N.Z. Towel Supply, Plessey N.Z., Pye, R & W Hellaby, Reckitt and Colman (N.Z.), Reid N.Z. Rubber, Smith and Brown, South British Insurance, University of Auckland, Wilson and Horton, Winstone and U.E.B. Industries.[7] It may be noted that this list is not complete, as of 1971, nor does it show the large Government investment in computers which is based in Wellington.

Of particular interest in the present context is Government and institutional computer use. The Treasury was the first organisation in New Zealand to install a computer and has now acquired its fourth. It uses one machine to pay more than 50,000 civil servants, and 27,000 superannuitants and does computer centre work for thirty government departments. Works, Defence and the D.S.I.R. will apparently utilise separate installations. The Health and Education Departments have already met problems in their use of computers.[8] It is not clear what are the contents of the rules governing or forbidding exchange of computer-stored information between government departments and disclosure to outside bodies.[9]

The Minister of Health has approved Hospital Board plans for computerisation which will eventually become part of a national system linking all hospitals. A computer will handle routine hospital administration, keep waiting lists, records, case histories and laboratory work.[10] The National Airways Corporation (N.A.C.) is using Development of Reservations and Communications (DORAC) to handle N.A.C. reservations amounting to 2,600,000 transactions per year.[11] DORAC will also assist other N.A.C. functions such as accounting, spare parts inventory, and the personnel records system. The computer can digest, inter alia, "salaries and wages, individually and in total; each person's location, occupation, grading and sex."[12]

One of the most interesting New Zealand business applications is that of Databank Systems Ltd. Databank Systems process an extremely large amount of transactions (750,000 daily) and has 1,750,000 customer account records on master file, for the five trading banks. From several points of view this company's computer applications, such as the "one job stream" (individual inputs from trading banks branches mixed inseparably but processed separately in the computer) have been highly innovative.[13] The Treasury hands over a reel of magnetic tape to the company for automatic crediting of salaries of government employees to their bank accounts, without individual salary forms.[14] Future developments of this system might lead to a "chequeless society."[15] A recent development is the capacity to enable customers to put questions to the computer by telephone and keyboard, after identification.[16] Databank Systems have given, and are giving, much attention to safeguards in their system,[17] but for obvious reasons, are not divulging full details of the privacy measures already taken.[18]

Present and Future Developments Abroad.

In the United States, United Kingdom and other developed countries, the debate on computer privacy has been carried on for several years. In the United States official proposals to establish a computerised National Data Center[19] followed the report of E.S. Dunn Jr. which had initiated a series of Congressional and Senate Hearings.[20] Among recent United States developments are the disclosure of the existence of an Army computer databank concerning itself with domestic manifestations of a lawful nature such as conscientious objectors, the N.A.A.C.P. and non-violent pacificist organisations,[21] and the creation of N.C.I.C.,[22] a national computerised record to be based on fingerprint identification, accessible by government agencies at all levels connected with criminal investigations, correction and parole. Examples of computer developments in the United Kingdom are Dun and Bradstreet's service

giving immediate data on 200,000 businesses, a vehicle a driver licensing control computer at Swansea to deal with 500,000 transactions a day, the £57,000,000 Inland Revenue computer covering the tax affairs of 25,000,000 people and a planned National Police computer with 700 terminals throughout the country.[23]

Tracing Services Group aim to have files on 80% to 90% of the population by 1980. Private detective agencies sell items of information such as a person's bank balance, criminal record (if any) or his ex-directory telephone number to any interested party. "Even dates are fixed from data banks by computer cupids."[24]

This brief review of some overseas developments may serve to show the extent to which computers have become repositories of information, confidential or otherwise, with the attendant possibilities of abuse.

The Law Today

The question whether a general right of privacy exists at common law is not settled. Despite assertions that there is no general right of privacy recognised by the common law,[25] and the possibility that Canadian common law jurisdictions might recognise a general right of privacy apart from statute,[26] it is generally accepted that no English court has given a remedy for invading the personal seclusion of an individual *per se*, apart from his occupancy of land or his holding of some form of private property.[27]

On the other hand, indirect protection is afforded by various heads of action in tort. But such actions are generally limited. For instance, trespass usually demands some physical interference which may be absent in cases of computer abuse. Defamation is only of limited utility.[28] Similar limitations appear in attempts to use other torts for the indirect safe-guarding of privacy. In United States jurisdiction a right to privacy has been elaborated upon the argument of Warren and Brandeis.[29] This right was in part based upon the English common law, and particular emphasis was placed upon the well-known case of *Prince Albert* v. *Strange*[30] in which Lord Cottenham L.C. specifically stated that privacy was the right invaded.[31] Whilst Warren and Brandeis regarded this case as a recognition of a more liberal doctrine than the protection of property[32] it has been argued that the decision of the court was based primarily on the plaintiff's proprietory rights.[33]

Although there has been much recent discussion regarding such a right of privacy, it is suggested that a general right of privacy, even if it were accepted by the New Zealand courts as part of the common law, provides no real solution of the problems of computer privacy. The general right as given in United States jurisdictions raises difficulties which courts have grappled with for long with little success,[34] and has been regarded as inadequate to deal with the realities of the computer age,[35] due to the possible absence of a duty of confidentiality between the parties, the necessity for the information concerned to be accurate to ground an action, and the question whether the information is "private".[36] Even if the United States general right of privacy is viewed as superior to the present English and New Zealand approach[37] the problems set by electronic data processing are not solved. If there is a general right of privacy we are still no nearer to a definition of the circumstances in which it is applicable to computers.

A possible approach to the definition of a duty of confidentiality of some particularity is to be found in *Furniss* v. *Fitchett.*[38] Dr Fitchett, the regular medical attendant of Mr and Mrs Furniss gave Mr Furniss a letter concerning his wife's health which was later produced in court by Mr Furniss's solicitor. Mrs Furniss sued Dr Fitchett on two causes of action. Her claim for libel was abandoned, the court holding that the defence of justification was bound to succeed. The second cause of action could, the court held, have been grounded in contract[39] on an implied term of confidentiality, but was actually pursued in tort.

The certificate was not deliberately false, incorrect or untrue. Dr Fitchett's negligence lay in the manner in which he released the report and in not foreseeing that at some stage Mrs Furniss could be confronted with it in circumstances which might injure her.[40] Here there was physical injury (shock) bringing this novel situation within the rule in *Donoghue* v. *Stevenson.*[41] Liability was incurred for a negligent act, not for a negligent use of words,[42] but the distinction between words and conduct in such cases is often a fine one.[43] Liability arose from the manner of communication not from the fact of communication.[44]

It would therefore appear that there are some substantial privacy safeguards at common law in regard to the medical use of computers. In an appropriate case it also might be possible to invoke the sanctions of the Medical Practitioners Act 1968 ranging from a fine up to $200 for professional misconduct,[45] to removal of the offender's name from the register for disgraceful conduct in a professional respect.[46] Some indication of the content of such offences may be gained from the very strict duty of confidentiality enjoined upon practitioners by their Code of Ethics. Such penalties could only be applied to a medical practitioner, and would therefore not be applicable to persons such as programmers and other employees of computer service firms. On the other hand, the medical practitioner might be held responsible for the unauthorised divulgence of such information by other persons if he should have foreseen such a possibility. The particular duties of medical practitioners appear to be capable of stringent definition from the point of view of civil liability[47] and disciplinary sanctions.[48] Computerisation of patients' medical records, as suggested in New Zealand,[49] therefore demands not only protection of the patient's privacy[50] but also clarification of the medical practitioner's liability.

Whilst the liability of a medical practitioner for computer privacy may well be more than complete, the same cannot be said in regard to hospitals. No person employed by a hospital board shall give a person not no employed any information concerning the condition or treatment of any patient in any institution without the prior consent of the patient or his representative.[51] But nothing in the section applies to information connected with further treatment or required in the course of official duties by officers of the Health, Justice, Social Security, Transport, Defence or Police Departments or any officer of Her Majesty's forces. Nor does the section affect information required pursuant to any Act or needed for health statistical purposes or required by persons prescribed by the Minister. Whilst the intent of these exceptions is clearly to enable such disclosure, it is not clear whether this intent is indeed carried out. It is stated that "nothing in this section shall apply with respect to"[52] the exceptions. In other words the section does not, *prima facie,* in any way affect

the medical practitioner's duties of confidentiality previously described. Clearly this will raise serious problems if patients' records are computerised and are thus easily accessible to (for instance) the Government departments or the persons named by the Minister under s.62(2)(h). Similar problems could well arise on the compulsory reporting by medical practitioners of deaths during and shortly after termination of pregnancy.[53]

Census

Censuses, processed by computer, have recently raised much controversy in several countries. Mr Thorpe, Leader of the British Liberal Party; contemplated refusing to fill in his own census form on 25 April 1971 having particular objections to questions concerning immigrants.[54] Official Government assurances pointed out that privacy was to be safeguarded by statutory penalties.[55] But there was no unequivocal Government statement that nothing apart from material available to all in published statistical material would not be sold to commercial interests or used by Government departments.[56]

Concern with privacy begins at the level of the enumerator. At least one conviction was entered against an enumerator for revealing information.[57] If census information is broken down into the 100 metre squares in accordance with the National Grid households occupying a single grid square can be instantly identified. 300 organisations have requested census information, and the question is to what extent area breakdowns are available and can be correlated.[58] The fact that data in a computer are not identified by name does not, of itself, provide a firm safeguard against persons wrongfully extracting information in an identifiable form.[59]

Whilst New Zealand's 1971 census was of relatively modest proportions,[60] complaints regarding privacy were numerous. In most cases these related to the questions put.[61] It was asked whether it is really essential to know people's religion, and how reliable the resulting answers are. Why were questions put regarding salaries which could be ascertained from the Inland Revenue Department? Doubts were expressed about the sub-enumerators whose "amateur short-lived bond of secrecy has to wrestle with the powerful natural forces of curiosity and gossip."[62]

The provisions of the Statistics Act, 1955 are not, it is submitted, suited to the current computerised census. Information furnished under the provisions of the Act shall be used for statistical purposes only.[63] There is no definition of "statistical purposes" and therefore no inherent limitation of use of information only for purposes not requiring individual identification. "A person working under arrangements with the Department" may be permitted to see individual schedules.[64] The central privacy provisions[65] forbid separate publication or communication of individual answers or parts of completed schedules to other Departments of State without prior written consent of the individual concerned.[66] In the computer context it is not clear what may be meant by "communication". Does this only cover the actual handing over of print-outs? Legal safeguards which may have been adequate in 1955 do not appear to be so today.

Credit Reporting

An area of business which is suitable for computerisation is credit reporting, and this has taken place in the United States.[67] Credit reporting has been the subject of recent study in Canada.[68] In Ontario a man was unable to obtain work due to an unspecified charge of loose morals. He was unable to get the reporting company to show him the file which any subscribing firm could see for about $25.00 a time nor did he have any means of compelling removal of the information.[69] A professional man in Winnipeg bought a car and decided to pay the balance by instalments. Shortly afterwards he learnt that a 19 year-old girl had been asking personal questions about him in the neighbourhood.[70]

The Legal Research Institute of the University of Manitoba has investigated the problem and recommended licensing legislation, prohibiting non-disclosure of the agency's identity and obliging credit agencies to furnish copies of reports to the individual reported on.[71] The Associated Credit Bureaus of Canada have published a policy statement to the effect that information on the file will be disclosed to the customer, no reference is to be made to race, religion, political affiliation or personality, and judgments will only be reported for seven years.[72] Most Canadian credit organisations consider that computerisation of credit reporting is inevitable.[73] Two Bills have been introduced into Canadian provincial legislatures to regulate credit reporting. One Bill provides, *inter alia,* for licensing by a Registrar of Credit Reporting Agencies and for penalties up to $25,000 for contraventions.[74] The second Bill has no such registration provisions and has a maximum penalty of $2,500.[75] The Ontario Bill specifies the information which may be collected or stored by an agency.[76] The Manitoba Bill does not do this but forbids personal reports containing specified information such as reference to race, religion, ethnic origin or political affiliation unless voluntarily supplied by the subject.[77] Both Bills will demand careful study when such legislation is contemplated in New Zealand, but it may be suggested that neither deals with computerised file problems.

In New Zealand credit managers may obtain information from a wide variety of sources. These include other creditors, trade groups, salesmen who may be trained to watch for "changes in personal habits that could be derogatory", banks, employers, landlords, relatives and neighbours.[78] The practice of some agencies of obtaining information from summonses before judgment is obtained is to be stopped,[79] and has brought a demand for legislative protection of privacy in this field.[80] Weight may be lent to this demand by the recent allegation that in New Zealand bank balances of other persons may be obtained by a telephone call without even giving the account number as can details of payments to finance companies. The credit manager of a leading credit information bureau, Dun's Agency, has asserted that "there is a definite need for some kind of statutory control on the sort of information disseminated".[81] The law as it stands is not overly helpful to the victims of any possible mistakes by credit reporting agencies[82] and requires examination with particular regard to the possibility of the future computerisation of credit data.

Identity Number

A central concept in the functioning of nationwide computer databands is a unique identifying system or number. Such a databank may also function by

record linkage without a unique identifying system but record linkage is far from perfect and presents many difficulties. On 1 January 1973, several "years ahead of Orwellian projection", every West German citizen will have a twelve-digit number as the government's registration system is being computerised.[83] The West German Interior Ministry asserted that there was no desire to encroach upon privacy.[84] The Japanese Administrative Management Agency hopes to have a national identity number in 1972[85]. A government interdepartmental committee is discussing the question in the United Kingdom.[86] The possibility of an E.E.C. uniform computer supported identification system has already been mooted.[87]

In New Zealand it has already been suggested that every person should have a number to be used only for National Health Service purposes.[88] This report anticipated fears about infringement of confidentiality together with "less rational feelings that a mechanism for totalitarian tyranny is being set up."[89] To allay such fears it was suggested that there be special restrictions to ensure that the number be only used for health purposes.

The late Minister of Justice, Hon. J.R. Hanan, stated that the Government had no intention of introducing a system compelling citizens to carry identity cards, this being "instinctively opposed by most New Zealanders.."[90] However, the 1970 Annual General Meeting of the New Zealand Computer Society resolved to "investigate a unique identification system to facilitate communication." The emphasis is to be on technical and economic aspects.[91] This writer can only reiterate that such a system would be a direct attack on privacy.[92] Such a number would permit the free exchange of information between government departments and to commercial undertakings. The most rigorous presently known technological safeguards would be quite insufficient to prevent abuse. Such possibilities have already been foreseen.[93]

Conclusion

It has been pointed out that the existing law relating to privacy was fragmentary and ineffective before the advent of computers. As an example, in a recent New Zealand case an electronics engineer monitored his wife's telephone calls and utilised the evidence in divorce proceedings in the Supreme Court. He was convicted of an offence, presumably under S.158 of the Post Office Act 1959, and fined $50 and costs.[94]

The Minister of Justice has recently emphasised that many feel the fear that centralisation of information in databanks is capable of serious abuse.[95] The Minister regards databanks as the most urgent privacy problem in New Zealand and envisages legislation. The Law Revision Commission's Criminal Law Reform Committee has invited a report on the law and the need for reform.[96] It is to be hoped that this report will be available to legal practitioners and computer professionals. The New Zealand Section of the International Commission of Jurists has prepared a Bill[97] giving a general right of privacy and making wilful and substantial interference therewith a tort. This Bill does not specifically deal with computer problems. In April 1971 Mr Ross Medland convened a Symposium on Computers' Challenge to Man's Social Conscience at the University of Otago.[98] The New Zealand Computer Society, apart from its previously mentioned unique identification system study[99] has taken for the theme of the Third National Computer Conference in August 1972 "Computers

in the Community" and will focus on "active symposia confronting the vital problems facing . . . the community as a whole."

It is suggested that attention could be given to the Privacy and Computers Task Force established by the Canadian Department of Communications and Justice, constituted of officers of the Departments and fifteen consultants. The Task Force is undertaking a multi-disciplinary study of the whole problem including, *inter alia,* study of present and future computer systems, statistical data-banks, security procedures, legal remedies, administrative and regulatory measures, self-regulatory provisions and constitutional considerations.[100] It is submitted that such a comprehensive investigation is needed before embarking upon the drafting of Bills, Codes of Ethics and administrative procedures. Numerous Computer Privacy Bills have been drafted,[101] but there is not yet, in New Zealand or elsewhere, a comprehensive review of the present and future impact of electronic data processing on society. Such a review is a prerequisite to legislative and administrative action affecting a vital and rapidly growing industry which impinges upon every aspect of the citizen's life.

APPENDIX

PERSONAL RECORDS (COMPUTERS /H.L./

A

BILL

INTITULED

An Act to prevent the invasion of privacy through the misuse of computer information. A.D. 1969

Be it enacted by the Queen's most Excellent Majesty by and with the advice and consent of the Lords Spiritual and Temporal and Commons, in this present Parliament assembled and by the authority of the same as follows:

Register of Data Banks.

1.- (1) A register shall be kept by the Registrar Trading Agreements (hereinafter in this Act referred to as "the Registrar") of all data banks as hereinafter defined which are operated by or on behalf of any of the following:—

(a) any agency of central or local government
(b) any public corporation
(c) any person exercising public authority;
(d) any person offering to supply information about any other person's credit-worthiness, whether to members of a particular trade or otherwise and irrespective of whether payment is made therefore;
(e) any private detective agency or other person undertaking to carry out investigations into any other person's character, abilities or conduct on behalf of third parties
(f) any person who offers for sale information stored in such data bank whether to the general public or otherwise.

(2). The register referred to in the foregoing subsection shall contain the following information concerning each data bank:—

(a) the name and address of the owner of the data bank
(b) the name and address of the person responsible for its operation
(c) the location of the data bank
(d) such technical specifications relating to the data bank as may be required by the Registrar;
(e) the nature of the data stored or to be stored therein
(f) the purpose for which data is stored therein;
(g) the class of persons authorised to extract data therefrom.

(3) The owner of the data bank shall be required to register the information referred to in pargraphs (a) to (c) of the foregoing subsection. The person responsible for the operation of the data bank shall be required to

register the information referred to in paragraphs (a) to (g) of the foregoing subsection.

(4). Any person responsible for registering information under this section shall be required to inform the Registrar of any alterations of additions to or deletions from the said information within four weeks of such alteration taking effect, subject to the provisions of subsection (6) below.

(5). If at any time the register is of the opinion that in the circumstances the information given or sought to be given under paragraphs (f) or (g) of subsection (2) above might result in the infliction of undue hardship upon any person or persons or be not in the interest of the public generally he may order such entry to be expunged from or not entered in the register. In reaching a decision under this or the next following subsection, the Registrar shall be guided by the principle that only data relevant to the purposes for which the data bank is operated should be stored therein, and that such data should only be disclosed for those same purposes.

(6) An alteration to the register in respect of paragraph (f) or (g) of subsection (2) above shall be made by application to the Registrar who shall, not earlier than four weeks after receipt of such application, grant or reject the application giving his reasons in writing.

(7) The register together with applications submitted in accordance with the last foregoing subsection shall be open to inspection by the public, including the press, during normal office hours:

Provided that entries relating to data banks operated by the police the security services and the armed forces shall be kept in a separate part of the register which shall not be open to inspection to the public.

Records to be maintained by operators of certain data banks.

2.- (1) This section shall apply to all data banks which are required to be registered under section 1 above except for the following:—

(a) data banks which do not contain personal information relating to identifiable persons;
(b) data banks operated by the police;
(c) data banks operated by the security services;
(d) data banks operated by the armed forces of the Crown.

(2) The operator of each data bank to which this section applies shall maintain a written record in which shall be recorded the date of each extraction of data therefrom, the identity of the person requesting the data the nature of the data supplied and the purpose for which it was required.

Annual Report

3.- (1) The Registrar shall submit annually to Parliament a report covering the previous calendar year in which he shall state the number of data banks entered on the register, the number of such data banks which fall within the terms of section 2(1)(a) and of section 2(1)(b) to (d) respectively and the number of instances in which he ordered entries to be amended under section 1(5) or refused an application to alter an entry under section 1(6).

(2) The Registrar's report may contain such additional information statistical and otherwise, as the Registrar may think fit.

Information to be supplied by operators of certain data banks.

4.- (1) Any person about whom information is stored in a data bank to which section 2 above applies shall receive from the operator, not later than two months after his name is first programmed into the data bank, a print-out of all data contained therein which relates to him. Thereafter, he shall be entitled to demand such a print-out at any time upon payment of a fee the amount of which shall be determined by the Registrar from time to time; and the operator shall supply such print-out within three weeks of such demand.

(2) Every print-out supplied in accordance with this section shall be accompanied by a statement giving the following information:

(a) The purpose for which the data contained in the print-out is to be used, as entered on the register referred to in section 1 above;
(b) The purpose for which the said data has in fact been used since the last print-out supplied in accordance with this section
(c) The names and addresses of all recipients of all or part of the said data since the last print-out supplied in accordance with this section.

Application for amendment or expunging of data.

5.-(1) Any person who has received a print-out in accordance with section 4 above may, after having notified the operator of the data bank of his objection, apply to the Registrar for an order that any or all of the data contained therein be amended or expunged on the ground that it is incorrect, unfair or out of date in the light of the purposes for which it is stored in the data bank.

(2) The Registrar may, if he grants an order under the foregoing subsection, issue an ancillary order that all or any of the recipients of the said data be notified of the terms of the order.

Offences

6.- (1) It shall be an offence punishable on summary conviction by a fine of not more than £500, or on conviction on indictment by a fine of not more than £1000 or imprisonment for not more than five years or both, for the owner or operator of a data bank to which this Act applies to fail to register it in accordance with this Act.

(2) If the operator of a data bank to which Section 2 above applies:—

(a) fails or refuses to send a print-out when under a duty so to do or
(b) permits data stored in the data bank to be used for purposes other than those stated on the register; or
(c) allows access to the said data to persons other than those entered on the register as having authorised access; or
(d) fails or refuses to comply with a decision of the Registrar,

he shall be liable in damages to the person whose personal data is involved and, where such acts or omissions are wilful, shall be liable on summary conviction to a fine of not more than £500 and on conviction on indictment to a fine of not

more than £1000 or imprisonment for not more than five years or both.

(3) A person who aids, abets, counsels or procures the commission of an offence described in this section or with knowledge of its wrongful acquisition receives, uses, handles, sells or otherwise disposes of information obtained as a result of the commission of such an offence shall likewise be guilty of the said offence.

Liability for damages

7. An operator of a data bank to which this Act applies who causes or permits inaccurate personal data to be supplied from the data bank as a result of which the person to whom the data refers suffers loss, shall be liable in damages to such person.

Rules

8. The Registrar may make rules relating to the implementation of any part or parts of this Act and in particular relating to –

(a) the keeping of the register and records referred to in sections 1 and 2 above;
(b) access by the public to the register referred to in section 1 above;
(c) procedure on hearing objections and argument on a proposal to alter or expunge from the register under subsection 5 of section 1 above;
(d) procedure on application to alter the register under subsection 6 of section 1 above
(e) verification of the identity of a person demanding a print-out in accordance with section 4 above.

Appeal

9. An appeal shall lie to the High Court from any decision made by the Registrar under this Act.

Definitions

10. In this Act, the following terms shall have the meanings hereby respectively assigned to them, that is to say –

"data" means information which has been fed into and stored in a data bank;

"data bank" means a computer which records and stores information;

"operator" means the person responsible for the operation of a data bank and for the introduction into and extraction from it of data;

"owner" means the person who owns the machinery comprising the data bank;

"print-out:: means a copy of information contained in the data bank supplied by the computer and translated into normal typescript.

11. There shall be paid out of moneys provided by Parliament any expenses incurred by the Registrar attributable to the provisions of this Act.

Short Title, commencement and extent.

12.- (1) This Act may be cited as the Personal Records (Computers) Act 1969.

(2) This Act shall come into force on the first day of July 1970.
(3) This Act shall extend to Northern Ireland.

FOOTNOTES:

1 Report of the Secretary-General, "Human Rights and Scientific and Technological Developments", E./C.N.4/1028/ Add.3, 4 March 1970.
2 "Are computer-programmers human beings? . . . will the computer disciples consistently use their special powers for the good of mankind? Or will they launch into a course of tyranny?" " 'Nannies' must be watched . . ." N.Z. Truth, 15 September 1970.
3. T.J. Vander Noot, "The Computer and Privacy: No Relationship" Conference on Computers:Privacy and Freedom of Information, Queen's University, 21-24 May 1970.
4 "Computer People and their Responsibility", 4(2) Data Processing in New Zealand, June 1971, p.5.
5 "Submission of evidence to the committee on privacy", 15(5) The Computer Bulletin, May 1971, p.169, at p.176.
6. "The establishment of an agency to supervise Government databanks and public access to information stored in them can only have a beneficial effect", Mr Parry Rogers, I.B.M.–U.K. quoted in "IBM goes public on computer privacy", New Zealand Scientist and Science Journal, 10 June 1971, at p.628.
7 "Computer Census", 2(4) Data Processing in New Zealand, December 1969, 14.
8 F.M. Auburn, 'Computers and Privacy in New Zealand", Otago University Computer Privacy Symposium, April 1971, 1.
9 F.M. Auburn, "The Databank Society", Recent Law, 1971 (to be published).
10 "Patient's history available from computer", N.Z. Herald, 18 November 1970.
11 Hon J.B. Gordon, N.Z.P.D. 9 March 1971, p.220.
12. Supplement to "Skylines", August 1970.
13. G.R. Davy, 'The Databank System", 1(2) Data Processing in New Zealand, October 1968, 13,15.
14. *Ibid.*, p.17
15. cf. *Ibid,* p.15.
16 Computer is given a T.V. voice', N.Z. Herald, 23 March, 1971.
17 F. Bland, "How computer utilities should protect users", Data Trend, June 1971, p.11.
18 F.M. Auburn, f.n.9.
19 e.g. Executive Office of the President, 'Report of the Task Force on the Storage of and Access to Government Statistics," October 1966, p.17.
20 A.F. Westin *Privacy and Freedom* (1967) 315 *et seq.*
21 C.H. Pyle. ' The Army watches politics", 2(12) Washington Monthly, (1970) 6.
22 National Crime Information Center.
23 M. Warner and M. Stone, *The Data Bank Society* (1970), 103 *et seq.*
24 M. Beloff, ' The Inquisitive Society", Encounter, December, 1970, 49.
25 Per Evatt J., *Victoria Park Racing and Recreation Co. Ltd.* v. *Taylor* (1937) 58 C.L.R.479,521.
26 *Krouse* v. *Chrysler Canada Ltd.* (1970) 12 D.L.R.3d.463.
27 D.A. Cornfield, 'The Right to Privacy in Canada", 25 Faculty of Law Review (Univ. of Toronto) (1967) 103,108.
28 Justice, *Privacy and the Law* (1970) 11.
29 S.D. Warren and L.D. Brandeis, "The Right to Privacy", 4 H.L.R.(1890) 193.
30 (1849) 1 Mac. & G.25.
31 *Ibid.*, 47.
32 F.n.29, at p.204.
33 B. Neill, ' The Protection of Privacy", 25 M.L.R. (1962) 393,395.
34 G.D.S. Taylor, "Privacy and the Public",34 M.L.R. (1971) 288,304.
35 A.R. Miller, 'Personal Privacy in the Computer Age: the Challenge of a New Technology in an information-oriented Society", 67 Mich.L.R.(1969) 1089,1156.
36. *Ibid,* 1158-1160
37 For a possible contrary view, see E.H. Flitton and G. Palmer, *"The Right to Privacy: A comparison of New Zealand and American Law."* 3 (4) Recent Law (1968) 86,97.
38 [1958] N.Z.L.R.396.
39 At p.400
40 At p.401
41 [1932] A.C.562.
42 L.L. Stevens, *Negligent Statements causing financial loss,* (1970) 48.

43 J.F.B., *"Hedley Byrne* and Financial Loss" (1971) N.Z.L.J.55.
44 B.D. Inglis, *Furniss* v. *Fitchett:* A Footnote (1958) N.Z.L.J. 235.
45 S.43(2)(a).
46 S.58(2)(a).
47 Cf. also, *Wyatt* v. *Wilson* (unreported) cited in *Prince Albert* v. *Strange,* f.n.30. at p.46.
48 For other aspects of medical computing liability see R.N. Freed, "Legal Aspects of Computer Use in Medicine", 32 Law and Contemporary Problems", (1967) 674.
49 T.K. Williams, "Responsibility for Health: The need for improved General Practitioner Records", 72 N.Z.Med.J. (1970) 304.
50 *Ibid.,* 307
51 S.62, Hospitals Act 1957
52 S.62 (2).
53 Maternal Mortality Research Act 1968, S.9.
54 R. Nelson, "Britons wary of census", Christian Science Monitor, 20 April 1971.
55 "The Population Census", Survey of Current Affairs, May 1971.
56 "The Census – Doing the Privacy Thing", 121 N.L.J.22 April 1971, at p.331.
57 *Registrar-General* v. *Charles Mann,* Clerkenwell Magistrates' Court, 4 June 1971 (unreported).
58 N. Foy, "A Bonfire of census forms", 50 New Scientist and Science Journal, 15 April 1971, p 132.
59 L.J. Hoffman and W.F. Miller, "Getting a Personal Dossier from a statistical data bank", Datamation, May 1971, p.74.
60 In Canada, for instance, 1971 Census Representatives were provided with a volume of 180 pages for answering householders' enquiries, Dominion Bureau of Statistics, *Content Manual* (1971).
61 For instance, Question 13 asked "If you are a woman who is or has ever been married, state the number of children born alive to you during your lifetime, including those now deceased." The Government Statistician undertook not to prosecute women married more than once who "suppress the facts"–"Secrets can stay despite Census", Auckland Star, 19 March 1971.
62 "Census-taking", Otago Daily Times, 3 April 1971.
63 S.18 (1)
64 S.18 (2)
65 Not applicable to persons under S.18(2).
66 S.18 (3)
67 See Miller, Footnote 35, at pages 1140-1154.
68 J.M. Sharp *Credit Reporting and Privacy* (1970)
69 Hon. Al. Mackling, Q.C., Attorney-General, Manitoba, Debates of Legislature of Manitoba, 24 June 1970, 3170,3172, quoting C. Tower, "The Credit–Spy can ruin you. He knows–and tells", Maclean's Magazine, March 1970.
70 R. McKeown, 'Your private life is public knowledge,' 19 Montreal Star Weekend Magazine, 22 November 1969.
71 R.D. Gibson and J.M. Sharp, *Privacy and Commercial Reporting Agencies* (1968) 31.
72 M.T. Pearson, "Data Banks for Credit Bureaus", in Conference, footnote 3.
73 *Ibid.*
74 The Consumer Credit Reporting Bill 1971, Ontario
75 The Personal Investigations Bill 1971, Manitoba
76 S.21, footnote 74.
77 S.4, footnote 75.
78 J.E. Allen, "Sources of Credit Information", Credit Management, May 1968.
79 "Early court search by credit bodies to be stopped", Auckland Star, 1 June 1971.
80 "Secrets on file", Auckland Star, 10 July 1971
81 T. Bell, "Don't Look now, but your skeleton is showing . . .", 8 O'Clock. 29 May 1971
82 J.M. Sharp, "Your credit and your privacy", 7(2) Canadian Consumer, Sept.-Oct. 1969, 59, 62.
83 "Just Call Him 181213 312345", Time, 12 July 1971
84 "Germans to get Identity Numbers", The Bulletin, 13 July 1971
85 "Numbers game in Japanese Bureaucracy", Auckland Star, 22 April 1971.
86 British Medical Association, Planning Unit Report No.3, "Computers in Medicine", 32.

87 "Common Market and Uncommon Privacy", New Scientist and Science Journal, 11 March 1971, at p.529

88 Medical Research Council of New Zealand, *Adequacy of Medical Statistics in New Zealand,* (1969) 21.

89 *Ibid,* 22

90 N.Z.P.D., 9 October 1968, p.2182.

91 Annual Report, New Zealand Computer Society (Inc.), 21 May 1971.

92 "Number Plan "attack on privacy' ", New Zealand Herald, 9 December 1970.

93 M. Still, "The Privacy Debate", 3(2) Data Processing in New Zealand, (1970) 3,4.

94 *Police* v. *Ian Ross Richards,* Magistrate's Court, Upper Hutt, 20 October 1970 (unreported), described in "$50 fine for tapping wife's phone calls", New Zealand Herald, 21 October 1970.

95 D.J. Riddiford, 'The future for Law Reform in New Zealand", (1971) N.Z.L.J.276, 279.

96 "Call to protect privacy", Auckland Star, 28 April 1971.

97 Protection of Privacy Bill, July, 1971

98 F.M. Auburn, footnote 9

99 Footnote 91

100 A.E. Gottlieb, Symposium on "Computers and Privacy", University of Toronto, June 1, 1971.

101 See, for instance, Personal Records (Computers) Bill 1969 (H.L.).