SOUTH AUSTRALIA

FIFTIETH REPORT

of the

LAW REFORM COMMITTEE
of
SOUTH AUSTRALIA

to

THE ATTORNEY-GENERAL

REGARDING DATA PROTECTION

1980

The Law Reform Committee of South Australia was established by Proclamation which appeared in the *South Australian Government Gazette* of 19th September, 1968. The Members are:

THE HONOURABLE MR. JUSTICE ZELLING, C.B.E., *Chairman.*

THE HONOURABLE MR. JUSTICE WHITE, *Deputy Chairman.*

THE HONOURABLE MR. JUSTICE LEGOE, *Deputy Chairman.*

D. W. BOLLEN Q.C.

M. F. GRAY S.-G.

J. F. KEELER.

D. F. WICKS.

The Secretary of the Committee is Miss J. L. Hill, c/o Supreme Court, Victoria Square, Adelaide 5000.

FIFTIETH REPORT OF THE LAW REFORM COMMITTEE OF SOUTH AUSTRALIA REGARDING DATA PROTECTION

To:

The Honourable K. T. Griffin, M.L.C.,
Attorney-General for South Australia.

Sir,

In 1973 we furnished the then Attorney-General with an Interim Report regarding the law of privacy, which contained recommendations for changes in the law falling under two broad headings:—

(1) creating a nominate tort relating to the loss of or violation to a person's privacy; and

(2) covering the use of surveillance techniques, computers, data banks and similar electronic inventions of the present day.

Our proposals under the first heading were sought to be enacted by the then Attorney-General Mr. L. J. King, Q.C., now the Chief Justice, when he introduced the Privacy Bill into the House of Assembly on 10th September, 1974.[1] That Bill failed to become law.

Therefore, with respect to the concept of a nominate tort of privacy, we would refer you to the following articles which have appeared since 1974 and which we feel may be of assistance to you in any further deliberations on this particular aspect of the law of privacy:

(1) "Privacy and the Public" by G.D.S. Taylor 34 M.L.R. 288.

(2) "Infringement of Privacy and its Remedies" by H. Storey, M.L.C. 47 A.L.J. 498.

(3) "Protection and Privacy" by Jane Swanton 48 A.L.J. 91.

(4) "Freedom from Unwanted Publicity" by C. J. F. Kidd being Chapter 4 of "Fundamental Rights" (Sweet & Maxwell 1973).

(5) "Debt Collection Harassment in Australia Part I" by B. Kercher (1978) 5 Monash Uni. L.R. 87.

(6) "The Law of Privacy: The Canadian Experience" by Burns (1976) 54 Can. B.R. 1.

(7) "Privacy and the Right of Access" by O'Brien 30 Adm. L.R. 45 (especially pages 62-79).

The above commentators trace in detail the development of a law of privacy (whether statutory or at common law) in other jurisdictions. American, Canadian and English attempts in particular are traced, analysed and criticized. These latest studies may help to identify the difficulties which lie in the path of the drafting of "tort of privacy" legislation.

In consumer areas there is legislation which in some senses touches the boundaries of this problem—see in particular the enactment of the Commercial and Private Agents Act, 1972-1978; the Fair Credit Reports Act, 1974-1975; the Listening Devices Act, 1972-1974; the Unordered Goods and Services Act, 1972; the Door to Door Sales Act, 1972 and the Ombudsman Act, 1972.

Data Protection

This report of the Committee concerns itself principally with the more limited, yet crucially important, aspect of data protection—by which we mean the protection of a person's privacy from unwarranted invasion as

the result of misuse or abuse of information respecting that person, which is collected, stored or retrieved in an information system in which a computer (or other data bank) is normally involved. In our earlier report we used as a basis for proposed legislation the English bill of 1969 entitled the "Data Surveillance Bill". That was introduced into the English Parliament as a private member's bill but failed to become law. Since then there have been developments in legal thinking as a result of the Report of the Younger Committee on Privacy (1972); the White Paper and its supplement on "Computers and Privacy" (1975); the English Law Commission Working Paper No. 58 on Breach of Confidence (1974) and finally the Lindop Committee Report on Data Protection (1978).

In the light of these developments, we feel obliged to state that the fears we had at the time of compiling our 1973 Report have been realized. The 1969 Bill on which we based our recommendations would have proved inadequate and would in all probability have become very quickly out of date in view of the enormous developments in computer technology in the past decade.

Our present recommendations on data protection flow from a considered appraisal of the English position, with particular reference to the Lindop Committee report.[2] This report is free from the technical dissertation and the complexity which have so often characterized such endeavours.

The Lindop Committee was able to draw upon the combined experience of Data Protection laws recently passed in Europe (e.g. Sweden, Norway and West Germany) and in North America (Canada and the United States of America).[3]

The English Model (The Lindop Proposals)

The broad outline of the proposed English Data Protection Act is contained in sixty-eight basic recommendations.[4] We shall outline, in a very general way, the scheme proposed:

(a) that the legislation apply to the "handling"—which term is very broadly defined—of "personal data" by "users", where a computer is wholly or partly involved in such process.

The term "computer" is nowhere defined because the Committee saw difficulties in a limiting approach. They say:

> "New techniques for handling data (e.g. Full Text Retrieval and Word Processing Systems) can pose new risks, for which established data protection measures may prove inappropriate or inadequate. Accordingly, the legislation, if it is not to become swiftly obsolescent, must enable the rules governing the handling of personal data to evolve over time."[5]

"Handling" in this report is a word of wide import which in addition to its normal usage, may also cover the translation or interpretation of data. It will cover some manual data handling as well as electronic or automatic data handling.

(b) That there be established an independent statutory body, to be called the Data Protection Authority (D.P.A.). Its duties are to oversee data users and accuracy, and to administer the act. It shall be bound to act according to seven principles[6] which reflect the interests of the users of data, the individuals who are the subjects of the data and the community at large.

(c) That the D.P.A. shall have the power to negotiate, prescribe and enforce sets of rules, to be called "Codes of Practice", which shall respectively apply to relevant, defined classes of data use. Thus, for example, one code of practice may be applicable to the data held on individuals and used by medical authorities (hospitals, clinics, etc.); another by police and security services; another by local and central government and so on. The Committee tentatively describes some thirty-seven possible classes for codes of practice.[7] Such codes of practice should bind the Authority, the Consumer Affairs Commission and the Public Service generally.

(d) That data users shall be registered with the D.P.A. A licence procedure is considered to be cumbersone and inappropriate.[8]

(e) That each code of practice shall have the force of law, after having been promulgated in the form of subordinate legislation and following the usual Parliamentary scrutiny for subordinate legislation. Breach of a code by a user may expose him to criminal sanctions as well as to a new civil remedy in favour of data subjects.

Each code will therefore differ from any other code in all or some of the following respects *(inter alia)*:

(i) the method of collection of data and the purpose of its collection;

(ii) the type of data which may be lawfully collected;

(iii) the use to which the data may be put and who may lawfully make use of it;

(iv) the method of transmission of the data;

(v) the right of access of the data subject to the data, and methods of correction or erasure of inaccurate, irrelevant or incomplete data;

(vi) the method of disclosure of data by users to subjects; destruction or erasure of obsolete data or data which is no longer required.

(f) That the D.P.A. have investigatory powers and powers to recommend that action be taken in appropriate cases. We think that prosecutorial and enforcement powers should not be vested in the investigatory body, but should be separate and vested in a body specially charged with that duty. The tribunal to hear any matter arising under this Report should be constituted by a Local Court Judge and two assessors, one appointed to represent the interests of the consumer and the other that of the department or other collector of data. Deregistration of a user could be the ultimate sanction. Generally the overriding interest that the D.P.A. should consider and protect is that of the individual from whom data has been collected. The essence of the legislation is that data information should only be used for the purposes for which it was collected or for a use consented to by the data subject; breach of these fundamental tenets is to be investigated or remedied by the D.P.A., either alone or concurrently with action taken by the data subject himself.

(g) That the D.P.A. should be fully accountable to the Legislature and its activities should in South Australian terms come within the purview of the Ombudsman.

(h) That the legislation should bind the Crown and its instrumentalities (of which the D.P.A. is itself *not* one—see the Lindop recommendation 30.40). The case of police and of security services would require a different type of code of practice ensuring that the interests of criminal and defence surveillance are accorded priority in the public interest.

(i) That the impact of the legislation on such other and diverse areas as medical, sociological, statistical and archival research (where risks of personal identification are minimized) the laws of defamation, privilege, survival of causes of action and breach of confidence be properly recognized and kept under scrutiny. In this context, the D.P.A. ought to have the power to recommend to you legislative reform to ensure an overall harmony of approach of statute and common law.[9] If such recommendations are made, you may feel it appropriate to refer them to this Committee for further appraisal of the situation as it then presents itself.

(j) That the accountability of the D.P.A. to Parliament and the investigatory powers of the Ombudsman exist and be used respectively, without unduly compromising the need for the independence of the D.P.A.[10]

(k) That the question of exemptions from a given code can only be worked out in relation to that code when it comes to be promulgated.

There is an admirable simplicity in this proposed legislative scheme which gives free scope for flexibility and the unforeseen developments of the future.

The American Model

Under the U.S. Privacy Act 1974 that country proceeded to regulate data use without establishing anything like a D.P.A.[11] One of the latest American States to legislate in this area is Minnesota (the Minnesota Data Privacy Act 1976) which adopts the U.S. Federal approach. The shortcomings of this technique, which relies upon vesting rights in individuals and upon the courts to assure exercise of those rights, are subjected to criticism by *Mitau*.[12]

The State legislation did not go far enough to protect expectations of data privacy and a Legislative Privacy Study Commission set up in 1975 explored areas of weakness and suggested reforms. Among critical points to emerge (and these could validly be applied also to the U.S. federal law) were the following:

(i) a lack of specific statutory guidelines for data collection led to the collection of too much, and also unnecessary or irrelevant information, by government agencies.

(ii) there was a lack of uniform criteria as to what constituted necessity of collection of information; and

(iii) there was a failure to analyze properly the costs and benefits to society at large.

To overcome problems of lack of clarity of definition, Mitau proposed that a "privacy impact statement" accompany all new legislative and

administrative programmes, which would require evaluation of such programmes in the light of the following considerations:

(i) quantitative intrusiveness;

(ii) qualitative intrusiveness;

(iii) collection techniques;

(iv) expected use and dissemination;

(v) anticipated length of retention of data; and

(vi) the designation of officials to be the "responsible" authority for data collection, use and dissemination.

A further difficulty is the classification of material which governs disclosure of data both to third parties and the data subject himself. We feel that the inadequacies of American legislation are convincingly avoided by the "Codes of Practice" technique, which, for want of a better description, can be seen as an individualized treatment of the subject matter. The proposed Codes will avoid the American difficulties if they are sufficiently tailored to suit the many and various information systems which exist or will come into being (i.e. they will have sufficient particularity and detail on all relevant matters in each case such as collection, use dissemination, retention, subject access, responsible authority, etc) whilst preserving the necessary flexibility for different systems at the same time, or the same system at different times.

Problems associated with the clarity of definition of principles guiding divergent systems should be reduced to a minimum.

Another illustration will show how advanced the Lindop approach is. Mitau proposes the following for Minnesota's consideration:

> "To avoid privacy problems caused by the currently available [public judicial] review procedure under the Administrative Procedure Act, provision should be made for an *in camera* examination citizen and the responsible authority in the dispute."[13]

The Lindop Committee makes more flexible recommendations.[14] The American Model is gradually groping its way from a purely private enforcement oriented model to that more nearly approaching a regulatory, publicly accountable model—(see *Mitau* page 673 and compare Lindop paragraphs 4.31-4.32).

South Australia

If legislation, along the lines proposed by the Lindop Committee, were contemplated for this State, the following matters ought to be borne in mind:

(1) Should groups, societies, firms, associations or corporations be included within the definition of "data subject", alongside of the English recommendation of "individuals"? We think they should be.

The English conclusion was that company law, patent law, copyright law or the law of confidential information in relation to trade secrets should adequately deal with non-individual data subjects.[15] We think that there are many matters outside these areas where a corporate body is in the same situation as an individual with regard to data. We feel that the situation ought to be declared equivocally. It is, for example, arguable that the protection provided by the Fair Credit Reports Act, 1974-1975, does extend to bodies corporate etc. The reason is that the Act applies to "credit information" which is defined as "information in relation to

the creditworthiness of any person". (Section 4). "Person" is not defined. However Section 4 of the Acts Interpretation Act, 1915-1975, states that, unless a contrary intention is shown in an Act, "person" includes a body corporate. In *Mobitel International Pty. Ltd. v. Dun & Bradstreet* our Full Court overruled the argument that the protection provided by the Act did not extend to bodies corporate.[15A] Doubts in this regard ought to be conclusively dispelled.

(2) Will there be a continuing need for the operation of the Fair Credit Reports Act, 1974-1975?[16] We think there will be, and the legislation proposed by this report and that existing in the Fair Credit Reports Act will have to be integrated.

(3) What impact ought the legislation to have on Court records, especially of judgment debtors, i.e. are the Courts to be regarded as data collectors and data users? We think that, subject to any orders actually given by a Court, they should be.

(4) What will be the legitimate scope or area of operation of the State Act, bearing in mind the implications of the Commonwealth Constitution, e.g. will the South Australian Act be competent to regulate data handling by a Commonwealth department or instrumentality? Can it cover data collection or use in the course of interstate trade and commerce? We think the answer to both these questions is in the negative. Perhaps one possible solution to avoid doubt or confusion could be that the Act contain a schedule setting out all the bodies, instrumentalities and agencies, whether in the private or the public sector, which come within the purview of the D.P.A. Additions to or deletions from such schedule could be achieved by a proclamation by His Excellency the Governor in Council notified in the *South Australian Government Gazette.*

(5) Whether or not there is a need to confine the legislation to "automatic" data handling or whether it should be extended wholly, or partly, to manual data applications as well? As appears elsewhere in this report, we think it should be so extended.

(6) Whether or not the data user ought to be obliged by law to furnish the data subject with a notice each time the personal data is in anyway utilised. The notice would need to specify what data was given, to whom, when and for what purpose. We do not think this is necessary but raise the problem for your consideration.

(7) Whether or not amendments would need to be made to the Consumer Credit Act 1972, the Ombudsman Act 1972-1974 and the Companies Act 1962 to deal with the position of the new State D.P.A. We think they would.

(8) A section similar to Section 14 of the Fair Credit Reports Act 1974-1975, dealing with the criminal responsibility of persons for the acts of a body corporate which is a data user, would need to be framed.

(9) The Lindop Committee's main thrust is succinctly phrased at page 164 of the Report:

> "Risks to privacy arise from what is done with personal data rather than from how it is done and so

Codes of Practice could be written to be applicable to all personal data handling activities of a particular class—i.e. those performing the same function for the same purpose—without regard to the particular configuration of computing machinery or softwares employed, or indeed to the extent to which computers are used."

By adopting this line of approach we see no compelling need for including within the proposed legislation a definition of "privacy"—a concept notoriously fraught with legal and philosophical difficulties.[17] It should not be necessary to define "computer" either on this approach.

To carry out its duties effectively the D.P.A. needs to be able to impose legal sanctions where necessary. The legal sanctions it can bring to bear are important.[18] We suggest consideration of the following legal sanctions:—

(i) a power to deregister or suspend a data user's operations;

(ii) a power to bring prosecutions against defaulting users for breaches of the Act and the relevant Codes. In this case it may be necessary, in the case of a company, to consider whether the directors as well as the company should not be liable to prosecution in a proper case.

(iii) a power to seek an injunction from a Court against a repeated user-offender, and order correction of data;

(iv) a power to require an apology to be given and published;

(v) a power to make a declaration of untruth or inaccuracy of data;

(vi) a power to order an explanatory or exculpatory note to be added to the data.

(10) A jurisdictional clause (e.g. whether in a court of summary jurisdiction, Local Court or the Supreme Court) will need to be included.

(11) In addition, a clause will be required indicating that no right or remedy at law or in equity should be in any way affected, abridged or diminished as a result of the Act's workings. It is essential that the few rights and remedies currently possessed (in the absence of enactment of a comprehensive privacy law) be preserved intact.

(12) We would go further. A data user should, in a proper case, be entitled to an injunction, a right to have the record corrected and an explanation, if necessary settled by the Court, sent to those to whom the wrong information was communicated.

(13) On the topics of death and liquidation,[19] we wish to make two comments:—

(i) The Lindop Committee saw fit to recommend (para. 36.04) that "the data user's obligations . . . remain in force when the data subject had died. Any right of action which had already accrued to the data subject before his death should survive for the benefit of his estate."

This should include a right to general damages in addition to special damages, but not to exemplary or aggravated damages.[20]

(ii) In paragraph 36.04 it is recommended that individual codes of practice should govern the right of access to information about a data subject who is dead or the use to which data about the deceased could be put, i.e. whether it may be used for a purpose other than that for which it was collected. This may require a general code of practice of an archival nature.[21]

If an historian or biographer obtains data on his subject and his use of it in publication varied from or conflicted with the code of practice binding on a data user, it may be that the data user and the third party recipient (historian, biographer) of the information should be liable for such use to the estate of the data subject who is deceased, but this is basically a question of policy.

The Lindop Committee's recommendation in this context appears to conflict with its earlier statement that:

> "[We] see no reason why the presence or absence of computers should make any difference to the legal rights and obligations of the parties who handle such information or are affected by it, whether under the law of defamation or any other branch of the law".[22]

We feel that the law on defamation of the dead ought to be maintained and that no Code of Practice ought to be allowed to interfere with or modify it in any way. As is said by Professor Fleming:—

> "To allow redress at the suit of his [the dead data's subject's] personal representatives or relatives and friends would seriously curb the freedom of biographers and historians and is, therefore, also socially undesirable."[23]

(13) There is one conceptual difficulty arising out of the Lindop Scheme. The problem is that data users become, perforce of the D.P.A.'s activities, themselves data subjects. Should not the D.P.A. itself be bound by a code of practice—perhaps the first Code to be enacted? The recommendations allow for D.P.A. accountability to Parliament and for the activities of the Ombudsman (see paras. 19.62, 19.87 and 20.61-64). To give added teeth to this accountability a code binding the D.P.A. ought to be implemented. The D.P.A. could itself become a "data user" of no small proportion. The recommendations do not exclude the D.P.A. from the proposed definition of "user" (18.08-10).

The D.P.A.'s legal independence should be conferred and assured by recommending that it be declared not to be a servant or agent of the Crown or to enjoy any status immunity or privilege of the Crown. The Answer to the question "Who watches the watchdog?" could be given practical "teeth" by the Code binding the D.P.A. Independence and accountability should not be seen as mutually exclusive or antagonistic notions—merely as correlatives with important practical ramifications. The individual "data subject", whose personal data the D.P.A.

itself handles, should have direct redress for the authority's non-feasance or misfeasance. Parliamentary and Ombudsman surveillance are good in theory, but actual daily practice will provide the test for proper performance.

(14) We believe that the Lindop proposals more than adequately satisfy the four criteria set out in Appendix E to the 1970 Justice Report.[24]

In conclusion, we would respectfully adopt *mutatis mutandis* the rest of the Lindop Report. The principal dangers to privacy arise from inaccurate, incomplete or irrelevant information, the possibility of access to information by people who should not or need not have it, and the use of information in a context or for a purpose other than that for which it was collected. The Honourable Haddon Storey Q.C., Attorney-General for Victoria, has said, and we agree with him:—

> "People have come to demand a preservation and in some cases restoration of the balance between the rights of the individual and the interests of the community, and they have looked to the law to supply this balance."[25]

We feel that the Lindop proposals, subject to our own recommendations contained in this Report, should ensure adequate protection and respect for privacy in this sensitive area.

We realize that this report breaks new ground. If it were not for the existence of the Lindop Report we would have held public hearings on the matter and will of course still do so if you desire.

We have the honour to be

HOWARD ZELLING.
J. M. WHITE.
CHRISTOPHER J. LEGOE.
D. W. BOLLEN.
M. F. GRAY.
JOHN KEELER.
D. F. WICKS.

The Law Reform Committee of South Australia

1st February, 1980.

Bibliography

1. See report in 48 A.L.J. 457-458.
2. "Report of the Committee on Data Protection" Command 7341.
3. ibid. : Appendix 10 : a helpful, tabular analysis of the existing or proposed legislation, its general impact and specific items of interest therein.
4. ibid. : Chapter 38.
5. ibid. : p. xix.
6. See paragraph 21.09.
7. See Appendix 9.
8. Paras. 19.39-19.42.
9. See Part V *passim* (Chapters 30-37).
10. Paras. 20.30-20.79.
11. Paras. 4.28-4.32.
12. *Mitau:* "Toward a Comprehensive Fair Information Standards Law" 62 Minn. L.R. 649 (1978).
13. ibid. : p. 675.
14. *Lindop* paras. 19.101-19.103.
15. ibid. : paras. 18.41-42.

15A. (1977) 17 S.A.S.R. 140.

16. See the engaging and helpful discussion in the similar, but by no means identical, English context at paras. 13.10-13.24.
17. See especially discussion on the semantics of privacy by *Burns, O'Brien* and *Benn* 52 A.L.J. 601, 686—"The Protection and Limitation of Privacy"—a detailed philosophical and linguistic analysis of privacy concepts. Note his comment at page 687:

    "The diversity of the interests claiming protection from a newly-proclaimed right to privacy, and the complex impact of such a right on existing interests, make it virtually impossible to legislate comprehensively and in detail for all the many different types of conflict."

    And reference is made to the 1973 Report by Professor W. L. Morison ("Report on the Law of Privacy") where he:

    "cautiously recommended to the Australian States that they adopt the device of a standing exploratory committee that would negotiate settlements of particular grievances, make recommendations piecemeal for quite specific legislation as experience recommends while encouraging the growth of voluntary professional codes."

    And see *Lindop* para. 21.29.
18. See paras. 19.89-19.95.
19. ibid. : Chapter 36.
20. See our previous 1973 recommendations Nos. 6 (2) and 7 in the context of a "tort" of privacy.
21. See *Fleming* "Law of Torts" 4th ed. (1971) pp. 470-471.
22. *Lindop* para. 32.14.
24. On the problem of a general right of privacy see the Australian Law Reform Commission Discussion Paper No. 3, where a right of action for breach or invasion of a limited, qualified privacy was drafted in a proposed Act (The Defamation Act 1978); Part III of which (clauses 20 to 26) conferred a limited right of action for the publication of private facts of a person or the appropriation of his name, identity or likeness for the defendant's own benefit or to the detriment of the plaintiff. The defences to this action are eight in number (see clause 24).
25. See 47 A.L.J. 498 at page 515.

D. J. WOOLMAN, GOVERNMENT PRINTER, SOUTH AUSTRALIA 200—7.80 A2067 O