

Other Privacy Protections (DP12)
Submissions on Discussion Paper No 12

R1	The Finance Sector Union
R2	Dr JN Mein
R3	NZ Employers Federation Inc
R4	Rae West, Royal NZ College of General Practitioners
R5	NZ Association of Social Workers Aotearoa
R6	Wellington City Council
R7	Inland Revenue Department
R8	Baynet CRA Ltd
R9	Sarah Kerkin
R10	NZ Video Dealers Association Inc
R11	Commonwealth Press Union
R12	Auckland District Council of Social Service
R13	Telecom NZ Ltd

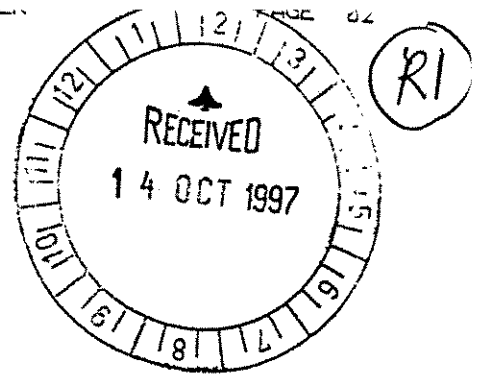
Cross references to submissions held on other series

S7	Healthcare Otago Ltd
S24	NZ Defence Force
S36	Nurse Maude Association
S39	Te Puni Kokiri
S40	NZ Bankers' Association
S42	Rosamund Averton
S45	Family Planning Association NZ
S46	New Zealand Medical Association
S52	Tranz Rail
S55	NZ Council for Civil Liberties
S56	Association of Market Research Organisations
UV16	Health and Disability Commissioner

REVIEW OF THE PRIVACY ACT 1993
DISCUSSION PAPER No. 12
NEW PRIVACY PROTECTIONS

- Q1. If new principles are to be considered for inclusion what qualities should they possess?
- Q2. Is a new principle, not linked to collection, desirable in respect of openness regarding agency information practices?
- Q3. Would a principle to allow individuals the option of anonymity when entering transactions be desirable? What exceptions might be appropriate?
- Q4. Should there be a principle concerning reasons for decisions when an agency makes a decision or recommendation in respect of an individual in his or her personal capacity? Would that sit comfortably with the private sector?
- Q5. Are any new principles or provisions desirable based upon the Australian Privacy Charter?
- Q6. Are any new principles or provisions desirable based upon the proposed Canadian Charter of privacy rights?
- Q7. Is there value in developing within the statutory framework a set of broad privacy principles, going beyond the existing emphasis upon information privacy and data protection issues, as a guide to the Privacy Commissioner in the exercise of his functions?
- Q8. If a set of broad privacy principles, going beyond data protection issues, were to be developed, would it be appropriate to require agencies to have regard to them?
- Q9. Should the Privacy Act include controls on the transfer of personal information to jurisdictions which do not apply a standard of protection comparable to those in the OECD guidelines? What factors should most influence the Privacy Commissioner in making any such recommendation? What issues should any recommended scheme particularly take account of?
- Q10. If a transborder data flow control is warranted, should it empower the Commissioner to take prohibition action in exceptional cases? Or should any provision place the responsibility on agencies which are contemplating transferring personal information out of the jurisdiction?
- Q11. What test should any transborder data flow control apply? Should a distinction be made between OECD countries "substantially observing" the OECD guidelines and other countries which might be expected to have, say, "equivalent protection"? Is a listing system to distinguish jurisdictions desirable?
- Q12. What are the positive reasons to impose controls on the handling of sensitive categories of personal information?

- Q13. What are the negative features of special controls on sensitive categories of information? Do the positive features outweigh the negative of having such controls?
- Q14. If controls on sensitive categories of personal information were to be introduced, should the Act specify the categories of information or should a process be established for these to be determined later?
- Q15. If the Act were to list sensitive categories of data, what categories should be listed?
- Q16. How best might a regime controlling sensitive categories of data best be implemented? Would the best approach involve a new part of the Act, the creation of regulation making powers, or an amendment to the powers to make codes of practice?



14 October 1997

Privacy Act Review 1997
Office of the Privacy Commissioner
P.O.Box 466
AUCKLAND

Email privacy@iprolink.co.nz

Dear Sir / Madam



Please find attached FinSec's submissions.

Should you have any queries, feel free to contact the writer.

Yours faithfully

Andrew Casidy
Senior Industrial Officer

FinSec (The Finance Sector Union) Submissions on the Review of the Privacy Act 1993

FinSec, the Finance Sector Union represents approximately 15,000 members working primarily in the New Zealand banking and insurance industries.

Discussion Paper 12

Question 3 - It is FinSec's submission that whilst there ought to be an entitlement for the individual to enter into a transaction with anonymity, it may not be in the finance sector. Financial transactions, by their very nature, must create trails which are traceable and the rapid movement to electronic transactions makes this easier. A financial institution's need to identify their customer and trace their customer's transactions is fundamental to the security of any banking or transaction system. Clearly then, whilst such a principle might be desirable, transactions in the finance sector would have to be excluded.

There are a number of areas where exclusions would also have to occur, such as:

- access to transaction information in criminal prosecution situations;
- where an employer in the finance sector suspects staff fraud;
- the Financial Transactions Reporting Act 1996.

It is our submission, therefore, that a broad principle requiring anonymity when entering transactions is desirable but this would need a qualification of "where reasonably justified" or "when appropriate".

Question 4 - It is FinSec's submission that reasons for decisions or recommendations regarding an individual should be provided upon request. Again, it is inequitable for the public and private sectors to have different requirements and the individual's need to know will be no different whether they make the request of a public or private sector agency. As this relates to employment matters. We believe such a provision would be best contained within the Employment Contracts Act.

Questions 5 & 6 - It is FinSec's submission that it is desirable to expand the privacy principles beyond those of straight data protection. Some of the concepts discussed in the Australian and Canadian models have implications in the finance sector workplace which need to be considered specifically:

Freedom from Surveillance - It is FinSec's submission that such a principle is desirable. A number of scenarios occur in our industry. For example, employers have used closed circuit television footage, ostensibly gathered for security purposes, for disciplinary purposes. It is our submission that this is unjust and a good example of why such a principle is desirable.

We have difficulty with the issue of 'Mystery Shoppers'. Our concern is with its clandestine nature and the fact that individuals are sometimes identified in the subsequent reports. This is unacceptable given that the purpose behind mystery shopping is to assess a work-sites customer service levels, not those of an individual.

The difficulty with surveillance is that the temptation to use it for unacceptable purposes is too great. The solution therefore, is to guarantee individuals freedom from such activity.

The reason for such a principle is, we submit, a simple extension of the Acts current requirement that information should be used in accordance with the purpose for which it is collected.

In our industry there is one significant area where an exception to this principle is vital. Nearly all banking institutions in this country now routinely use closed circuit television as a security device. It is one of the fundamental tools used in our industry to protect staff's and customers' physical well being. We submit that whilst a freedom-from-surveillance principle is desirable for both staff and customers alike it must not be allowed to limit the use of surveillance as a security device.

Physical Privacy - It is our submission that such a principle is desirable. There are two issues:

Drug Testing

Employers and their representatives have been pressing for **compulsory** drug testing in the work place. It must be accepted that the right to **require** a 'sample' is an infringement of a person's rights. We submit that in the employment context, the right of the individual must be of greater importance than that of the employer. An employer who has genuine concerns about their employee's fitness to perform their functions may already instruct an employee not to work. We submit that there needs to be a very high level of justification for any breach of this principle and we see it as being limited to areas involving the appropriate legal authorities.

471871337 13.37 03 3022000

Psychological Testing

This is occurring more frequently in our industry despite little evidence of its usefulness. Our concern is that this is an invasion of a person's privacy and that there is nothing voluntary about it - employees has no choice but to submit if they want the job or the promotion. Failure to consent rules the employee out of the selection process. In our view this is blatantly unfair.

Questions 9, 10 & 11 - The issue of trans-border data flows is likely to become increasingly important in our industry. With most of our employers being foreign owned there is scope for centralisation. Such things as information processing, transaction processing, information and technology systems, marketing analysis, and human resource functions etc. can be based off-shore and this would require data transmission and storage overseas. Consequently, there is a potential need for protection of this information outside New Zealand. It is our submission that such a principle is desirable and necessary. We believe the most effective principle would permit such trans-border flows only to those countries which are observing privacy protection guidelines similar to or better than our own.

(R2)

DP7

- Q2 Yes. The same sort of evidence the police present when applying for a search warrant.
- Q3 It seems a good safeguard.
- Q4 The frequency of matching should be restricted.
- Q5 All such programmes should be under control.
- Q6 Yes.

DP12

- Q3 Yes. The example given seems appropriate.
- Q4 I do not feel that an employer needs to give a reason for choosing one candidate over another when both have similar qualifications.
- Q5 Perhaps it would be better to stipulate when privacy may be invaded, as outlined in the next section.
- Q6 Doctor's notes are a memory aid for the doctor, and although they contain information about the patient, they primarily record what the doctor thought and did. How much of this needs to be revealed to the patient should be at the doctor's discretion.
- Q7 This seems a good idea.
- Q8 Yes, otherwise why have them.
- Q9 Yes.
- Q10 Yes to both. They do not seem to be exclusive.

End of submissions.
J.N.Mein

Dr

[Redacted signature area]



DISCUSSION PAPER No. 12
 NEW PRIVACY PROTECTIONS

Q.1 If new principles are to be considered for inclusion what qualities should they possess?

The Federation does not support the extension of the Privacy Act. However, were new principles to be included in the Act they would need to be transparent, capable of being clearly understood, impose no or minimal cost and be capable of enforcement.

Q.2 Is a new principle, not linked to collection, desirable in respect of openness regarding agency information practices?

No. Privacy principles 1, 2 and 3 effectively require openness as compared with the Australian provision cited which may sound fine but which gives no indication of how openness is to be achieved.

Q.3 Would a principle to allow individuals the option of anonymity when entering transactions be desirable?

As the discussion points out, the option of anonymity currently exists - with cash transactions and the like. However, by their nature, many, if not all, current electronic transactions require identification and it is not entirely clear how this fact can be overcome. The incorporation, in the US and Australian examples, of the words "where appropriate", and in the Canadian example of the words "reasonably justified", highlights the problem. It would remain to be seen whether an anonymity principle could operate in practice.

Q.4 Should there be a principle concerning reasons for decisions when an agency makes a decision or recommendation in respect of an individual in his or her personal capacity? Would that sit comfortably with the private sector?

From the point of view of the private sector, the incorporation of such a provision is unnecessary since employees can already seek reasons for dismissal, or for an action to an employee's disadvantage, under the Employment Contracts Act. And, the Human Rights Act is available where there has been a failure to employ or to promote. There would also be likely problems associated with the right to withhold the evaluative material which may well have influenced a particular employment or promotion decision.

Q.5 Are any new principles or provisions desirable based upon the Australian Privacy Charter?

The Australian principles are characterised by a degree of vagueness which limits their usefulness. The "private space" provision is a case in point. In many workplaces it will be impossible to provide genuinely private space in

which to conduct personal affairs (query whether, in any event, the workplace should be the place where private business is conducted). Would the stated qualification, "to varying degrees", cover such a situation? Similarly, freedom from surveillance will not always be possible when security needs make surveillance in otherwise public places essential (in shops, banks, and so on). The Australian principles would only further complicate an already complex legislative intervention.

Q.6 Are any new principles or provisions desirable based upon the proposed Canadian Charter of Rights?

No. The Canadian Charter is full of inherent contradictions (recognised to some extent by the presence of a "justification for exceptions" provision) and poses more problems than it solves. How, for example, does the assertion "Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable" relate to New Zealand provisions which, in some circumstances, permit the withholding of certain personal information? The litigation-generating potential is huge. And "The duty not to disadvantage people because they elect to exercise their rights to privacy" is also fraught with problems. Does this mean, among other things, that failure to disclose, in writing to a prospective employer, a pre-existing gradual process injury, could not be penalised in the way section 7(6) of the Accident Rehabilitation and Compensation Act 1992 envisages? That is just one instance where giving precedence to privacy legislation would make a reasonable legislative provision unworkable. However, good the intentions, such a Charter would essentially be invalidated by the number of exceptions needed to make it workable.

Q.7 Is there value in developing within the statutory framework a set of broad privacy principles, going beyond the existing emphasis upon information privacy and data protection issues, as a guide to the Privacy Commissioner in the exercise of his functions?

It is always hazardous to import principles from overseas legislation into domestic legislation given the likelihood of unforeseen consequences. The Privacy Act already contains references of this kind and the inclusion of the somewhat amorphous references found in the Australian Charter would only further serve to complicate matters.

Q.8 If a set of broad data principles, going beyond data protection issues, were to be developed, would it be appropriate to require agencies to have regard to them?

No. In an area such as privacy, legislative impositions on agencies should be limited to what it is possible, in practical terms, to achieve. "Principles" will always be open to the uncertainty of interpretation, which will impose its own costs. They will inevitably be undermined by the need for exceptions. That need will not always be obvious in advance but may well become apparent only as a consequence of costly litigation. Where the difficulties of compliance are

too great, the response of legislative avoidance will serve only to bring the legislation itself into disrepute.

- Q.9** Should the Privacy Act include controls on the transfer of personal information to jurisdictions which do not apply a standard of protection comparable to those in OECD guidelines?
- Q.10** If a transborder data flow control is warranted, should it empower the Commissioner to take prohibition action in exceptional cases? Or should any provision place the responsibility on agencies which are contemplating transferring personal information out of the jurisdiction?

The further questions which need to be asked in this context are, what is the purpose of imposing transborder data controls and can they be effectively enforced? Given that the possibility of effective enforcement is questionable - leading to controls more honoured in the breach than the observance - it is likely that their real purpose is to act as a quasi tariff barrier. This is not an appropriate reason for imposing controls of this kind.

If transborder controls are to be imposed, responsibility for transfer (or not) should rest with the agencies concerned.

- Q.11** What test should any transborder data flow control apply? Should a distinction be made between OECD countries "substantially observing" the OECD guidelines and other countries which might be expected to have, say, "equivalent protection"? Is a listing system to distinguish jurisdictions desirable?

The attempt to compare the legislation of different countries is always fraught with difficulty, the more so in that the existence of legislation is no necessary guarantee of legislative compliance. Since this will always be the case, it is likely to make little difference from a control point of view which test is applied. However, an "equivalent protection" test would accommodate a wider variety of approaches than would requiring "substantial observance" of OECD guidelines.

- Q.12** What are the positive reasons to impose controls on the handling of sensitive categories of personal information?
- Q.13** What are the negative features of special controls on sensitive categories of personal information? Do the positive features outweigh the negative of having such controls?

It is difficult to see what the inclusion of a sensitive categories regime would do that the Human Rights Act does not do already. While it is true that the Human Rights Act provides a remedy only after the event, the fact of its existence means that in an employment situation, sensitive information about race or religion, for example (the two "sensitive" categories cited in the discussion paper) can only be sought with the consent of the individual concerned. Paradoxically, however, this kind of information is often important for equal employment opportunities (EEO) purposes (the antithesis of the European fear). A privacy prohibition would have its own adverse effects in

the EEO area, making it far more difficult for employers to measure the progress of EEO policies and programmes and so to provide evidence of progress in this important area.

- Q.14** If controls on sensitive categories of personal information were to be introduced, should the Act specify the categories of information or should a process be established for these to be determined later?
- Q.15** If the Act were to list sensitive categories of data, what categories should be listed?

There are (as above) already sufficient protections in New Zealand law. Moreover, there will always be some categories to which exceptions must apply in certain circumstances (political opinion, health - particularly in relation to health and safety in employment requirements, where the health of others could be endangered, or certain provisions of the ARCI Act). There is also the previous conviction category, where in respect to certain jobs, the nature of a previous conviction may be relevant (such as a fraud conviction to work in the financial sector). There is little to be gained from introducing sensitive categories of data of which, in practical terms, will be more likely to hinder than enhance employment opportunities.

- Q.16** How best might a regime controlling sensitive categories of data best be implemented?

The implementation of such a regime is not supported

Q 2 Yes, based on Australian "Openness".

Q 3 Yes, on Canadian model.

Exceptions depend on applicable laws eg driving and drinking age and credit, all in accepted situations.

Q 4 Arguable.

Q 5 Surveillance and Communications deserve public discussion.

Q 6 I am not convinced of the necessity for such loose definitions.

Q 7 Yes

Q 8 Should be in public education and ethics rather than enforceable law.

Q 9 Worth discussion.

Individual harm; Commercial or financial disadvantage; others as in Official Information law.

Q I0 Responsibility on agencies but with controls available (though I'm not sure that process works in eg aviation safety).

Q I2 & I3 Controls by legislation should be avoided if possible.

Q I4 Third option, as a process.

Q I6 Codes of practice developed within organisations are more likely to be observed by peer pressure.



NEW ZEALAND R5
ASSOCIATION OF SOCIAL WORKERS
AOTEAROA

- 7 NOV 1997

P O Box 9298
Te Aro
WELLINGTON

23 October 1997

Blair Stewart
Manager, Codes and Legislation
Privacy Commissioner
P.O. Box 466
AUCKLAND

Dear Mr. Stewart

**Submission : Review of Privacy Act 1993
Discussion Papers**

Thank you for the opportunity to comment on the above matter. Unfortunately we only have the last five papers distributed. Thus, given the short timeframe, I can only comment on discussion papers 5, 6, 7, 9 and 12.

On behalf of the New Zealand Association of Social Workers, I will make every endeavour to attend the consultation meeting in Christchurch on 19th November 1997. Please send me the details of this meeting when they are available.

Yours sincerely,

Lynne Briggs
NZASW Ethics Convenor

National Office
GAYLENE LAWRENCE
Administration Officer
P.O. Box 9298
Te Aro
Wellington
3rd Floor
39-41 Ghuznee Street
Wellington
Tel. (04) 384 7761
Fax. (04) 384 7761
NZ STD - 64

President
DAVID McNABB
P.O. Box 4233
Hamilton East
Tel. (07) 856 7351 Pvt
(07) 856 7351 Bus
Fax. (07) 856 7351
Mob (025) 585 232
Email elganabb@wave.co.nz

Vice President
TUROA HARONGA
Specialist Maori Mental Health
P.O. Box 2056
Palmerston North
Tel. (06) 323 6843 Pvt
(06) 350 8373 Bus
Fax. (06) 350 8374

Secretary
JUSTINE KINGI
P.O. Box 4233
Hamilton East
Tel. (07) 843 8984 Pvt
(09) 418 1951 Pvt
(07) 834 8800 Bus
Ext. 8974
Fax. (07) 834 8858
Email cejlk@twp.ac.nz

*Ngata Whenua
Representative*
MERLE DAVIS
P.O. Box 4233
Hamilton East
Tel. (07) 847 5708 Pvt
(07) 839 4536 Bus
Fax. (07) 839 4515

Discussion Paper 12.

New Privacy Protections.

- Q1. No comment.
- Q2. Yes - a new principle regarding openness of agency information in relation to personal data is desirable. The precision of the Hong Kong principle is a good guideline.
- Q3. The option of anonymity when entering transactions is desirable except when doing so could result in a breach of criminal law.
- Q4. No comment.
- Q5. The Australian Privacy Charter extends the extent of privacy rights in a desirable way. There would be some exceptions to some of these principles where there were risks of a breach of the criminal law e.g. the need for surveillance cameras in banks.

Physical privacy - this principle suggests restricting psychological measurement to where there is a very high degree of justification. While it is worthwhile to be reminded of the need to be cautious about the use of such methods of investigation, as a diagnostic tool its use can be more routine in some settings perhaps the wording should be 'high degree of justification', rather than 'very high'.

- Q6. The Canadian principles, if not already included in the NZ principles, should be considered, including the duty not to disadvantage people because of their decision to exercise their rights to privacy.
- Q7. Yes, there is value in developing a broad set of privacy principles going beyond the existing emphasis on information privacy and data protection.
- Q8. It would be appropriate to require agencies to have regard to and comply to broader privacy principles.
- Q9. New Privacy controls may be required for New Zealand covering the transfer of personal information to places that do not have a standard of protection comparable to AECD guidelines.
- Q10. The Commission should be able to prohibit transferable data flow if necessary, rather than relying on individual agencies to take responsibility for this.
- Q11. No comment.
- Q12. There should be controls on the handling of sensitive categories of personal information because of the discrimination that may ensue, This measure would have preventative qualities and would add to the effectiveness of the Human Rights Act.
- Q13. The positive features of these special controls definitely outweigh the negative.

- Q14.** Yes, categories of information should be specified beforehand.
- Q15.** The act should specify sensitive categories of personal information - although the list should be open to additions. The EU Directives offer a guideline as to a suitable list.
- Q16.** No comment.

WELLINGTON CITY COUNCIL
SUBMISSION TO THE REVIEW OF THE PRIVACY ACT

DISCUSSION PAPER 12
NEW PRIVACY PROTECTIONS

Question 1. If new principles are to be considered for inclusion what qualities should they possess?

Any new principles should apply to all agencies unless there are clear reasons why they are exempted.

Question 2. Is a new principle, not linked to collection, desirable in respect of openness regarding agency information practices?

Public sector agencies already have a requirement to make the policies, principles, rules or guidelines available under the official information acts. Therefore it would be consistent that private agencies be required to a similar 'openness' requirement. This requirement would only relate to personal information policies and should be able to be applied without prejudicing the commercial activities.

However, increasing the number of Information Privacy Principles will make compliance more complex.

Question 3. Would a principle to allow individuals the option of anonymity when entering transactions be desirable? What exceptions might be appropriate?

While the right to anonymity appeals, we wonder how realistic it is. Putting the emphasis of existing privacy principles on being able to justify the purpose of holding the information and restricting the use and disclosure of it to that purpose could be more effective.

Question 4. Should there be a principle concerning reasons for decisions when an agency makes a decision or recommendation in respect of an individual in his or her personal capacity? Would that sit comfortably with the private sector?

Individual should be able to obtain the reasons for decisions, eg refusal of loans or insurance. This would have to be consistent with the provisions of the evaluative material clauses for reference checks for employment. WCC have already indicated that they recommend insurance companies are exempted from the use of 'evaluative material' as a reason to refuse access to personal information.

Question 5. Are any new principles or provisions desirable based upon the Australian Privacy Charter?

WCC believe that the principles and provisions in the Australian Charter are more extensive than the scope of the current Privacy Act and would be more appropriate in legislation such of the Human Rights Act.

Question 6. Are any new principles or provisions desirable based upon the proposed Canadian Charter of privacy rights?

The duty not to disadvantage an individual if they refused information could be included as part of IPP3 (1)(f) where the consequences of not supplying the information has to be provided.

Question 7. Is there value in developing within the statutory framework a set of broad privacy principles, going beyond the existing emphasis upon information privacy and data protection issues, as a guide to the Privacy Commissioner in the exercise of his functions?

Extending the emphasis of the current act would require a major revision as it specifically concentrates on personal information. Broad privacy principles could be included in the Human Rights Act.

Question 8. If a set of broad privacy principles, going beyond data protection issues, were to be developed, would it be appropriate to require agencies to have regard to them?

Care would need to be taken of the impact on compliance costs for agencies. Any requirement would have to apply to both public and private sector agencies.

Question 9. Should the Privacy Act include controls on the transfer of personal information to jurisdiction which do not apply to a standard of protection comparable to those in the OECD guidelines? What factors should most influence the Privacy Commissioner in making any such recommendation? What issues should any recommended scheme particularly take account of?

Yes there should be controls on the transfer of personal information to other jurisdictions. While those jurisdictions with a comparable standard of protection would be less of a concern, there must be a justified reason for the transfer.

WCC recommends that the information matching rules explicitly apply to international transfers and that there should be rules defined for transferring information outside of New Zealand to be consistent with the information privacy principles.

Question 10. If a transborder data flow control is warranted, should it empower the Commissioner to take prohibition action in exceptional cases? Or should any provision place the responsibility on agencies which are contemplating transferring personal information out of the jurisdiction?

It seems appropriate to have rules similar to the Information Matching Rules to enable protection in exceptional cases. Agencies must take responsibility for compliance but there needs to be a monitoring body.

Question 11. What test should a transborder data flow control apply? Should a distinction be made between OECD countries “substantially observing” the OECD guidelines and other countries which might be expected to have, say, “equivalent protection”? Is a listing system to distinguish jurisdictions desirable?

Use the European Union work as a basis. The list could be a separate schedule or available from the Privacy Commissioner.

Question 12. What are the positive reasons to impose controls on the handling of sensitive categories of personal information?

WCC believe that the current information privacy principles protects sensitive information adequately now if the principles are applied correctly.

Question 13. What are the negative features of special controls on sensitive categories of information? Do the positive features outweigh the negative of having such controls?

Extra compliance and education costs for no added benefits. It also distinguishes between what is general personal information and sensitive personal information. It would be difficult to distinguish adequately as the category may change for information depending on the circumstances.

Question 14. If controls on sensitive categories of personal information were to be introduced, should the Act specify the categories of information or should a process be established for these to be determined later?

WCC does not support separate categories for sensitive information. However, if this was introduced the categories must be established at the time of implementation.

Question 15. If the Act were to list sensitive categories of data, what categories should be listed?

The European Union list seems a sensible one if we introduce a separate category.

Question 16. How best might a regime controlling sensitive categories of data best be implemented? Would the best approach involve a new part of the Act, the creation of regulation making powers, or an amendment to the powers to make codes of practice?

A new part in the act would be the best approach.

National Office
Plaza Chambers
107 Manners Street
PO Box 2198
Wellington
New Zealand

Telephone: (04) 472-1032
Facsimile: (04) 802-6100

10 November 1997

Office of the Privacy Commissioner
P O Box 10-094
WELLINGTON

Dear Sir

You have sort comment on the discussion documents regarding the review of the Privacy Act 1993. Attached are comments from Inland Revenue on some of these discussion papers.

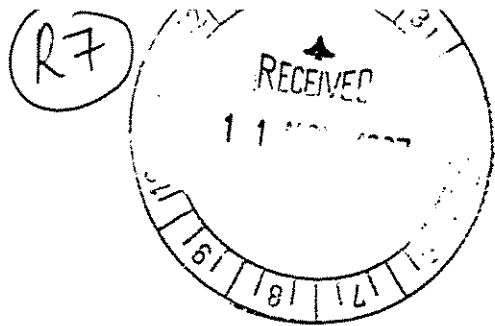
Overall the Department does not have a significantly large number of comments to make. In general we have, to date, not had to many concerns with the current legislation. The majority of comment revolves around either the areas of the Act where there have been some issues or where the Department has comment to make on the question of changes to the Act.

In some cases we have commented on all of the questions raised in the discussion papers, but in others the comments are limited to the questions where an interest exists.

You may also wish to note that the recently created corporate legal services is completing a review of the information statutes (Privacy Act 1993, Official Information Act 1982 and Tax Administration Act 1994) and how they apply to Inland Revenue. As the review progresses and Privacy Act related issues arise, it is anticipated that where appropriate such issues will be brought to the Privacy Commissioner's attention for his input. The review is being completed by David Woodnorth (ph 471-4935).

If you have any questions or would like any further information on any of these comments please contact me on (04) 802-7205.

Paul Matson
Privacy Officer



DP 12 : New Privacy Protections

Q9 The Acts that Inland Revenue administers provide for the exchange of information between New Zealand and certain other overseas countries for the purposes of the administration of the tax system or the collection of child support.

The double tax agreements have exchange of information provisions and generally the following restrictions are placed on the exchange:

The exchange is necessary for the carrying out of the agreement or the domestic tax laws of the overseas country;

The information received by the overseas country will be treated as secret in the same manner as information obtained under their domestic law;

The information can only be used or disclosed by the overseas tax authority to another overseas agencies for the purpose of the administration of the tax system (for example, an overseas court); the overseas country shall not use the information to disclose a trade secret.

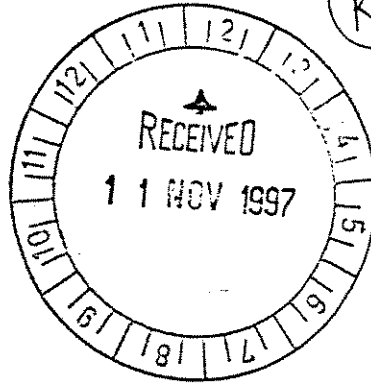
Other agreements that provide for the exchange of information with overseas countries require the information to be used for tax collection purposes only.

The other countries involved are likely to have similar secrecy provisions as those contained in the Tax Administration Act relating to information collected for tax purposes.

Inland Revenue would like to be consulted on any changes to the Privacy Act to control the transfer of information to overseas jurisdictions as this could impact on the tax and child support agreements between New Zealand and overseas countries as well as Inland Revenue's ability to collect tax revenue.



BAYNET C.R.A.
LIMITED



2nd Floor, Baycorp House
15 Hopetoun Street, Ponsonby
Private Bag 92156
Victoria Street, Auckland
Telephone 0064-9-356 5800
Facsimile 0064-9-356 5844
E-mail baynet@baycorp
Reg'n No 371735

10 November 1997

Privacy Act Review 1997
Office of The Privacy Commissioner
P O Box 10 094
WELLINGTON

Dear Sir

Please find enclosed Baycorp's submission on the review of the Privacy Act.

At this point I have not enclosed our submission on Discussion Paper 9. This will follow later this week.

I would like to attend a consultation meeting in Auckland and would appreciate if you could notify me of the date.

Yours faithfully

Gladys Rowley
GENERAL MANAGER

REVIEW OF THE PRIVACY ACT 1993

New Privacy Protections (DP12)

1. **Question 1**

No comment.

2. **Question 2**

We do not consider that the public should be involved in the decision making process as to whether say a new business can be established if that business deals with personal information. However, we do not have any objection to and support the existence of a principle which promotes openness and accountability in respect of that business' database and use thereof.

3. **Question 3**

We consider that any right to anonymity should be balanced against a business' legitimate need for positive identification.

4. **Question 4**

No comment.

5. **Question 5**

No comment.

6. **Question 6**

No comment.

7. **Question 7**

No comment.

8. **Question 8**

No comment.

9. **Question 9**

We do not consider that the fact that say a developing country does not have data protection laws comparable to those in the OECD guidelines should preclude the provision of personal data to the jurisdiction. It has taken New Zealand many years to develop its own Privacy Act and no doubt other developing countries will require time to develop theirs. In the interest of free trade it is important that information flow freely to assist those countries.

10. **Question 10**

We consider that it may be preferable for the Commissioner to have the power to prevent the movement of data if warranted after the proposed transferor of the data has had an opportunity to state its case to the Commissioner.

11. **Question 11**

No comment.

12. **Question 12**

No comment.

13. Question 13

No comment.

14. Question 14

We consider that the Act should specify the categories of information in order that certainty applies.

15. Question 15

No comment.

16. Question 16

No comment.

R 9



Privacy Commissioner
Te Mana Matapono Matatapu

10 November 1997

Office of the Privacy Commissioner

Blair Stewart
Manager, Codes and Legislation
Office of the Privacy Commissioner
P O Box 466
AUCKLAND

Auckland
20 Waterloo Quadrant, Auckland
PO Box 466, Auckland, New Zealand
Telephone 64-9-302 8680
Facsimile 64-9-302 2305
Email privacy@prolink.co.nz

Dear Blair

Discussion paper 12 - New privacy protections

The following are my submissions on some of the questions posed in discussion paper 12. I have only answered the questions which address issues I have had some experience with through my work at the office.

Question 1

I believe that new privacy principles should have the following qualities:

- relevance to most agencies: if a principle is not relevant to the activities carried out by most agencies, it should be placed in a discrete part of the Act, as public registers or information matching have been separated from the information privacy principles;
- relevance to personal information handling: the existing principles tend to deal with information handling policies and processes. Any new principle should have the same relevance;
- state a general principle and then provide specific exceptions: there are two advantages to this. First, it will maintain consistency with the existing principles. Secondly, it states the ideal but also recognises the operational realities.

I do not think the length of a principle should influence its inclusion in the information privacy principles. However, if a new principle is too long, it may be unworkable in practice - there could be too many exceptions or it could be unnecessarily complex.

Question 2

I think a principle of openness that is not linked to collection would be desirable. However, some issues might first need to be addressed:

- would it impinge on the practical operation of principle 2? (it need not necessarily do so)
- how would the information be made available?

- how would the principle be enforced?
- what are the likely compliance costs?

Question 3

A principle allowing individuals to enter transactions anonymously may well be desirable, given the increasing use of electronic transactions. Purpose is a key concept in the information privacy principles, so if information can be collected, uses can, and will, be found for it. This cannot occur if the information is not collected in the first place. So while the information privacy principles provide some protection to individuals, the greatest protection is restricting or prohibiting the collection of information.

A principle of anonymity would have to be subject to some limitations. There will be times when an individual has to be identified, perhaps for verifying claims to various entitlements. There may also be a need to identify individuals to prevent some kinds of criminal activity. Given the developing nature and uses of electronic transactions, it may be appropriate to include a general limitation such as "reasonably justified" and require agencies to do impact assessments to help them assess whether it is necessary to identify individuals in the particular activity.

Question 4

An extension to principle 6 providing that individuals were entitled to reasons for decisions (unless the withholding grounds applied) would be useful, particularly in the employment and education sectors. Many people seem to request access to their files in the hopes of finding why they have been treated in a particular way. They may not get this information because it may not have been stored in a form they can access, or they may not have asked the right questions. A provision allowing for access to reasons might simplify the process for them, and allow agencies to respond more speedily.

The public sector would not have a great difficulty with this concept, given that it has been in the Official Information Act for some years. The private sector might find it difficult conceptually, but it would adjust in time. It would only be an extension of the Privacy Act regime the private sector has been getting used to. Now that there is a privacy regime extending to both sectors, it is hard to justify limiting access to reasons to the public sector.

Question 5

The principles contained in the Australian Privacy Charter seem vague in terms of their ambit. I suspect they would be difficult to enforce. Having said that, the principles about surveillance, physical privacy and not being disadvantaged by exercising privacy rights seem consistent with the Privacy Act's philosophy and could be considered for inclusion in a modified form.

Question 6

The duty of transparency is consistent with the philosophy of the Privacy Act. Transparency and openness are key concepts in the Privacy Act already, but not as duties.

The duty to build privacy protection features into technological designs would be a useful addition to the Act. The lack of privacy safeguards in computer systems has generated a few complaints and frustrated some settlements because of the prohibitive expenses involved in altering the systems. Requiring privacy protection to be built into technological design would solve problems before they arose and before the solution became prohibitively expensive. Although the office recommends agencies carry out privacy impact assessments before commencing an activity, it seems not to be widely done.

The concept of inalienable rights of ownership over personal information could lead to more problems than it would solve. The Act gives a right of access to personal information and ignores property rights. I think this is the preferable approach.

Question 7

Broad privacy principles might be of assistance to the Commissioner in carrying out some of his functions, such as making public statements and reporting on proposed legislation.

Question 8

If broad privacy principles are developed, they should apply to both public and private sectors. Given the broad based application of the Privacy Act, it does not seem appropriate to limit the application of new principle to the public sector.

If new principles are developed, some thought would have to be given to enforcement. It would be difficult to require agencies "to have regard" to principles if that cannot be enforced directly. It is not possible to seek a remedy for breaches of the public register principles, yet the people who have complained of breaches may well have suffered tangible loss.

Question 14

If controls on sensitive categories of personal information are to be introduced, it would seem sensible to introduce a process for determining the categories, rather than specifying them in the Act. The Act's approach to defining information is not prescriptive, and this gives it flexibility to deal with new situations as they arise. The same approach should be taken for sensitive information so the Act is not restricted to some limited categories which seemed sensible at the time an amendment was enacted or regulations issued.

Question 16

I would be inclined to give the Privacy Commissioner the power to develop codes of practice to deal with sensitive information, rather than to require sensitive information

to be categorised in legislation or regulations. The codes process allows matters to be dealt with urgently, as well as giving an opportunity for wide consultation.

Some thought may have to be given to extending the Commissioner's powers so that activities can be prohibited. The current powers allow the Commissioner to modify the information privacy principles to widen or restrict them. This may not be sufficient to allow the Commissioner to prohibit something.

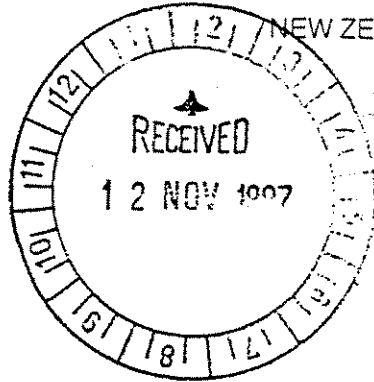
Yours sincerely

A handwritten signature in black ink that reads "Sarah". The letters are cursive and fluid.

Sarah Kerkin
Executive Officer

c:\sarah\misc\submit

R10



NEW ZEALAND VIDEO DEALERS ASSOCIATION INC.
P.O.Box 36-067, Northcote, North Shore City 1330
Phone 9-419 0042 Fax 9-419 0059 Tollfree 0800 999 933

6 November 1997

Privacy Act Review 1997
Office of the Privacy Commissioner
P O Box 10-094
WELLINGTON

Dear Sir

The New Zealand Video Dealers Association, an Incorporated Society, established in 1983, represents some 310 video libraries - approximately 80 percent of the video rental market in New Zealand. Included in our membership is 100 percent representation of the franchises, chain and groups - United Video Franchise Ltd; Video Ezy; Video Village; Blockbuster Video and the 1st Group.

The Privacy Act is an important piece of legislation for every one of our members as in their day to day business each video library captures and holds data in respect of their members (customers). Membership can take the form of individual, joint or family. The data captured is held for the purpose of establishing the identity of the person renting product or equipment in order that it may be recovered in the event it is not returned or, establishing a credit rating where goods over a specified value are rented.

We attach our comments on aspects of the Discussion Papers as we see them affecting our business.

We would like to be included in the consultation meetings.

Yours sincerely

A handwritten signature in black ink, appearing to read "Rosemarie Dawson".

Rosemarie Dawson
Executive Officer

PRIVACY ACT REVIEW

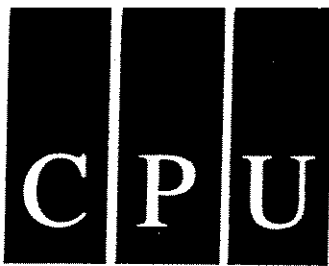
Paper 12, Q 3 Anonymous Transactions

As long as people use charge cards of some form it will probably be impossible to remain completely anonymous. However, it should not be difficult to incorporate say the levels of data control into the system which could either be entered as part of the PIN number to allow the individual to vary the level of control depending on the transaction or part of the card number which would give a fixed level of control. Obviously the Agency must be able to use any data for stock control purposes. However, the wishes of the individual will vary from those who don't want anything recorded about the transaction, through those who don't really care, to those who wish to receive further promotional material based on previous transactions. Exceptions to anonymity would have to be provided still for credit and hire transactions.

Paper 12 Australian Privacy

Private Space

If a blanket rule was to be introduced requiring the provision of private space in all retail environments this could impose a huge cost which would ultimately be reflected in prices. The question is, do people want to pay for this level of privacy or is it better to leave those who wish for this privacy to seek out retail environments that already provide it.

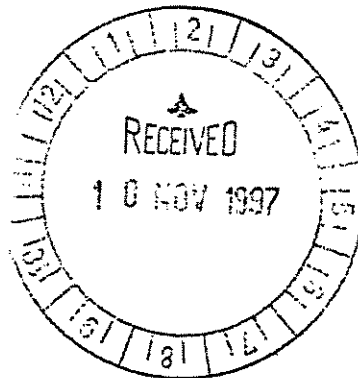


R11

Commonwealth Press Union
New Zealand Section

10 November 1997

Mr Bruce Slane
Privacy Commissioner
5th Floor
Unisys House
44 - 52 The Terrace
WELLINGTON



Dear Bruce

Privacy Act Review

Please find enclosed the Commonwealth Press Union (New Zealand Section) submission to the Privacy Act Review.

If you have any queries or would like any further information please do not hesitate to contact me.

Yours sincerely

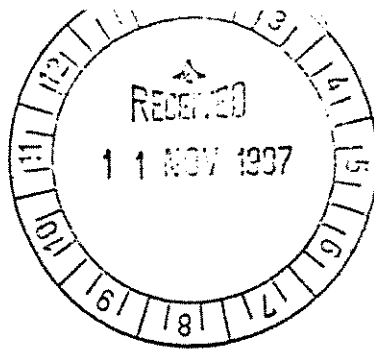
A handwritten signature in black ink, appearing to read 'Phil O'Reilly'.

pp Phil O'Reilly
HONORARY SECRETARY

DISCUSSION PAPER 12 - NEW PRIVACY PROTECTIONS

Discussion paper 12 lists a number of new areas or categories in which the Privacy Act could cover or which new privacy protections could address. We believe that discussion of these issues is premature. It is our view that the current Privacy Act is widely misunderstood and misapplied. We believe that the job of this review should be to clarify the way in which the current Privacy Act operates and to make useful changes to it so that New Zealanders understand important balances between rights related to privacy and those related to, for instance, freedom of information or the need for a free flow of information.

Instead of setting off down new paths we believe it would be better for the Privacy Commissioner's office to ensure that New Zealanders better understand existing protections and freedoms. To further develop the types of issues discussed in discussion paper 12 might lead to further confusion, misunderstanding and misuse of any widened or new statute.



(R12)

NORTHEYPUBLIC & VOLUNTARY
SECTOR CONSULTANT184 Arthur Street, Onehunga,
Auckland, 6. New ZealandPHONE/FAX +64-9-634 1494
EMAIL northey@voyager.co.nz

November 9, 1997

Wendy Bertram
Codes and Legislation Officer
Office of Privacy Commissioner
PO Box 10094
Wellington

Dear Wendy:

Auckland District Council of Social Service Submission on the Review of the Privacy Act 1993

Further to our telephone conversation on Thursday, I attach the submission of the Auckland District Council of Social Service on the remaining discussion papers: 5, 6, 7, 9, and 12 on the Review of the Privacy Act 1993. This follows on from our submissions on discussion papers; 1, 2, 3, 4, 8, 10 and 11 which were posted to Blair Stewart on 17 October. I look forward to taking part in the consultation meeting in Auckland on 24 November where I shall be accompanied by Mike Darke, another Auckland DISCOSS Executive Member, who works for the Combined Beneficiaries Union, Private Bag 68905, Newton, Auckland.

Yours sincerely

Richard Northey

Executive Member

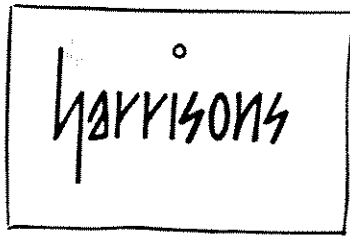
Auckland District Council of Social Service

Attachments: Submissions on papers

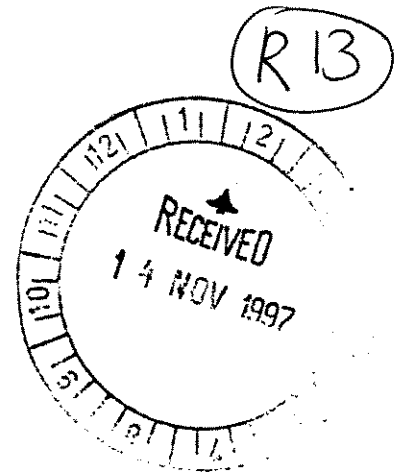
5, 6, 7, 9, and 12.

ADCOSS Submission on Discussion Paper No. 12: New Privacy Protections

- Q1. Yes. If any new principles were required, they should possess the three qualities suggested in the paper.
- Q2. Yes indeed.
- Q3. No. We doubt that this is required as a principle. However, there should be provision for people to obtain anonymity where they request it and provide reasonable justification.
- Q4. Yes, there definitely should be a principle to be required to provide reasons for decisions. This should also be provided in the private sector.
- Q5. Yes. These five principles from the Australian Privacy Charter in general ought to apply in New Zealand.
- Q6. Yes. The principle of a requirement not to disadvantage people who choose to exercise their rights to privacy should be added.
- Q7. Yes.
- Q8. Yes.
- Q9. Yes. The Commissioner should be obliged to take account of how much below New Zealand's standards the other country's privacy standards and laws are.
- Q10. No transborder data flow control is warranted until it has been recommended by the agencies concerned and approved by the Commissioner, who shall have regard to the issues raised in the discussion paper concerning question 9, particularly how far below our standards the other country's are.
- Q11. The test that should apply is that of "equivalent protection". There should be a prohibition applied by the Commissioner until that test is met
- Q12. Protection of the members of stigmatised minority groups. Ensuring health information, eg being HIV positive, has a high level of security compared to benefit and payment information held in agencies like the ACC and Income Support.
- Q13. It might be better to have high minimum standards for the handling and protection of all personal information, particularly by agencies which hold such sensitive information. However, on balance the positive aspects of having such controls predominate.
- Q14. Yes. They should be specified in the Act while providing for further categories to be added by the Privacy Commissioner through codes of practice and then subsequently added to the Act.
- Q15. Those we have listed earlier, particularly spent or live criminal convictions, disabilities, political, religious or other belief and health and sexual behaviour data.
- Q16. If it were decided to introduce such a regime, an amendment to the powers to make codes of practice would be best.



Principal: Cathie Harrison, MA LLB Dip NZLS
Barrister & Solicitor



By Hand

November 14, 1997

Privacy Act Review 1997
Office of the Privacy Commissioner
P O Box 10-094
Wellington

**Telecom New Zealand Limited: Submissions on 1997 Privacy Act Review
Discussion Papers**

I enclose submissions on discussion papers 6, 9 and 12. These are lodged on behalf of Telecom New Zealand Limited.

Telecom has one further set of submissions to make. These are on paper 5 (public register privacy issues) which have a bearing on (among other things) shareholders' registers. The submissions will be brief but unfortunately we are unable to finalise them until early next week because of the unavailability of one or two key people. I will get the submissions to you as soon as possible.

Yours faithfully

Cathie Harrison.

Cathie Harrison
Principal

cc Jonathan Leach
Don McIlroy

REVIEW OF THE PRIVACY ACT 1993
DISCUSSION PAPER NO. 12
NEW PRIVACY PROTECTIONS

Party Making Submission: This submission is lodged on behalf of Telecom New Zealand Limited ("Telecom").

Consultation Meeting: Telecom would like to be invited to attend any consultation meeting.

General Comments: Telecom's comments do not cover situations that are specific only to itself and other telecommunications companies, as these matters have been addressed in the draft Telecommunications Privacy Code submitted to the Commissioner earlier this year. However, Telecom has drawn on its own experience to make comments where it believes that this experience has parallels outside the telecommunications industry.

In some cases, Telecom may state (for example) that it does not believe that any changes to certain principles are required, even though the draft Telecommunications Privacy Code has incorporated changes. Telecom's comments in such instances are directed to the application of the Act in general. They do not relate to the application of the Act to telecommunications companies in particular, since these issues have been covered in the draft Code.

New Principles

Q1: If new principles are to be considered for inclusion what qualities should they possess?

Telecom believes the existing Principles cover all of the core privacy issues. For this reason, if it is thought desirable to introduce further principles, care should be taken to ensure that these do not increase compliance costs. An increase in compliance costs cannot be justified, given that all of the basic privacy concerns are already captured in the Principles.

Q2: Is a new principle, not linked to collection, desirable in respect of the openness regarding agency information practices?

Such a principle could be difficult to comply with in a meaningful way and could significantly increase compliance costs if it is to be observed in other than a token manner. The wording of the Australian Privacy Charter is very open-ended. It would cover practices which do not *actually* interfere with privacy but merely have the potential to do so - even if it is unlikely that such potential will ever be realised.

The introduction of such a principle would add to agency costs - which in the end have to be passed on to the consumer in one way or another - without significantly furthering privacy concerns.

Q3: Would a principle to allow individuals the option of anonymity when entering transactions be desirable? What exceptions might be appropriate?

Telecom could not provide many of its telecommunications services if such a principle was introduced. There are some commercial transactions where anonymity may be an option, eg where payments are in cash or a cash equivalent (such as a phone card). However, most commercial transactions of any substance cannot be provided under conditions of anonymity. At the very least, anonymity should not be an option where this would adversely affect the provision of a service or add to the cost of doing so.

Q4: Should there be a principle concerning reasons for decisions when an agency makes a decision or recommendation in respect of an individual in his or her personal capacity? Would that sit comfortably with the private sector?

Telecom does not believe that such a provision should be incorporated in the Privacy Act. It has the potential to interfere with normal commercial transactions outside the employment field, such as the awarding of contracts or tenders, where individuals are involved. This would significantly increase compliance costs, because agencies would have to change the procedures for dealing with such matters. It would also give individuals an unfair commercial advantage over companies and other bodies.

Q5: Are any new principles or provisions desirable based upon the Australian Privacy Charter?

The Australian Privacy Charter was developed in a quite different environment and does not have the same legal status as the Information Privacy Principles. It is dangerous to treat the Charter's provisions as if they were comparable to the Information Privacy Principles and capable of being applied in the same way. They are not.

Openness and anonymous transactions: These matters have been commented on in Q. 2 and Q. 3 above.

Freedom from surveillance: These concerns are already met by Information Privacy Principles 1 - 4.

Privacy of Communications: Does this mean that (for example) hotels could no longer offer public phones in their foyers, or that public call boxes would have to be replaced? And what implications does it have, for example, for restaurants and other similar venues?

Private space: It is difficult to see how such a principle would sit with the existing exemption for domestic and personal affairs. Introduction of such a principle would lead to enormous compliance costs. It would arguably require all existing public telephone booths to be replaced and would make it difficult for telephone companies to minimise vandalism. Open plan offices (as opposed to partitioned office space) would be ruled out. Hospital wards (as opposed to single rooms) would be ruled out. There appears to be no significant privacy need that would demand such an extreme provision.

Physical privacy: Such matters are adequately covered by the existing Principles.

No disadvantage: Again, such a principle entirely ignores the compliance costs involved.

In short, Telecom does not believe that any new principles or provisions based on the Australian Privacy Charter are merited. The existing Principles and Privacy Act provisions adequately cover the privacy interests concerned.

Q6: Are any new principles or provisions desirable based upon the proposed Canadian Charter of privacy rights?

No. Taking the examples in turn:

- Traditionally the law has never recognised property rights *in* information (as opposed to rights or duties *in respect of* information, eg copyright or duty of confidentiality). Any introduction of a concept of *ownership* of personal information would have consequences that extended far beyond issues of privacy. For example, it could be used to support arguments that individuals have a right to be remunerated because their personal details appear in a publication which is available for public search, or in a biography, or because such details are used for market research.
- The question of anonymity has already been commented on in Q. 3 above.
- Introduction of a duty not to disadvantage anyone who elects to exercise a right to privacy could also have very far-reaching effects. It would seem to undermine the right of private sector agencies to charge in connection with access requests. More importantly, it could impose significant financial burdens on agencies in some circumstances. For example, an agency could be required to provide a service to a small number of customers at great cost to the agency without being able to recover the costs of doing so.

Q7: Is there value in developing within the statutory framework a set of broad privacy principles...as a guide to the Privacy Commissioner in the exercise of his functions?

Possibly, provided the principles apply only to the Commissioner and do not have to be observed by other agencies.

Q8: If a set of broad privacy principles...were to be developed, would it be inappropriate to require agencies to have regard to them?

Yes - as noted above, principles of the type proposed would result in a very substantial increase in compliance costs.

Q9: Should the Privacy Act include controls on the transfer of personal information to jurisdictions which do not apply a standard of protection comparable to those in the OECD Guidelines?

Such controls could seriously hamper the provision of international telecommunication services if they extended to telecommunications companies. Whereas it is possible for a telecommunications company to block the presentation of CLI, it is not technically feasible for such a company to block the *content* of those voice, fax, or data transmissions (including Internet transmissions) that contain personal information, while permitting other telecommunications to proceed unimpeded. The telecommunications company is not in a position to monitor content. It would therefore be futile to purport to put in place controls restricting it from providing telecommunications service where this involved the transfer of personal information to certain countries.

Moreover, such a provision would represent a move away from the "principled" approach that New Zealand has adopted to privacy to date. The beauty of the information privacy principles is that they can be applied in such a way as to take the particular circumstances of use, disclosure, collection etc into account. Introduction of controls of the type proposed, would not permit this. For example, they would not cater for transactions which of themselves raise no privacy concerns, eg where the parties to a transfer of information have put in place measures to ensure a secure environment notwithstanding any lack of *legislative* privacy protection in the country concerned, or where individuals have been given the choice of whether or not information should be disclosed and have consented to such disclosure.

If such controls were nevertheless introduced, it is crucial that the provision of telecommunications services be excluded from their operation. (That is not to say that such controls should not apply to third party agencies that *make use of* such services to transmit data - as opposed to the agencies that provide the telecommunications services.)

If controls were to be adopted, it would be necessary to provide that such controls do not apply to any agency providing telecommunications services

in relation to such services - much the same as the exemption for the news media. In other words, the exemption would not extend to activities undertaken by a telecommunications service provider that were not directly or indirectly related to the provision of telecommunications services.

However, Telecom reiterates that it does not believe that it would be appropriate to introduce such controls.

Q10: If a transborder data flow control is warranted, should it empower the Commissioner to take prohibition action in exceptional cases? Or should any provision place the responsibility on agencies...?

Telecom believes the responsibility should be on the agency concerned. Again, however, it is crucial that telecommunications services be excluded from any controls.

Q11: What test should any transborder data flow control apply?

Telecom makes no comment on this matter at this stage, save to reiterate the points made above.

Q12 - 16:

The same comments apply.

LIST OF SUBMISSIONS

The following is an alphabetical list of people and organisations which made submissions by 23 December 1997. Many organisations are listed here as having made a submission. In some cases the submission may not be the formal position of the whole organisation but rather an expression of views of an officer, employee or division of that organisation.

S35	Age Concern Canterbury
O10	Anti-Bases Campaign
S22	Ashburton Branch, NCW
S56, K5	Association for Market Research Organisations
K24	Association of Superannuation Funds NZ Inc
H13	Auckland City
O2	Auckland Council for Civil Liberties (Inc)
G6, H3, K11, L7, M4, N3, O15, PQ8, R12, T9, UV12, WX8	Auckland District Council of Social Service
S1	Auckland Healthcare Services Ltd
O4	Bagozzi, Daniela
UV14	Banking Ombudsman
G13, H7, K21, L17, M12, N12, O13, PQ7, R8, T10, UV8	Baynet CRA Ltd
N14	Bertram, Wendy
G20	Cairns, Joanne
O7	Campaign for Nuclear Disarmament (Wellington) Inc
O3	Chapple, Jim
G17, H8, K23, M13, N13, R11, T8, UV11, WX7	Commonwealth Press Union
G1, H1	Comrie, Clive
K18, L13, M9	Consumers' Institute
G16	Crown Law Office
N6, S6	Dalziel, Kathryn
M15	Debenham, Terry
S33	Department for Courts
S18	Department of Corrections
G19, H9, K27, M14, T12	Department of Internal Affairs
S41	Department of Internal Affairs - Local Government and Community Policy
PQ10	Department of Labour
S21	Dynamic Controls Ltd
S43	Eastbay Health
S45	Family Planning Association NZ
L20	Federation of Women's Health Councils Aotearoa NZ
L1, R1, UV1, WX1	FINSEC
G3, K8, L2, M2, N2, T2, WX2	Franklin District Council
S37	Gordon, Mary-Ellen
K4, S30	Government Communications Security Bureau
K17	Government Superannuitants Assn of NZ (Inc)
O8	Hager, Nicky
S16	Hattaway, Peter
S31	Health and Disability Commissioner
S7	Healthcare Otago Ltd
S4	Human Rights Commission
H11	Hutt City Council
K20, L16, M11, PQ6, R7, UV7	Inland Revenue Department
O1	Inspector-General of Intelligence and Security

L9	Insurance Council of New Zealand Inc
K9	Investment Savings and Insurance Association
S54	Janczewski, Dr Lech
K15	Jorgensen, Murray
S38	Kaitaia Council of Social Services
PQ2	Kelly, Paul
S15	Kensington Swan
R9	Kerkin, Sarah
S5	King, Chris
L8	Langdon, Kristin
S51	Local Government New Zealand
WX10	MacDonald, Ian
G9	MacFarlane, J J D
T14	Makani, Tania
T11	Manukau City Council
S32	Market Research Society of New Zealand
UV2, K3, N1, PQ1, R2, T1	Mein, Dr J N
S27	Ministry of Agriculture
S20, S20(a)	Ministry of Commerce - Business and Registries Branch
L11, S53	Ministry of Education
S58	Ministry of Transport
S23	Napier Council of Social Services
S12	National Council of Women
S44	National Library
S9	Northland Chamber of Commerce
S36	Nurse Maude Association
T15	Nursing Council of New Zealand
L6	NZ Airline Pilots' Association
S26	NZ Association of Citizens Advice Bureaux
G5, L5	NZ Association of Crown Research Institutes (Inc)
PQ4, R5, T5, UV3, WX4	NZ Association of Social Workers Aotearoa
N10, S40, S25	NZ Bankers' Association
S50	NZ Business Roundtable
K13, M7, N9, O5, S2	NZ College of Midwives (Inc)
S55	NZ Council for Civil Liberties
S24	NZ Defence Force
G10, H5, K14, L12, M8, Mc1, N4, R3, UV4, WX3	NZ Employers Federation
S29	NZ Federation of Family Budgeting Services (Inc)
S28	NZ General Practitioners' Association Inc
S46	NZ Medical Association
K7	NZ Railway Superannuitants' Association
S10	NZ School Trustees Association
O14, S8	NZ Security Intelligence Service
G14, K22, R10, WX6	NZ Video Dealers Association Inc
L3	Office of the Commissioner for Children
M5	Office of the Controller and Auditor-General
K6, M1, T4	Palmerston North City Council
H10	Parry, David
K2	Pateriki-Davenport, Angela
S47	Patients Rights Advocacy
G15	Paton-Simpson, Elizabeth
S13	Porirua City Council
G2, K1	Rajasingham, Dr Lalita
O6	Riley, G F
N5	Robinson, Trevor

S42	Rosamund Averton
S49	Roth, Dr Paul
G4, H2, K10, L4, M3, N8, O9, PQ3, R4, T3, UV5	Royal NZ College of General Practitioners
S3	Service Workers Union
K16	Simon, Silke
S11	State Services Commission
O12	Suggate, Richard
H12, T7	Tauranga District Council
S39	Te Puni Kokiri
S48	Teeuwen, W P
G8, H4, K12, L10, M6, N7, T13, UV13, WX9, R13	Telecom New Zealand Ltd
L21	The Health Alternatives for Women (Inc)
S14	Transit New Zealand
L15	Transport Accident Investigation Commission
G18, K25, L19, S52	Tranz Rail
G7	Tribunal for the Catholic Church for New Zealand
G11	Tucker, Jim
UV10	TVNZ Group
T16	Valuation New Zealand
G12, H6, K19, L14, M10, N11, O11, PQ5, R6, T6, UV6, WX5	Wellington City Council
L18	Wellington Community Law Centre
S19	Wellington District Law Society - Constitutional Matters Committee
S34	Westpac Trust
S57	Westwater, Margret
PQ9	Omitted

compile\submis

