The Security Intelligence Service Amendment Act 1977 and the state power to intercept communications

G. Crowder*

In the wake of the controversy attracted by the passage of the New Zealand Security Intelligence Service Amendment Act 1977, this article examines the law in New Zealand relating to the power of the state to intercept communications. It is contended that wide powers of interception existed prior to the passing of the Amendment Act. The writer suggests that Parliament, in enacting the new legislation, failed to take this into account and that it also failed to provide adequate protection for the individual against abuse of the power.

In 1976 the then Chief Ombudsman, Sir Guy Powles, tabled in Parliament a Report on the Security Intelligence Service.[1] That Report contained the recommendation[2]

> That the 1969 [New Zealand Security Intelligence Service] Act be amended to provide for authority being given to the Service to intercept communications under specific conditions and subject to satisfactory control.

The specific amendments were set out in a draft clause, preceded by a discussion of the need for such authority and the present doubtful adequacy of the law to provide it. This, along with other recommendations from the Report, was implemented in the New Zealand Security Intelligence Service Amendment Act which was passed into law on 16 November 1977. Inevitably the Act has been a source of controversy, at its peak unusually heated for the New Zealand political climate, touching an area frequently described by the Prime Minister as very "delicate".

The delicacy of the situation refers to the great difficulty, where the particular value called "national security" is at stake, of reconciling the interests of the state with those of the individual. The problem is greatest in a legal system which aspires to democratic ideals. Freedoms said to reside as of right in the individual are restricted to an unusual extent in favour of the security purpose. Clearly, the

* This article is based on a research paper submitted for the LL.B.(Honours) degree.

1. Report by Chief Ombudsman *Security Intelligence Service* (Wellington, 1976) hereinafter referred to as the Report or the Powles Report. The Security Intelligence Service is hereinafter referred to as the S.I.S.
2. Ibid., 9.

issue of interception of communications is fertile ground for the constitutional lawyer.

I. THE PRE-EXISTING LAW

Is the interception of communications by the state lawful in New Zealand apart from the Amendment Act? The Powles Report suggests that for the purposes of the S.I.S. it is not, and hints that the Service may thus have engaged in activities which were then illegal.[3] The main concern that emerges from Sir Guy's draft amendment, and which has now been translated into the Amendment Act, is the establishment of a lawful procedure enabling the Service to carry out surveillance which would otherwise be unlawful but which is necessary.

The question of the prior legality of interception is basic to an assessment of the effect of the new Act. If no lawful power existed before the passing of the Act, as appears to be the theme of the Powles Report, the Act then clearly creates such a power. But if a similar power was already in existence, the effect of the Act takes on a different complexion. It is submitted, with respect, that some of the conclusions on the law contained in the Powles Report are doubtful, and that wide powers to intercept communications pre-dated the Act.

A. Interception of Post and Telephone

The Powles Report contains the conclusion of legal counsel that in New Zealand:[4]

> There is no legal basis for the interception by postal authorities of letters, telegrams, and telephone conversations in times of peace other than for the purpose of protecting postal facilities and communications and of ensuring the operation of adequate and efficient postal services.

Clearly this formulation does not include the purposes of the S.I.S. Unfortunately, the conclusion is supported only by a series of statements about the law which are themselves conclusionary. The Report appears to have sought a legal basis for the power in the practice of the United Kingdom, which is accepted as lawful. The conclusion of the Chief Ombudsman is that British practice is unhelpful to the identification of a legal basis for the power in New Zealand.[5] The basis of the legality of the British practice is uncertain. It may be based upon prerogative powers, common law rights, usage, implication from statutory provision or absence of legal prohibition. These were the bases considered by the Committee of Privy Councillors (the Birkett Committee) whose Report in 1957[6] is the most comprehensive examination of the British executive power to intercept communications. The Committee affirmed the legality of the power, but despite its extensive researches it was unable to identify any of the five possibilities as definitely being the source. In the opinion of the Powles Report, none of the possible bases has application in New Zealand other than for the limited purposes already mentioned.

3. Ibid., 57-58. 4. Ibid., 58. 5. Idem.
6. *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications* (London, 1973, Cmnd. 283).

1. Prerogative

The Powles Report states that the prerogative power can afford no basis to authorise interception of postal communications in New Zealand, at least in time of peace.[7] The Chief Ombudsman appears to give this as the main reason why the British practice is unhelpful in the New Zealand situation, on the premise that the ancient prerogative of the Crown is, at least in part, the basis of the legality of that practice. With respect it is submitted that the Birkett Committee gave so little weight to the argument that the power was a prerogative power, as almost to dismiss it entirely. In its Report, the Committee observed that no writer on the subject of the Royal Prerogative mentions the power to intercept as being a prerogative power.[8]

That the power to intercept was never a prerogative power in England is one argument why prerogative cannot be the basis of a New Zealand power. A second argument could be that in this country the prerogative power to intercept has been superseded by statute,[9] either substituting a statutory power to intercept or creating a prohibition. Otherwise, there appears to be no reason why a prerogative power to intercept, if it existed in England, cannot be exercised in New Zealand. When the Crown came to New Zealand the prerogative travelled with it.

2. Common law

The Powles Report considers that there may be a common law right in the postal authorities to intercept communications in New Zealand, but only for the purpose of protecting postal facilities and communications.[10] This is in line with the argument put to the Birkett Committee that the power to intercept derived from an inherent power in the Crown to protect the realm against the misuse of postal facilities by ill-disposed persons. But again the Committee could find no support for this view in any judicial pronouncement or legal text-book, and considered it scarcely different in substance from the prerogative argument.[11]

3. Long usage

The Birkett Committee appeared to be impressed most by the argument that, although the origins of the power may only be conjectured, the power to intercept and open letters has been in existence from the earliest times, and the practice has continued throughout many centuries.[12] Long usage does not of itself establish legal authority. But the Committee appears to have accepted it as a sufficient justification for affirming the legality of the power when it was taken together with the possible bases already canvassed, and evidenced by implication from statutory provisions and the absence of legal prohibitions.

The Powles Report baldly asserts that usage can confer no legal right upon postal authorities to intercept communications in New Zealand.[13] This might be because the power has not been exercised in New Zealand over a sufficiently long period — although this argument falls if the New Zealand usage is viewed as a continuation of the English. Otherwise the rejection of this possibility turns on the rejection of the others, especially the evidentiary ones.

7. Ibid., 58.
8. Ibid., 10, para. 23.
9. See discussion of Post Office Act 1959, post, p. 148.
10. Ibid., 58.
11. Ibid., 11, paras. 27-29.
12. Ibid., 11, para. 30.
13. Ibid., 58.

4. Statute

The most contentious of the conclusions of the Powles Report on the law is that statutory provisions in New Zealand may impliedly authorise interception of letters, telegrams and telephone conversations, but only for the purpose of ensuring efficient and adequate postal facilities.[14] It seems that statutory provisions authorise interception both impliedly and expressly, but it is difficult to find any authority for the claimed limitation as to purpose.

Section 109 of the Post Office Act 1959 may impliedly recognise a lawful power to intercept telephone conversations when it makes it an offence for every officer of the Telephone Service to divulge information obtained by him from telephone conversations overheard in the course of his official duties "without good and sufficient cause". The same implication is raised by section 158 of the Act, which makes it an offence to connect "any additional apparatus or equipment" to the telephone system when this is done "without the authority of the Postmaster-General". In respect of these provisions the limitation argument is at its strongest. It is unlikely that either section was intended to comprehend a wide interception power, but merely to assist the efficient running of the telephone service.

In particular, however, section 34 of the Post Office Act appears to provide express authorisation for the general interception of letters and telegrams. Section 34(1) states that:

> The Governor-General may, by Warrant under his hand, direct the Postmaster-General or any officer to detain or open any postal article for any purpose mentioned in the Warrant.

Under section 12(1) of the Act, "postal article" includes telegram. How can section 34(1) be read subject to the limited purpose defined in the Powles Report? That purpose is close to the formulation used in respect of the claimed common law right, but it is hard to see any necessary connection between that right, if it exists, and the present legislation. It might also be argued that the exercise of the power under section 34 can be limited by the willingness of the courts in some cases to read wide statutory provisions as conferring powers limited to the promotion of the policy and objects of the particular Act, which are to be determined by the construction of the Act.[15] But in this case the scheme of the Act seems to manifest an intention in the legislature that section 34 should provide a power of very wide scope. Sections 27 to 33 of the Act provide powers of interception, examination and in some cases disposal for specific purposes. For example, under section 27, the Postmaster-General may authorise interception for the purpose of returns. Section 34 seems to provide a power over and above the powers available for specific purposes. It is available only under warrant from the Governor-General, which implies a decision at Cabinet rather than merely departmental level.

Further, an examination of the historical policy of the English Post Office statutes tends to support the wider interpretation of the power to intercept postal articles. Legislation of 1657 and 1660 created a General Post Office, and thereby a monopoly for the Crown in the carrying of letters. Part of the object of these provisions is said to be that the mail should be liable to inspection by the Crown, and the Crown alone. The Ordinance of 1657 recites one advantage of settling the General Post Office as

14. Idem.

15. *Padfield* v. *Minister of Agriculture* [1968] A.C. 997.

> the best means to discover and prevent many dangerous and wicked designs which have been and are daily contrived against the peace and welfare of the Commonwealth, the intelligence whereof cannot well be communicated but by letter of script.

Since 1710 the Post Office statutes have apparently recognised a lawful power to intercept mail under warrant from a Secretary of State. The current Post Office Act 1953 makes it an offence under section 58(1) for any officer of the Post Office to detain or delay a postal packet, except, inter alia, when he acts "in obedience to an express warrant in writing under the hand of a Secretary of State". That section is of the same effect as the New Zealand provisions.

5. Absence of legal prohibitions

Arguments that a lawful power to intercept exists because there are no legal prohibitions against it clearly cannot apply to the interception of postal articles. Both in the United Kingdom and in New Zealand Post Office legislation secures the inviolability of letters and telegrams against unauthorised opening, delaying or disclosure.[16] However, in relation to the interception of telephone communications, the Powles Report seeks another distinction between British practice and New Zealand law in that the former jurisdiction appears to enforce no relevant prohibition, while there are such prohibitions here.[17]

Although this conclusion seems strictly correct, it may be noted that the informal practice of the Home Office in permitting telephone interceptions to take place only under warrant is probably, in effect, more restrictive of such activity than are the few statutory prohibitions available in New Zealand. Until 1937 the United Kingdom Post Office had acted upon the view that the power which the Crown exercised in intercepting telephone messages was a power possessed by all other operators of telephones, and was not contrary to law.[18] In that year, however, it was decided as a matter of policy to bring such interception within the control of the warrant of the Secretary of State.

The major prohibition in New Zealand is section 158 of the Post Office Act 1953. But, recalling that this section at the same time implies the existence of a power to intercept telephone conversations on the authorisation of the Postmaster-General, one might be reluctant to advance it as an important ground for distinguishing the British practice. Again it is doubtful that the legislature had the broader interception situation in mind when section 158 was drafted. The policy of that provision is merely to maintain the Post Office telephone monopoly.[19] The same arguments apply to section 109.[20] Hence there is little substantial difference between the New Zealand and British positions as regards the presence or absence of legal prohibitions relating to the wider interception situation. In any case, it may be argued that absence of prohibition is merely evidentiary of long usage or of a prerogative power.

The above discussion indicates that there must attach considerable uncertainty to the final conclusion of Sir Guy Powles' legal counsel on the state of the law prior to the Act. There seems to be no particularly compelling reason why any

16. Post Office Act 1953 (U.K.) s. 58(1); Post Office Act 1959, ss. 55-59.
17. Ibid., 58.
18. Birkett Committee Report, op. cit., 13, para. 37.
19. See *Machirus* v. *Police* (1977) 3 Recent Law 103, noted by W. Hodge *N.Z. Listener* September 15, 1977, p. 16.
20. See also Telephone Regulations 1976 Regs. 56, 62, 154.

of the five possible bases for the power, if they were held to be valid in an English context, ought not to apply to the New Zealand situation. In general, there does not seem to be that great a distinction between the legal positions of the two jurisdictions to justify the affirmation of the existence of a lawful power in one but not in the other.

The Birkett Committee could not dispel the obscurity of the legal basis of the power, although it purported to affirm its existence. The Committee could find no direct basis for the power in prerogative or common law. It leaned heavily on long usage, as evidenced by statutory implication and absence of legal prohibition. Even in its conclusion, the Committee was unable to declare with certainty that there is a lawful power in England to intercept telephone communications.[21] Therefore, if it is argued that there is no legal basis for the power to intercept in New Zealand, a good ground may be that the British practice from which it developed has itself no proven basis in law, even though it has been historically recognised as lawful. However, both this argument and the conclusion of the Powles Report run into difficulties when the wide provision for interception under warrant in section 34 of the Post Office Act is taken into account. There seems to be no way that section 34 can be convincingly accommodated within a conclusion that in New Zealand there is no lawful power to intercept, or that the power is narrowly defined to perfunctory purposes. Uncertainty on this issue is admitted in the Powles Report itself when it is noted that at least one Postmaster-General, the late Hon T. P. Shand, did not accept the view that the statutory authority must be used for the purpose of protecting postal facilities. He was prepared to exercise the authority in respect of national security matters if he considered it necessary and the Prime Minister so requested.[22]

B. Eavesdropping Devices

The Powles Report does not discuss the law relating to the use of eavesdropping devices, other than by implication when it states that the New Zealand legislation deals only with postal communications.[23] There is no statutory provision which suggests that there might be a lawful power to use such devices. The position is the same in the United Kingdom. Presumably, the argument that the prerogative may authorise interception of postal communications might be extended to include the eavesdropping situation, but this has never been pursued. No such argument was canvassed before the Birkett Committee, which indeed had difficulty even in extending the power to telephone interception.

But even if the state has no express power to use such devices, it appears that the individual will have a remedy against their use only if there is an incidental infringement of his proprietory rights.[24] Thus, the user of the device may be liable in trespass when he enters or interferes with another's property in order to plant it. In *Sheen* v. *Clegg*[25] damages in trespass were awarded against a

21. Ibid., 15.
22. N.Z. Parliamentary debates Vol. 311, 1957: 2, 325, 726, 737. See also Hon. Dr A. M. Finlay, then Minister of Justice, N.Z. Parliamentary debates Vol. 400, 1975: 3413.
23. Ibid., 59.
24. See Burns "Privacy and the Law: 1984 is Now" [1974] N.Z.L.J.1.
25. *Daily Telegraph* June 22, 1961, cited in R. F. V. Heuston *Salmond on the Law of Torts* (16th ed., London, 1973) 35.

defendant who secretly installed a microphone over the plaintiff's marital bed. Similarly, the incidental invasion of the proprietory right may attach criminal liability for breaking and entering.[26]

But if no such invasion has occurred, there is no action at common law for the act of eavesdropping per se. No recognised legal right has been infringed. Technological developments have virtually removed any effect the trespass action may have had in this area in that many devices are now available which are effective in monitoring conversations in other rooms and buildings without entry having to be gained to plant them. Contact microphones, or "detectaphones", which are attached to the opposite side of a wall in a room, have been in use for many years now.[27] A more recent development is the parabolic microphone, which can monitor conversations in the open air, or in rooms with open windows, from hundreds of yards away.[28] At common law just as no action lies for the overhearing of a conversation in the street, there is no remedy against the use of sophisticated eavesdropping equipment. It appears that this area virtually represents a legal vacuum.

In summary, the state of the New Zealand law relating to interception prior to the passing of the Amendment Act may be stated thus:

(1) There appears to be wide statutory authority for the interception of postal articles under warrant.
(2) Interception of telephone conversations may be impliedly authorised by statute.
(3) Without the authorisation of statute or warrant, the interception of postal articles and telephone conversations is prohibited.
(4) The use of eavesdropping devices is restricted only by the law of trespass.

II. THE NEW ZEALAND SECURITY INTELLIGENCE SERVICE AMENDMENT ACT 1977

As it relates to the interception of communications, the New Zealand Security Intelligence Service Amendment Act 1977 gives the Service the power under warrant to intercept communications for security purposes and within the confines of certain safeguards. For the most part it follows quite closely the draft amendment recommended by the Powles Report, which in turn was modelled largely on section 6 of the Canadian Protection of Privacy Act 1973-74. The major issues raised by the Amendment Act range from the specific to the very broad.

A. The Need for the Power

Some of the most critical statements made in respect of the Amendment Act have questioned the necessity or the desirability of institutionalising any power to intercept communications. Mr David Lange M.P. has described the proposals as anathema to the whole of New Zealand's previous constitutional history.[29] The opposing argument stresses that interception is a valuable tool with which to combat individuals and groups who threaten the security of the state. The conflict is

26. Crimes Act, ss. 241, 242.
27. See *Goldman* v. *U.S.* 316 U.S. 129 (1942).
28. Joseph W. Bishop "Privacy vs Protection — The Bugged Society" *New York Times Magazine* 8 June 1969, 31.
29. *Evening Post* Wellington, August 9, 1977.

deep-seated, and flows into the broader question of how the functions of a security service in general may be reconciled with the ideals of democracy. The very existence of a security service in New Zealand creates this conflict. On the one hand the state claims to guarantee freedoms, and on the other monitors the activities of people who exercise them.

In an extract from the "Statement by the Service" published in the Powles Report, the S.I.S. itself adopted a qualification to the requirement for security procedures stated in the 1969 Canadian Royal Commission Report:[30]

> Because security procedures may so closely affect the fundamental freedoms of individuals, in a democratic society, they must be shown to be necessary and must operate within a framework of a carefully formulated and consistently enforced policy.

Are the conflicting values "security" and "democracy" irreconcilable? There exists a considerable body of opinion to the affirmative. In particular, the New Zealand Council for Civil Liberties and the Public Service Association have argued that the Service should be dispensed with, making similar submissions to that effect at the time both of the passing of the New Zealand Security Intelligence Service Act 1969 and of the Powles Report.[31]

The Powles Report justified the need for a security service principally for the purpose of protecting state secrets either generated within New Zealand or received through cooperation with other countries.[32]

Assuming the validity of the security interest in general, does it justify the practice of interception? The Powles Report implies an affirmative response when it states that the law should allow such methods "[w]here there is good ground", and that in some cases there will be no other way of obtaining "essential information".[33]

This seems to reflect the generally held view that there is little question that state security is an ample justification of interception. The Birkett Committee was in no doubt on this matter.[34] Even in the context of a strong constitution guaranteeing individual rights, as in the United States, the national security interest is consistently recognised as paramount, and as justifying the taking of whatever means may be considered necessary for its protection.[35]

Although the weight of these arguments is difficult to resist, one might express some significant reservations about them. First, several commentators and interested groups have questioned the need for a power to intercept in terms of how effective it will be in achieving its supposed goals in respect of security. Those intended to be the subjects of such provisions will to a great extent wade them simply by ceasing to communicate by telephone or mail. The people most affected will be ordinary citizens. Secondly, the scope of security surveillance in New Zealand, prescribed in the Act by formulations as broad as "subversion" and "security",

30. Ibid., 18.
31. Report on the 1969 Act, cited in the Powles Report, 21.
32. Ibid., 19-23; see also L. Atkins "The Parliamentary Process and the New Zealand Security Intelligence Service" in *New Zealand Politics: A Reader* ed. Levine (Melbourne, 1975) 384, 386 who provides another interesting reconciliation in ideological terms.
33. Ibid., 57.
34. Ibid., 32, para. 141.
35. See American Bar Association *Standards Relating to Electronic Surveillance* (1971, New York) 120.

is a disturbingly wide area over which to authorise a power to intercept. Thirdly, the need for the power in areas where the functions of the S.I.S. overlap with those of the police involves a rather different judgment than does the security question.

B. Definitions

The greatest danger in the provisions of the Amendment Act relating to the power to intercept stems, not from the enactment of the power per se, but from the application to that power of the wide and uncertain terms intended to delimit the boundaries of the general functions of the S.I.S. At the heart of this danger is the word "security". Section 4A(1) (as inserted by Section 4 of the Amendment Act) provides that the first criterion for the issue of a warrant is that the interception is necessary either for the detection of activities prejudicial to security, or for the purpose of gathering foreign intelligence information essential to security. What is "security"? Section 2 of the principal Act defines it as

> the protection of New Zealand from acts of espionage, sabotage, and subversion, whether or not it is directed from or intended to be committed within New Zealand.

The Amendment Act widens the security definition further by incorporating into it the protection of New Zealand from acts of "terrorism". The formula "the protection of New Zealand" is itself a limitation on the kind of security that the S.I.S. ought to be concerned with. It should be concerned only with the security of the nation as a whole, and therefore the information it seeks under its general intelligence gathering function[36] ought to be confined to that which affects the nation as a whole. This policy is derived from British practice which describes the function of the security service as being "the Defence of the Realm".[37]

But the term "subversion" represents a very difficult gray area, making the whole "security" concept an open-ended one. Section 2 of the principal Act defines subversion as

> attempting, inciting, counselling, advocating, or encouraging —
> (a) The overthrow by force of the Government of New Zealand; or
> (b) The undermining by unlawful means of the authority of the State in New Zealand.

"Subversion" is not a term traditionally known to the law. It is also difficult to say what is meant by "undermining by unlawful means". However, the particular danger, as noted by the Powles Report,[38] is that the function of the S.I.S. to gather information relevant to subversion has in the past led to a tendency to monitor individuals and groups which are not subversive, but are potentially subversive. The target of the surveillance then becomes political opinion. The monitoring of opinion, dissent and protest is not, without more, comprehended by the "Defence of the Realm" limitation on security service functions.

One of the more significant provisions added to the Amendment Bill after the first reading is that the Service is now expressly excluded from surveillance of any person by reason only of his involvement in lawful protest or dissent in relation

36. See New Zealand Security Intelligence Service Act 1969, s. 4(1)(a).
37. Directive of Sir David Maxwell Fyfe, the Home Secretary ,to the Director-General of the Security Service, September 24, 1952; see also *Lord Denning's Report* on the Security Service (London, 1963, Cmnd. 2152).
38. Ibid., 28-30.

to the laws or Government of New Zealand.[39] As far as it goes, this is a welcome re-definition of the general functions of the Service. But, leaving aside the obvious doubts about enforcement of the new limitation, the question still remains of what constitutes subversion. With the removal of "lawful protest or dissent" from the purview of the Service, "subversion" no longer appears to have any practical content.

The problem of the scope of the powers is compounded by the wide definition of "intercept" contained in the Amendment Act. A warrant to intercept may authorise a seizure of communications, or a recording of something less than the precise wording of the communication. "Intercept" probably does not mean listening in to a conversation with the consent of one of the parties, because this is already lawful. Therefore, a warrant need not be issued in the situation, for example, where the S.I.S. or the Police listen in to a conversation on an extension telephone with the consent of either party.

C. Ministerial or Judicial Power?

Under section 4A(1) of the Act the basic power to issue a warrant to intercept communications is vested in the Minister responsible for the S.I.S. Whether the warrant ought to be issued by the Minister or by a judicial or other non-political officer is perhaps the most discussed issue connected with the Amendment Act. The vesting of the power in the Minister raises in the minds of many people the ogre of abuse of the power for party political ends along the lines of the American Watergate affair. Few of those individuals and groups who have criticised the proposed provisions have not expressed some misgivings about ministerial control in this area.

Section 4A(1) does not sit entirely comfortably within the framework of English constitutional law. The general rule that the courts rather than the executive should control the issue of warrants to search the premises of a private individual was firmly established in a series of cases in the 1760s following the issue by the Government of the day of general warrants, not specifying either the person or the property to be searched. In the great case of *Entick* v. *Carrington*[40] the Lord Chief Justice castigated the conduct of the Government and awarded £300 damages in trespass to a plaintiff whose papers were seized under a general warrant. The concurring judgment of Lord Camden in the Court of Common Pleas was cited in the Birkett Committee's Report as a major argument against the claim that the power of the executive to intercept is a prerogative power.[41]

The Powles Report, although noting the strong reactions against executive warrants to be found in our constitutional history, and observing that the argument that an independent judicial officer should have the power is a strong one, nevertheless recommended that the Minister should have the power. The Chief Ombudsman gave four reasons for this view:[42]

(1) The Minister is responsible for the Service.

(2) The grant of the warrant is likely to be part of an on-going intelligence exercise not resulting in court proceedings (unlike the situations where a judicial officer grants a warrant).

39. S. 3(2), amending s. 4(2) of the principal Act.
40. (1765) 19 St. Tr. 1030. 41. Ibid., 10-11. 42. Ibid., 57.

(3) There are problems in properly briefing a person issuing a warrant.
(4) Judicial officers should not be involved in what is essentially executive business.

It is submitted that these arguments, at least in the summary form in which they appear in the Report, are not wholly convincing. As to the first point, the extent of ministerial responsibility for the S.I.S. is at present uncertain, as is noted elsewhere in the Report.[43] Further, another issue attaches to the question of just to what extent the Minister may be held accountable for the interception warrants themselves.[44] Secondly, one may question the validity or need of an "ongoing intelligence exercise" that is not likely to lead to any court proceedings. This again relates to the scope of S.I.S. functions in general. Thirdly, what substantive problems can it be said arise in the briefing of a judge as opposed to the Minister? In the past the Minister appears to have had no consistently close contact with the Service which might place him at an advantage here.[45] The fourth reason appears to relate to the general practice of the courts in avoiding interference with the exercise of executive discretion in the national security area. Again, however, one may ask what exactly is the scope of this area. Under the terms of the principal Act, the Minister may claim the national security blanket for a huge field of reasons.

But, as the Chief Ombudsman notes, the power to intercept in the security area rests with the executive in the United Kingdom, Australia and Canada. In respect of the former jurisdiction the Birkett Committee was satisfied that the power was "properly and wisely executed" by the Secretary of State without further safeguards.[46] In Australia, the Attorney-General has the power to issue warrants to intercept telephone conversations on broadly defined Commonwealth security grounds, and the Director-General of the Australian Security Intelligence Organisation may exercise the same power in an "emergency".[47] The Canadian Protection of Privacy Act 1973-74 gives the power to the Solicitor-General.

Only in the United States, of comparable common law jurisdictions, does there appear to be some doubt as to whether the executive ought to control security related intercepting. In that country the general rule is that the Fourth Amendment to the Bill of Rights prohibits unreasonable searches and seizures, and usually law enforcement officers must obtain a judicial warrant before searching. The landmark decisions of the Supreme Court in 1967 in *Berger* v. *U.S.*[48] and *Katz* v. *U.S.*,[49] made it clear that all wiretaps and other forms of surreptitious electronic surveillance were within the field of investigative activities that ordinarily require prior judicial approval. The President may be able to act without such approval when national security is involved.[50] But there may be a relevant distinction between security matters of a purely domestic nature and those connected with foreign relations. In the former situation the Supreme Court has held that a warrant is required, the case having "no significant connection with a foreign power, its agents or agencies".[51] But, the Court expressly left open the question

43. Ibid., 51.
44. Post p. 158, "Review of the Power".
45. Ibid., 51.
46. Ibid., 31, para. 139.
47. Telephonic Communications (Interception) Act 1960, ss. 6 and 7.
48. 388 U.S. 41 (1967).
49. 389 U.S. 347 (1967).
50. Nelson Rockefeller *Report to the President by the Commission on CIA Activities within the United States* (New York, 1975) 63.
51. *U.S.* v. *U.S. District Court for the Eastern District of Michigan* 407 U.S. 297, 309 (1972).

of whether a significant foreign connection would justify a different result. Some lower courts have held that no warrant is required in such cases.[52] The distinction is supported by the American Bar Association in its 1971 Approved Draft on minimum standards relating to electronic surveillance.[53]

The distinction ought properly to be recognised in New Zealand, especially as the S.I.S. surveillance net is cast so widely over internally "subversive" elements. This area will inevitably overlap with the police sphere of operations, where the courts have an established role in issuing search warrants. Indeed, to some extent the Amendment Act already implies the distinction in separating alternative reasons for the interception in section 4A(1)(a)(i) and (ii). Under subsection (4) only information about warrants issued for the purposes of subsection (1)(a)(i) may be contained in the report to Parliament. The use of the formula in subparagraph (ii) of "gathering foreign intelligence information" implies a foreign relations element contrasting with the "detection of activities prejudicial to security" wording of subparagraph (i), although the latter is wide enough to cover an international situation too.

It should be mentioned that a safeguard similar to that contained in the Australian Telephonic Communications (Interception) Act 1960[54] exists in the requirement under section 4A(1) that the Director make an application in writing and give evidence on oath that the criteria of the subsection are made out before the Minister can issue the warrant. The initiative is thus claimed to be non-political, and the process is described as an upward rather than downward moving power. Section 6 amends the principal Act by providing that the Director shall hold office under a contract of service, apparently to provide an assurance that the position will not become a political appointment. At present the Director is employed on a five year contract — long enough to survive a change of government.

Further, it might be noted that the question of who should have the power to issue warrants does not necessarily present a clear-cut alternative between the executive and the courts. Even if the power were vested in the courts it is unlikely that they would cease to recognise an executive content in the decision. The courts would still accept the Minister's affidavit to the effect that the grounds for issuing the warrant have been made out but that in the public interest they ought not to be disclosed.[55]

D. The Issue and Content of Warrants

The criteria that must, in the Minister's opinion, be satisfied before a warrant may be issued represent a mixture of the grounds used in this context. First, section 4A(1)(a) requires that the interception or seizure should be necessary for the purpose of either subparagraph (i) or (ii).

The wording of paragraph (a) relates closely to that of paragraph (c) of section 4A(1), which requires that "[t]he information is not likely to be obtained by any other means". This represents a departure from the Powles Report draft by substituting "is not likely to" for the recommended "cannot". The formulation used in the United Kingdom by the Home Office to assess applications for warrants from the Security Service is that:[56]

52. Rockefeller Report, op. cit. 53. Supra, n. 35, at 121. 54. S. 6(1).
55. See Lord Atkin in *Liversidge* v. *Anderson* [1942] A.C. 206, 241.
56. Birkett Committee Report, op. cit., 17.

> Normal methods of investigation must have been tried and failed, or must, from the nature of things, be unlikely to succeed if tried.

This implies a preference for "normal methods", but in practical terms the provision in the New Zealand Amendment Act seems to fall within its ambit.

However, the British criteria corresponding to paragraphs (a) and (b) of section 4A(1) are more apparently more restrictive. Under Home Office practice, first there must be a major subversive or espionage activity that is likely to injure the national interest. The Amendment Act in general terms requires only a purpose related to "security", which as has been seen has a wide meaning. Secondly, the requirement under paragraph (b) of the Act that the particular interception should be justified by "[t]he value of the information sought" is a rather looser formula than the British rule that the information must be of direct use in compiling the information that is necessary to the Security Service in carrying out the tasks laid upon it by the state. These distinctions are perhaps most significant in that they are indicative of the general move of the New Zealand law away from the British "defence of the Realm" limitation on the security service task. But neither the British practice nor the New Zealand Amendment Act places any emphasis on the likelihood of obtaining convictions or other terminal results as a criterion for the issue of the warrant. This recognises the on-going intelligence gathering function of the Service.

Like the criteria of issue, the requirements in the Act as to what information must be contained in the warrant are modelled principally upon the corresponding Canadian provisions, which were by and large adopted by the recommended draft in the Powles Report. The general policy basis of section 4A(2), which lays down the series of specifications which the warrant must contain, may be traced back to *Entick* v. *Carrington*[57] and the traditional abhorrence by English courts of general warrants. But by its nature the warrant to intercept communications is difficult to limit by stated specifications. Subsection (2)(b), for example, recognises that the identity of the persons whose communications are to be intercepted may not be known. Telephone tapping or electronic aural surveillance is indiscriminate. In many cases, unlike the situation of the police warrant to search and seize, it will not be known what kind of information is being sought until it has actually been overheard.

The Powles Report stands alone in recommending that any warrant to intercept should have a maximum period of validity of ninety days.[58] The Amendment Act provides under section 4A(2)(d) that the warrant shall "[b]e valid for the period specified therein". The Canadian legislation provides a ninety day limitation in respect of ordinary investigatory warrants to intercept,[59] but in the security area has effectively the same provision as is contained in the Amendment Act.[60]

United Kingdom practice requires no time limit to be stated, but substitutes a system of regular review of outstanding warrants by all the authorities concerned. The Permanent Under-Secretary to the Home Office makes a quarterly review of all such warrants. The Board of Customs and Excise also undertakes a quarterly review of warrants in its area, the Metropolitan Police reviews every week, and

57. Supra. n. 40.
58. Ibid., 60.
59. Protection of Privacy Act 1973-74, s. 2, inserting Part IV.1 into the Criminal Code.
60. S. 16(4)(c) Official Secrets Act R.S. 1970 as inserted by s. 6 Protection of Privacy Act 1973-74.

the Security Service every six months. In the absence of any express statutory time limit such a system might well be appropriate in New Zealand.

The principal reason for the provision in section 4A(3) that the warrant may contain a request to any persons to assist in making the interception or seizure appears to be the inclusion of such persons in the warrant authorisation for the purpose of granting immunity from suit under subsection (5).

Initially, the Bill had contained in clause 4(3)(a) a further provision for inclusion in the warrant of a direction to state servants to give assistance as specified in the warrant. This appeared to raise more sinister implications. Every state servant, it was argued, would become a potential S.I.S. employee, and after much of the early criticism of the Bill had been directed to that paragraph, it was eventually omitted.

E. Review of the Power

Coupled with the vesting in the Minister of the power to issue warrants to intercept is the fact that the courts are both implicitly and expressly excluded by the Amendment Act from reviewing the Minister's exercise of the power. As previously noted the national security area is usually a purely executive domain in which the courts will not intervene. Section 4A(1) as inserted by the Amendment Act implicitly and effectively denies the courts access to a review of the Minister's decision by providing that "the Minister may issue an interception warrant . . . if he is satisfied" that the criteria of the subsection are complied with. His only duty under subsection (1) is to hear the evidence of the Director and be "satisfied" by it. There is nothing to say that his belief need be a reasonable belief. Assuming that the courts could review the issue of the warrant, the only way they could question the decision of the Minister would be to cast doubt on his honest belief that the criteria were present. Falsity of the Director's evidence, whether intended or not, would not invalidate the issue of the warrant if a lack of such honest belief could not be shown in the Minister. In these circumstances section 4A(6)(b), which expressly states that the issue of a warrant shall not be subject to judicial review, seems unnecessary, although it does represent a clear indication of the intention of the legislature.

Subsection (6)(a) also excludes the court's jurisdiction with regard to certain actions done pursuant to a warrant. No civil or criminal proceedings will lie against a person authorised, directed or requested to act or assist by the warrant for "taking any reasonable action necessarily involved in making or assisting to make or attempting to make the interception or seizure". Actions that are "necessarily involved" would appear to cover trespass and breaking and entering in many cases, and theft or conversion in some. The law on this question will likely develop by analogy with that relating to police search warrants.

The only provision in the Act for independent review of the exercise of the power is the requirement that the Minister make an annual report to Parliament under section 4A(5). How effective this kind of check will be is very much open to question. The Minister does not have to report on warrants for the foreign intelligence purpose of subsection (1)(a)(ii), which limitation is a departure from both the Powles draft and the corresponding Canadian parliamentary report

provisions.[61] The report is to relate only to warrants issued under subsection (1)(a)(i), that is, for the purpose of the detection of activities prejudicial to security. Yet subsection (5) provides that the report shall not disclose "information prejudicial to security". One might wonder what information of any significance the report might contain.

Although the Act appears to provide no opportunity for review of the decision to issue the warrant or of actions done pursuant to the warrant other than the report to Parliament, an individual or group suffering damage in other ways because of the interception might be able to involve the general S.I.S. complaints procedure contained in the principal Act. One case where this might be relevant is where the complainant has been injured by an unauthorised disclosure of the intercepted communications.[62]

Unfortunately the appeals procedure is another area where the general provisions of the principal Act are even less satisfactory than the provisions of the Amendment Act. Section 14 of the 1969 Act provides for the appointment of a Commissioner of Security Appeals whose function, under section 17, is to inquire into any complaint made by a citizen of an act or omission by the Service which has "adversely affected" his "career or livelihood". The scope of appeals is thus severely limited. The Commissioner is not empowered to make any decision, but to forward his findings to the complainant and the Minister, and any findings of breach of duty or misconduct of Service employees to the Director under section 21. Under section 22, the Minister may take "such further action as he considers appropriate".

Such an appeals procedure is rather considerably removed from the usual principles of judicial review of executive authority. The Powles Report recommends substantial re-drafting of seven of the eleven sections of the Act concerned with appeals.[63] Atkins describes the present provisions as "minimal paper protections" and as operating to "keep most of the service's mistakes from the public".[64]

Neither the parliamentary report in the Amendment Act, nor the appeal to the Commissioner under the principal Act seem very satisfactory checks on the exercise of the power. But it is also apparent that because of the delicate nature of national security matters they ought not to be subject to court review, although the argument may be made as before that purely domestic security affairs may be distinguished from those having international connotations, and that the former class of cases may be subject to judicial review but not the latter. The American Bar Association makes the same distinction in relation to public disclosure reporting,[65] and in that context the distinction is recognised in the New Zealand Amendment Act when it excludes from the report under section 4A(5) reference to warrants issued for the purpose of section 4A(1)(a)(ii).

61. Cf. Protection of Privacy Act 1973-74 s. 6, inserting s. 16(5) in the Official Secrets Act R.S. 1970.
62. See discussion of "Disclosure and Destruction: Protection for the Individual", post p. 160.
63. Ibid., 83-94.
64. Supra n. 32, 394, 396.
65. Ibid., 121. With reference to foreign intelligence, the American Bar Association considered "that a system envisioning judicial supervision and public disclosure reporting would be unworkable in this area".

F. Disclosure and Destruction: Protection for the Individual?

Section 7 of the Amendment Act, inserting section 12A into the principal Act, prohibits in broad terms the unauthorised disclosure of information concerning an interception under warrant. There are three major elements to section 12A(2). First, it prohibits unauthorised disclosure by a person acting or giving assistance under the authorisation of the warrant. Secondly, the prohibition applies to unauthorised disclosure of the existence of the warrant. Thirdly, it applies to unauthorised disclosure of any information gained when acting pursuant to the warrant.

The latter two elements probably represent twin policy grounds for the inclusion of the section in the Act. The existence of the warrant ought not to be revealed as a matter of administrative expediency, at least while it is still in force. The broader informational prohibition is probably intended as a safeguard for the individual against the kind of situation found in the Marrinan case, which prompted the setting up of the Birkett Committee in the United Kingdom. That affair became a matter of public controversy in 1956 when the Home Office had authorised the tapping of certain telephone conversations in the course of criminal investigations. It then disclosed transcripts of the conversations to the Bar Council, which was inquiring into allegations of misconduct by a barrister. The Birkett Committee concluded that the disclosure had been a mistake, and recommended that there should be no disclosure of information obtained on public grounds by the exercise of the power to intercept to private individuals or bodies, or domestic tribunals of any kind.[66] While the New Zealand Amendment Act appears to extend this prohibition to disclosure within the public service itself, it should be noted that to be caught by section 12A(2), the disclosure must be unauthorised. Therefore any disclosure may in fact be made if it is authorised. Either the warrant, the Minister or the Director may authorise any disclosure, and there is nothing to say that such disclosure should not contain information "prejudicial to security" as does section 4A(5). It is even doubtful whether there is any need for section 12A at all. The situation envisaged by section 12A(2) seems to be largely covered by section 12A(1) already. All that section 12A(2) adds to section 12A(1) is the inclusion in the class of persons who may not make unauthorised disclosure, of persons other than S.I.S. employees or former employees who are authorised to act under the warrant. The entire section is probably wholly covered by the Official Secrets Act 1951.[67] Perhaps section 12A covers a point of some doubt as to whether the Official Secrets Act 1951 does in fact catch all of the relevant classes of information.

Further, although section 12A(2) may be intended to provide a safeguard for the individual, it gives him no remedy. The penalty under subsection 4 is clearly a deterrent to unauthorised disclosure, but what redress does the individual have when a disclosure (whether authorised or not) is actually made and injury results? A person under surveillance lives with a constant threat of having personal communications divulged to the world at large. That occurrence alone might be claimed by the proponents of a general privacy law to constitute a cause of action

66. Ibid., 23.
67. S. 6(1) and (3). See also Public Service Regulations 1964, regs. 42, 43, and Post Office Staff Regulations 1951, reg. 80.

which ought to be recognised by the law.[68] As the law stands the individual might have a cause of action in defamation if he could show damage to reputation and overcome defences of justification and qualified privilege. It may be noted that such an action is not affected by the provision for immunity from suit in section 4A(6)(a), which applies only to actions "necessarily involved in making or assisting to make or attempting to make the interception or seizure". The other possible remedy for the individual is again in the S.I.S. appeals procedure in the principal Act, with all the limitations that entails. The claim may not be as harsh as might be first supposed that the only effect of section 12A will be to prevent disclosures by S.I.S. officers of illegal actions by the Service, or of political manipulation, similar to the revelations which have occurred in the United States and which have resulted in reforms in the operations of the C.I.A.[69] The possibility of such disclosure has been described as one of the only real forms of control on the activities of the S.I.S.[70] The lessening or even the abrogation of this possibility might have been justified in the interests of a meaningful protection for the individual, but this is not the effect of the Amendment Act in its present form.

Similarly, it may be questioned whether the late addition of section 5 of the Amendment Act, inserting section 4B into the principal Act, will assist the individual to any great extent. That section provides principally for the destruction, as soon as practicable, of any record of information obtained under warrant "except so far as the information recorded therein relates directly or indirectly to the detection of activities prejudicial to security or comprises foreign intelligence information essential to security". It is one of the few safeguards in the Act which attaches an enforcement provision. Clearly, it goes some way to answering the threat to the individual from the inherently indiscriminate nature of interception techniques. But the obvious questions are when does information not relate to security and whether the right person is making that decision. Again, breach of section 4B gives no remedy to the individual.

III. THE RELATIONSHIP BETWEEN THE AMENDMENT AND THE PRE-EXISTING LAW

The much publicised criticisms of the new legislation by Mr Michael Minogue M.P.[71] are central to the question of how the Amendment Act will fit within the existing framework of the law. Mr Minogue's main concern was that the whole area of surveillance and privacy should be examined, instead of which he saw the Act as an example of people going off at a tangent and looking at only a small part of the problem. This approach he described as "piecemeal". The Act does not deal either with the conduct of the police,[72] or with the general law in relation to the use of surveillance equipment or its sale.

68. Such an action is recognised in the United States: see W. Prosser *Handbook of the Law of Torts* (4th ed., St. Paul, Minn., 1971) 802 ff.
69. See Rockefeller Report, 1975, supra n. 50.
70. *Salient* Victoria University student newspaper, September 19, 1977.
71. *Evening Post* Wellington, September 9, 1977.
72. For a fuller discussion of the relationship between the Act and the functions of the police see G. Crowder "The N.Z.S.I.S. Amendment Bill, 1977" unpublished LL.M. research paper, Victoria University of Wellington, October 3, 1977.

The significance of the latter point may be tested by asking the question, what is the legal position when an unauthorised interception occurs, that is, if the S.I..S acts without a warrant, or acts pursuant to a warrant which does not conform to the provisions of the Act, or where anybody else makes an unauthorised interception? The answer is that section 4 of the Amendment provides no penalty for non-compliance with its provisions. Putting aside any possible challenge to the issue of the warrant, a warrant that does not comply with the specifications of section 4A(2) might be called "invalid", but what is this going to mean in practice? It may or may not avoid the warrant. Assuming that a warrant is void, or that an interception has been made without a warrant, the legal position will presumably return to that subsisting prior to the passing of the Amendment Act — except that unauthorised disclosure of the information gained raises a separate issue under section 12A. The conclusion compelled by these observations is that Mr Minogue's criticism is well founded. The area covered by the Amendment Act is only a comparatively small part of a much greater problem that is left mostly unsolved. This very fact was recognised by Sir Guy Powles in his Report when he emphasised that his recommendation on interception legislation was necessarily restricted to the terms of his current inquiry, and that it might have to be considered in the context of police powers and pending privacy and related legislation.[73] The Government does not seem to have taken this point at all.

As the Powles Report points out,[74] only Canada of comparable common law jurisdictions has comprehensive legislation covering the whole interception field. The Protection of Privacy Act 1973-74 was clearly the model for the recommended draft, but only as it related to the security area relevant to the Report. The security provisions were taken out of the context of the overall scheme of the Act, which when taken into account gives the final position a rather different appearance than that which is represented by the New Zealand law as it stands in the shadow of the Amendment Act.

It is submitted that the general scheme of the Canadian Act is a useful indicator of the direction in which the New Zealand legislation ought to be developing. The Act not only deals with the whole issue, but in broad terms approaches it from quite the opposite angle to that of the New Zealand Amendment Act. Thus, the Act amends the Criminal Code of Canada to provide an across-the-board prohibition of wilful interception by any person of private communications, attaching an indictable offence punishable by imprisonment for up to five years.[75] "Intercept" is defined broadly, and "private communication" is wide enough to include postal, telephonic and eavesdropping situations. To the general rule are added certain tightly defined exceptions,[76] including consent, accidental or necessary interception by official communications workers, and particularly authorisation. In cases not related to security, authorisation can be obtained only by a written application to a senior or specially appointed judge, which must be signed by the Attorney-General, or the Solicitor-General or their agents, and accompanied by a sworn affidavit setting out defined grounds for the application.[77] The judge must be satisfied by another set of criteria, including one that the authorisation serves the best interests of justice.[78] A private communication which has been

73. Ibid., 59-60.
74. Ibid., 59.
75. S. 178.11(1).
76. S. 178.11(2).
77. S. 178.12.
78. S. 178.13.

unlawfully intercepted is generally inadmissible in evidence.[79] The Solicitor-General is required to make an annual report setting out a considerable amount of information relevant to authorised interceptions.[80] Further, the Crown Liability Act R.S. 1970 is amended to provide for a special action against the Crown for interceptions made unlawfully by its servants.[81] The remedy includes compensation for loss or damage suffered, and punitive damages of up to $5,000. The Official Secrets Act R.S. 1970 is amended to provide the security exception.[82]

The American Bar Association's 1971 Approved Draft[83] recommends the same basic scheme of general prohibition attaching criminal and civil sanctions with closely defined public exceptions. There is also some question of whether a basic prohibition should go further than the Canadian legislation and restrict sales or even outlaw unauthorised possession of interception equipment, as appears to be suggested by Mr Minogue and Professor Palmer.[84] The American Bar Association's Approved Draft similarly recommends the criminal prohibition of the intentional possession, sale, distribution or manufacture of a device the design of which makes it primarily useful for the surreptitious overhearing or recording of private conversations. It was felt by the drafting committee that prohibition of objectionable conduct alone was insufficient to protect the privacy interest.[85]

The New Zealand law does not compare favourably with the Canadian and United States material. In those jurisdictions the emphasis is consistently placed on the protection of the individual from interceptions which are not strictly necessary. By contrast the interception provisions of the 1977 Amendment Act may be described as an isolated statutory affirmation of the existence of a dubious executive power which has survived largely by means of the obscurity surrounding it. Throughout its genesis, dating from the Powles Report recommendations, the major concern it has represented has been that of securing the legality of S.I.S. operations. It is now discovered, on re-examination of the law, that wide powers to intercept already existed in the Post Office Act 1959. Therefore, it might be said that the Amendment Act in fact assists civil liberties by narrowing the pre-existing powers by means of statutory safeguards which did not exist before. It is hard to say what weight should be given to that argument. But the evidence of the Powles Report and the scheme of the Act itself tend to suggest that the Government was disturbed by the possibility that the S.I.S. did not have legal powers to intercept communications, and intended that priority should be given to the establishment of such powers. Hence, while the Canadian legislation begins with a prohibition of interception, the Amendment Act is concerned first with making interception lawful.

Wherever the emphasis in the Act was intended to lie, it is clear that it does not come down in fact on the side of civil liberties. Inevitably, a certain amount of trust must be reposed in those who exercise the power, but that trust must be tied to an understanding of how far the power runs and to an understanding

79. S. 178.16 Cf *Kuruma* v. *R.* [1955] A.C. 197, *R.* v. *Maqsud Ali* [1966] 1 Q.B. 688.
80. S. 178.22.
81. S. 4, amending s. 7.2 of the Crown Liability Act R.S. 1970.
82. Ss. 5 and 6.
83. Supra., n. 35.
84. "Privacy and the Law" [1975] N.Z.L.J. 747, 755-6.
85. Ibid., 106-108.

that it is subject to controls sufficient to protect the legitimate privacy interests of the individuals. The particular inadequacy of the latter element in this Act casts a pall of doubt over the whole area of interception. The relevant sections contain few provisions for enforcement and none for remedies for the individual. The matter remains in the hands of the executive at almost every stage. It is practically unreviewable by the courts, and the main review mechanism of the parliamentary report is of questionable value. The wide powers under the Post Office Act 1959 have not been repealed, and so continue in force independently. The Amendment Act will do very little to promote the interests of the individual.