ANALYSIS

1997, No. 98

An Act to amend the Telecommunications Act 1987

[*1 December 1997*

BE IT ENACTED by the Parliament of New Zealand as follows:

1. Short Title and commencement—(1) This Act may be cited as the Telecommunications Amendment Act 1997, and is part of the Telecommunications Act 1987 ("the principal Act").

(2) This Act comes into force on 1 February 1998.

2. Interpretation—Section 2 (1) of the principal Act is amended by inserting, in their appropriate alphabetical order, the following definitions:

" 'Call associated data', in relation to a telecommunication,—

"(a) Means dialling or signalling information—

"(i) That is generated as a result of the making of the telecommunication (whether or not the telecommunication is sent or received successfully); and

"(ii) That identifies the origin, direction, destination, or termination of the telecommunication; and

"(b) Without limiting the generality of paragraph (a), includes any of the following information:

"(i) The number from which the telecommunication originates:

"(ii) The number to which the telecommunication is sent:

"(iii) If the telecommunication is diverted from one number to another number, those numbers:

"(iv) The time at which the telecommunication is sent:

"(v) The duration of the telecommunication:

"(vi) If the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network; but

"(c) Does not include the content of the telecommunication:

" 'Call data warrant' means a warrant issued under section 10B:

" 'Content', in relation to a telecommunication,—

"(a) Means the data, image, sound, writing, or other information that the sender of the telecommunication intends to convey to its recipient; and

"(b) For the avoidance of doubt, and without limiting paragraph (a), includes information (such as passwords, personal identification numbers, and other similar information) sent or generated in the course of using any device or service (such as electronic mail) that uses telecommunications for its operation:

" 'Telephone analyser' means any device—

"(a) That can be connected to any part of a network, or to any line, apparatus, or equipment connected to any part of a network; and

"(b) That is designed to record or enable the recording of call associated data, but cannot record or monitor, or enable the recording or monitoring of, the content of any telecommunication:".

3. Interference with network—Section 6 of the principal Act is amended by inserting after subsection (2), as subsections (2A) and (2B), the following subsections:

"(2A) A network operator must not agree to the connection, by or on behalf of any person, of a telephone analyser to any part of a network, or to any line, apparatus, or equipment connected to any part of a network, owned or operated by that network operator, unless the connection is for 1 or more of the following purposes:

"(a) To enable a person to which the network operator provides telecommunications services to monitor telecommunications between that person and other persons:

"(b) The maintenance of the network:

"(c) The detection, investigation, or prosecution of any offence against section 5B or section 8 or section 8A.

"(2B) Sections 10B to 10F affect the operation of subsections (1) and (2A)."

4. New heading and sections inserted—The principal Act is amended by inserting, after section 10, the following heading and sections:

"Call Data Warrants

"10A. **Application for call data warrant**—(1) Any member of the Police or any Customs officer may apply to a District Court Judge for the issue of a call data warrant.

"(2) An application must be made in writing and on oath.

"10B. **Issue of call data warrant**—(1) On an application made under section 10A, a District Court Judge may issue a warrant under this section if he or she is satisfied that there is reasonable ground for believing—

"(a) That an offence punishable by imprisonment has been, or is being, or is likely to be committed; and

"(b) That evidence relevant to the investigation of the offence will be obtained—

"(i) By the use of a telephone analyser; or

"(ii) From call associated data provided by a network operator.

"(2) A District Court Judge may issue a warrant under this section—

"(a) In respect of a person who is suspected of having committed, or of committing, or of being likely to commit, the offence to which the warrant relates; or

"(b) In respect of someone other than the suspected offender, in any case where obtaining call associated data in respect of that person may lead to the identification of the suspected offender.

"(3) A warrant issued under this section must comply with the requirements of section 10I.

"10C. **Effect of warrant**—(1) A call data warrant authorises any member of the Police or (as the case requires) any Customs officer to do the following things:

"(a) To connect a telephone analyser, or to have a telephone analyser connected, to any part of a network, or to any line, apparatus, or equipment connected to any part of a network, that is used, or (where applicable) is suspected of being used, by the person named in the warrant:

"(b) To monitor the telephone analyser, or to have the telephone analyser monitored:

"(c) To require the network operator whose network is subject to the warrant to supply, to a member of the Police or (as the case requires) a Customs officer, call associated data in respect of the person named in the warrant.

"(2) Where subsection (1) (c) applies, and for as long as the warrant remains in force, the network operator must supply the call associated data—

"(a) At such intervals, or at such times; and

"(b) In such manner, or in such form, or both,—

as the member of the Police or (as the case requires) the Customs officer requires.

"(3) Before requiring a network operator to supply call associated data under subsection (1) (c), the member of the Police or (as the case requires) the Customs officer must consult with the network operator to ensure that compliance with the terms of the requirement will not unreasonably interfere with the normal operation of the operator's network.

"(4) Except as provided in section 10D, a call data warrant does not authorise any person to enter any premises or place without the consent of the owner or occupier of those premises or that place.

"10D. **Network operator required to assist in execution of warrant**—A network operator that owns or operates a network that is subject to a call data warrant must provide such assistance as is necessary to enable any person who is authorised by the warrant to connect a telephone analyser—

"(a) To locate the part of the network to which the analyser is to be connected (including, where necessary, any relevant line, apparatus, or equipment); and

"(b) To connect the analyser in accordance with the warrant.

"10E. **Failure to comply with call data warrant**—Every network operator commits an offence and is liable on summary conviction to a fine not exceeding $2,000 who,—

"(a) Fails, without reasonable excuse, to comply with the requirements of section 10D; or

"(b) Having been required under a call data warrant to supply call associated data,—

"(i) Fails, without reasonable excuse, to comply with that requirement (including any requirement imposed under section 10C (2)); or

"(ii) Knowingly supplies information that is false or misleading in purported compliance with that requirement.

"10F. **Telephone analysers must comply with technical requirements**—(1) A telephone analyser must not be connected under a call data warrant to any part of a network unless—

"(a) The analyser is approved (or is of a kind approved) for connection to that network by the network operator that owns or operates the network; and

"(b) The analyser is connected to the network in the manner (if any) approved by that network operator.

"(2) A network operator may—

"(a) Refuse to approve a telephone analyser or a kind of telephone analyser for the purposes of subsection (1) (a); or

"(b) Determine the manner in which telephone analysers are connected to the operator's network for the purposes of subsection (1) (b)—

only if it is necessary, and only to the extent necessary, to prevent interference with or damage to the network.

"10G. **Existence of call data warrant not to be disclosed**—(1) A network operator whose network is, or has been, subject to a call data warrant must not disclose the existence or operation of the warrant to any person except—

"(a) The Commissioner of Police or a member of the Police who is authorised by the Commissioner to receive the information; or

"(b) The Comptroller of Customs or a Customs officer who is authorised by the Comptroller to receive the information; or

"(c) An employee or agent of the network operator, for the purpose of ensuring compliance with the warrant; or

"(d) A lawyer, for the purpose of obtaining legal advice or representation in relation to the warrant.

"(2) A person referred to in paragraph (a) or paragraph (b) of subsection (1) to whom disclosure of the existence or operation of a call data warrant has been made must not disclose the existence or operation of the warrant except to another person of the kind referred to in that subsection, for the purpose of the performance of the first-mentioned person's duties.

"(3) A person referred to in paragraph (c) of subsection (1) to whom disclosure of the existence or operation of a call data warrant has been made must not disclose the existence or operation of the warrant except to another person of the kind referred to in that subsection, for the purpose of ensuring that the warrant is complied with or obtaining legal advice or representation in relation to the warrant.

"(4) A person referred to in paragraph (d) of subsection (1) to whom disclosure of the existence or operation of a call data warrant has been made must not disclose the existence or operation of the warrant except to a person of the kind referred to in that subsection, for the purpose of giving legal advice or making representations in relation to the warrant.

"(5) Nothing in subsections (1) to (4) prevents the disclosure of the existence or operation of a call data warrant—

"(a) In connection with, or in the course of, proceedings before a court; or

"(b) Under section 10R; or

"(c) By the Police or the New Zealand Customs Service, where disclosure is made in response to a request made under the Official Information Act 1982 or the Privacy Act 1993.

Cf. 1991, No. 120, s. 80

"10H. **Offences**—(1) Every person commits an offence who knowingly contravenes any of subsections (1) to (4) of section 10G.

"(2) Every person who commits an offence against subsection (1) is liable on summary conviction,—

"(a) In the case of an individual, to a fine not exceeding $2,000:

"(b) In the case of a body corporate, to a fine not exceeding $5,000.

"(3) Every person commits an offence who discloses any information in contravention of any of subsections (1) to (4) of section 10G, in any case where that person—

"(a) Knows that the person is not legally authorised to disclose the information; and

"(b) Discloses the information either—

"(i) For the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person; or

"(ii) With intent to prejudice any investigation into the commission or possible commission of any offence.

"(4) Every person who commits an offence against subsection (3) is liable on summary conviction,—

"(a) In the case of an individual, to imprisonment for a term not exceeding 6 months or a fine not exceeding $5,000:

"(b) In the case of a body corporate, to a fine not exceeding $10,000.

Cf. 1991, No. 120, s. 81; 1996, No. 9, s. 22 (5), (6)

"10I. **Form and content of warrant**—(1) A call data warrant must be in the prescribed form.

"(2) A call data warrant must be directed—

"(a) To members of the Police generally; or

"(b) To Customs officers generally.

"(3) A call data warrant must contain the following particulars:

"(a) The offence or offences in respect of which the warrant is issued:

"(b) The kind of telecommunication in respect of which call associated data is authorised to be obtained:

"(c) The name and address of the person in respect of whom call associated data is authorised to be obtained:

"(d) If known, the telephone number to which the warrant relates:

"(e) If that telephone number is not known, the premises or place in respect of which a telephone analyser may be used, being premises or a place used or suspected

of being used, by the person to whom the warrant relates, for the purposes of, or for any purpose relating to, an offence in respect of which the warrant is issued:

"(f) The period for which the warrant is to be in force.

"10J. **Duration of warrant**—Unless renewed under section 10K, a call data warrant expires at the end of the period (not exceeding 30 days) specified in the warrant.

"10K. **Renewal of warrant**—(1) Any member of the Police or any Customs officer may apply to a District Court Judge for the renewal of a call data warrant that has not expired.

"(2) An application for the renewal of a call data warrant must be in writing and on oath.

"(3) On an application made under this section, a District Court Judge may renew a call data warrant if he or she is satisfied that the circumstances specified in section 10B (1) still apply.

"(4) A call data warrant may be renewed under this section for a period of not more than 30 days.

"(5) The period for which a call data warrant is renewed must be endorsed on the warrant, and (unless renewed again) the warrant expires at the end of that period.

"(6) A call data warrant may be renewed 1 or more times under this section.

"10L. **Security of applications for warrants**—(1) As soon as a District Court Judge has determined an application for a call data warrant or for the renewal of a call data warrant, all documents relating to the application (except the warrant itself) must be dealt with in accordance with subsection (2).

"(2) Where this section applies, the Registrar of the relevant District Court must—

"(a) Place the documents in a packet; and

"(b) Seal the packet; and

"(c) Keep the packet in safe custody, subject to sections 10M to 10Q.

Cf. 1961, No. 43, s. 312H (1); 1987, No. 167, s. 4

"10M. **Restriction on production of documents relating to application**—(1) Regardless of any enactment or rule of law or any rules of court entitling any party to any proceedings to demand the production of any documents, no such party is entitled to demand the production of any documents held in safe custody under section 10L.

"(2) Subsection (1) is subject to sections 10N to 10Q.

Cf. 1961, No. 43, s. 312H (2); 1987, No. 167, s. 4

"10N. **Application for production of documents**—(1) Any party to any proceedings who requires the production of any document held in safe custody under section 10L must (except in a case to which section 10P applies) apply in writing to the Registrar who holds the document.

"(2) On receiving notification under subsection (1), the Registrar must, without delay, notify—

"(a) The senior Police officer in the district, in any case where the document is or relates to an application for a call data warrant sought by a member of the Police:

"(b) The senior Customs officer in the district, in any case where the document is or relates to an application for a call data warrant sought by a Customs officer.

"(3) If, within 3 days after notice is given under subsection (2), the officer to whom the notice is given notifies the Registrar in writing that the officer intends to oppose the production of the document, the Registrar must refer the application for production to a District Court Judge.

"(4) Where the officer does not notify his or her opposition to the Registrar within the period specified in subsection (3), the Registrar must produce the document to the party applying for production.

Cf. 1961, No. 43, s. 312H (3)-(5); 1987, No. 167, s. 4

"10O. **Application referred to Judge**—(1) If, under section 10N (3), a Registrar refers an application for production to a District Court Judge, the application must be dealt with in accordance with this section.

"(2) Both the person applying for production of the document and the member of the Police or Customs officer opposing production must be given an opportunity to be heard.

"(3) If the District Court Judge is satisfied that information in any document whose production is sought identifies, or is likely to lead to the identification of,—

"(a) A person who gave information to the Police, or to the New Zealand Customs Service; or

"(b) Any member of the Police, or any Customs officer, whose identity was concealed for the purpose of any relevant investigation and has not been subsequently revealed,—

the Judge may, if the Judge believes it in the public interest to do so, order that the whole or any specified part of the document not be produced.

"(4) If the Judge does not make an order under subsection (3), the Judge must order the production of the document to the party requesting it.

Cf. 1961, No. 43, s. 312H (6)-(8); 1987, No. 167, s. 4

"10P. **Request for production made in course of proceedings**—(1) If—

"(a) A request for the production of any document kept in safe custody under section 10L is made in the course of any proceedings presided over by a District Court Judge or a Judge of the High Court; and

"(b) The request is opposed,—

that Judge must adjudicate on the matter as if it had been referred under section 10N (3) to a District Court Judge, and section 10O applies accordingly with any necessary modifications.

"(2) If—

"(a) A request for the production of any document kept in safe custody under section 10L is made in the course of any other proceedings; and

"(b) The request is opposed,—

the presiding judicial officer must, without delay, refer the matter to a District Court Judge for adjudication under section 10O.

Cf. 1961, No. 43, s. 312H (9)-(10); 1987, No. 167, s. 4

"10Q. **Judge entitled to inspect any relevant document**—Regardless of anything in any of sections 10L to 10P, any Judge who is presiding over any proceedings in which the issue of a call data warrant is in issue is entitled to inspect any relevant document held under section 10L.

Cf. 1961, No. 43, s. 312H (11); 1987, No. 167, s. 4

"10R. **Reports to Parliament on call data warrants**—(1) The Commissioner of Police must include in every annual report prepared by the Commissioner for the purposes of section 65 of the Police Act 1958 the following information in respect of the period under review:

"(a) The number of applications made by members of the Police for call data warrants:

"(b) The number of applications made under section 10K by members of the Police for renewals of call data warrants:

"(c) The number of applications referred to in each of paragraphs (a) and (b) that were granted, and the number that were refused:

"(d) The average duration of call data warrants (including renewals) issued to members of the Police.

"(2) The Comptroller of Customs must include in his or her annual report under section 30 of the State Sector Act 1988 the following information in respect of the period under review:

"(a) The number of applications made by Customs officers for call data warrants:

"(b) The number of applications made under section 10K by Customs officers for renewals of call data warrants:

"(c) The number of applications referred to in each of paragraphs (a) and (b) that were granted, and the number that were refused:

"(d) The average duration of call data warrants (including renewals) issued to Customs officers.

"10s. **Regulations**—The Governor-General may from time to time, by Order in Council, make regulations prescribing the form of call data warrants."

This Act is administered in the Ministry of Commerce.