



Telecommunications Information Privacy Code 2003

*Incorporating
Amendments No 3, No 4, No 5, No 6 and No 7*

Privacy Commissioner
Te Mana Matapono Matatapu

NEW ZEALAND

This version of the code applies from 7 May 2020 and incorporates the changes made by Amendments No 3, No 4, No 5, No 6 and No 7.

Telecommunications Information Privacy Code 2003

CONTENTS

Page

Issuance.....	2
---------------	---

PART 1: PRELIMINARY

1. Title.....	3
2. Commencement.....	3
2A. Review.....	3
3. Interpretation.....	3
4. Application of Code.....	7

PART 2: TELECOMMUNICATIONS INFORMATION PRIVACY RULES

5. Telecommunications information privacy rules.....	8
<i>Rule 1: Purpose of Collection of Telecommunications information.....</i>	<i>8</i>
<i>Rule 2: Source of Telecommunications Information.....</i>	<i>9</i>
<i>Rule 3: Collection of Telecommunications Information from Individual.....</i>	<i>11</i>
<i>Rule 4: Manner of Collection of Telecommunications Information.....</i>	<i>13</i>
<i>Rule 5: Storage and Security of Telecommunications Information.....</i>	<i>14</i>
<i>Rule 6: Access to Telecommunications Information.....</i>	<i>15</i>
<i>Rule 7: Correction of Telecommunications Information.....</i>	<i>17</i>
<i>Rule 8: Accuracy etc of Telecommunications Information to be checked before use.....</i>	<i>18</i>
<i>Rule 9: Retention of Telecommunications Information.....</i>	<i>19</i>
<i>Rule 10: Limits on Use of Telecommunications Information.....</i>	<i>20</i>
<i>Rule 11: Limits on Disclosure of Telecommunications Information.....</i>	<i>22</i>
<i>Rule 12: Unique Identifiers.....</i>	<i>25</i>

SCHEDULES

<i>Schedule 1: Complaints of breach of code.....</i>	<i>26</i>
<i>Schedule 2: Directories and directory enquiry services.....</i>	<i>27</i>
<i>Schedule 3: Caller Line Information Presentation.....</i>	<i>29</i>
<i>Schedule 4: Emergency location information.....</i>	<i>30</i>

APPENDIX

Appendix 1: Telecommunications Information Privacy Code 2003 Amendment No 2 (Temporary).....	37
Legislative history.....	40

This version of the code includes various notes which are set out in italics. This material is not part of the code but is included to assist users of the code. Reference must always be made to the rules or clauses themselves.

Part 1: Preliminary

1. Title

This code of practice may be referred to as the [Telecommunications Information Privacy Code 2003].

Note: Amendment No 3 corrected an error in the name of the code.

2. Commencement

(1) Subject to subclause (2), this code will come into force on 1 November 2003.

(2) Clauses 3(e) and (f) of Schedule 2 will come into force on 1 April 2005.

Note: Amendment No 3 commenced on 1 August 2004.

[2A. Review

The Commissioner will review the operation of Schedule 4 from time to time, and no later than 1 May 2022.]

Note: Clause 2A. was inserted by Amendment No 7.

3. Interpretation

In this code:

Act means the Privacy Act 1993

Note: Used in clause 5; rules 2(2)(k), 6(5), 7(6), 10(1)(i), 11(1)(o); Schedule 1.

call means a telephone call

Note: Used in definition of “CLIP”, CMS; rules 10(2), 10(3) 11(1)(e); Schedule 3.

call associated data has the same meaning as in [section 3(1) of the Telecommunications (Interception Capability and Security) Act 2013]

Note: The Telecommunications (Interception Capability and Security) Act 2013 defines the term as follows:

“call associated data, in relation to a telecommunication:

- (a) means 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) includes, without limitation, 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.”*

Note: Amendment No 4 amended the definition of call associated data.

Note: Used in definition of “traffic information”; rule 4(2).

CLIP means Calling Line Identification Presentation, being technology which enables an answerer (or a device receiving a call) to identify the calling number, name of the subscriber and time and date of the call, prior to answering the call or in the course of receiving a message

Note: Used in rule 11(1)(n); Schedule 3. CLIP is sometimes known as “caller ID” or “caller display”.

CMS means call management service

Note: Used in rules 3(4)(f), 10(1)(h), 11(1)(l). Examples of CMS include CLIP, call trace and call forwarding.

direct marketing means:

- (a) the offering of goods or services; or
- (b) the advertising of the availability of goods or services; or
- (c) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political, or other purposes,

by means of:

- (d) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or
- (e) calls made to specific persons by name,

but does not include:

- (f) information sent by a telecommunications agency to a subscriber advising of a rate or service change to an existing service; or
- (g) information sent by a telecommunications agency to a subscriber advising of alternative services, or charging plans, which may be of interest to the subscriber as a result of a rate or service change to an existing service.

Note: The definition is derived from a definition of “direct marketing” in section 9(2) of the Act but with the inclusion of exceptions (f) and (g).

Note: Used in rules 10(1)(b) and 10(2).

directory means a list of the names and contact details of subscribers, whether in printed or electronic form, available to the public or a section of the public

Note: Used in definitions of “directory enquiry agency”, “directory enquiry service”, “directory publisher” and “reverse search facility”; rules 2(3)(a), 10(3)(c), 11(1)(m); Schedule 2. The telephone book is an example of a directory. A private directory, such as the internal directory of a large company, is not a “directory” for the purposes of the code as it is not available to the public.

directory enquiry agency means an agency which provides a directory enquiry service

Note: Used in clause 4(2); rules 2(3), 11(1)(m); Schedule 2.

directory enquiry service means a service which provides subscriber contact details on request

Note: Used in definitions of “directory enquiry agency” and “reverse search facility”; rules 2(3)(a), 11(1)(m); Schedule 2.

directory publisher means an agency which prepares or publishes a directory

Note: Used in clause 4(2); rules 2(3), 11(1)(m); Schedule 2.

Note: Amendment No 3 removed the definition of “foreign telecommunications law”.

Internet service provider means a service provider which provides access to the Internet

Note: This definition does not capture agencies which are purely content providers.

linked traffic information means traffic information which is linked to, or matched with, subscriber information by a telecommunications agency

Note: Used in rule 6(4).

network has the same meaning as in section 5 of the Telecommunications Act 2001

Note: The Telecommunications Act defines the term to mean “a system comprising telecommunication links to permit telecommunication”. That Act also defines “telecommunication links” to mean “any line, radio frequency or other medium used for telecommunication”.

Note: Used in definitions of “seamless”, “telecommunications service provider or TSO provider”; rules 2(2)(d), 2(2)(i), 3(4)(b), 4(4), 10(1)(c), 11(1)(f), 11(1)(m); Schedule 3.

Network operator has the same meaning as in section 5 of the Telecommunications Act 2001

Note: The Telecommunications Act defines network operator to mean any person declared by the Minister to be a network operator, except for Chorus and Telecom which are declared to be network operators by the Act directly. Network operators are those agencies which are in the business of providing:

- *facilities for telecommunications between 10 or more other persons that enable at least 10 of those persons to communicate with each other; or*
- *facilities for broadcasting to 500 or more persons that enable programmes to be transmitted along a line or lines to such persons. (Telecommunications Act 2001, section 103).*

Note: Used in clause 4(2); rules 2(2)(i), 2(3), 4(2), 10(1)(h), 10(2), 11(1)(m); Schedules 2 and 4.

reverse search facility means a directory which is arranged, or a directory enquiry service which is operated, for the purpose of enabling an individual’s name or address to be obtained by reference to a telephone number alone or an address alone, or a combination of telephone number and address

Note: Used in Schedule 2.

seamless means the provision of a telecommunications service in such a way that it is not evident to the subscriber that a particular service may be or has been delivered by different networks, equipment or providers

Note: Used in rules 10(1)(h), 11(1)(l).

subscriber means an individual who has entered into a contract with a telecommunications agency for the supply of a telecommunications service

Note: Used in definition of “CLIP”, “linked call”, “subscriber information”; and extensively in rules 1, 2, 10 and 11; Schedules 2 and 3.

subscriber information means personal information about a subscriber which is obtained by a telecommunications agency when that subscriber subscribes to a telecommunications service or during the term of such a contractual relationship

Note: Used in the definition of reverse search facility”; clause 4(1); rule 2(3); Schedule 2.

telecommunication has the same meaning as in section 5 of the Telecommunications Act 2001

Note: The Telecommunications Act defines the term as follows:

“telecommunication –

- (a) means the conveyance by electromagnetic means from one device to another of any encrypted or non-encrypted sign, signal, impulse, writing, image, sound, instruction, information, or intelligence of any nature, whether for the information of any person using the device or not; and
- (b) for the purposes of subpart 2 of part 4, includes any conveyance that constitutes broadcasting; but
- (c) for all other purposes, does not include any conveyance that constitutes broadcasting”

telecommunications agency means an agency of a class listed in subclause 4(2)

telecommunications information means information listed in subclause 4(1)

telecommunications service has the same meaning as in section 5 of the Telecommunications Act 2001

Note: The Telecommunications Act defines the term to mean “any goods, services, equipment and facilities that enable or facilitate telecommunications.” Used in definition of “seamless”, “subscriber”, “subscriber information”.

[telecommunications service obligation provider or TSO provider] has the same meaning as in section 5 of the Telecommunications Act 2001

Note: The Telecommunications Act defines the term to mean “a provider of a telecommunications service under a TSO instrument”. A “TSO instrument” is a telecommunications service obligation instrument declared or deemed under that Act.

Note: Amendment No 4 replaced the term telecommunications service provider to reflect changes made to the Telecommunications Act 2001. The definition of the term remains the same.

Note: Used in clause 4(2).

traffic information means call associated data and any other dialling or signalling information generated as the result of making a telecommunication (whether or not the telecommunication is sent or received successfully).

Note: Traffic information does not include the content of a call. In addition to call associated data it would include, for example, location information generated by cellphone use (i.e. cell location).

Note: Used in clause 4(1); rules 2(2)(h) and 10(2).

Note: Terms defined generally in the Privacy Act take the same meaning in the code – Interpretation Act 1999, section 34. Terms defined in section 2 of the Privacy Act and used in this code include: action, agency, collect, commissioner, correct, individual, individual concerned, information privacy principle, personal information, public sector agency, publicly available information, publicly available publication, unique identifier, working day.

4. Application of code

- (1) This code applies to information about an identifiable individual that is:
- (a) subscriber information;
 - (b) traffic information;
 - (c) the content of a telecommunication[;];
 - (d) additionally, for the purposes of Schedule 4, location information as defined in clause 1 of Schedule 4].

Note: Clause 4(1)(d) was inserted by Amendment No 7. Schedule 4 permits location agencies to collect, use and share location information for the purpose of responding to an emergency.

Note: The code covers personal information collected or held by telecommunications agencies relating to individuals who subscribe to, or use, the telephone or other telecommunications services. The information privacy principles in the Privacy Act continue to apply to other personal information which is not listed here. Staff records are an example of personal information held by a telecommunications agency which is not covered by the code.

Note: This information is collectively referred to in the code as “telecommunications information” – see clause 3.

- (2) This code applies to the following classes of agency:
- (a) a network operator;
 - (b) a telecommunications service obligation provider or TSO provider;
 - (c) a directory publisher;
 - (d) a directory enquiry agency;
 - (e) an Internet service provider;
 - (f) a call centre which provides call centre services on contract to another agency;
 - (g) a mobile telephone retailer[;];
 - (h) additionally, for the purposes of Schedule 4:
 - (i) the relevant government agency;
 - (ii) an emergency service provider].

Note: Clause 2(b) was amended by Amendment No 4.

Note: Clause 2(h) was inserted by Amendment No 5. “Relevant government agency” and “emergency service provider” are defined in clause 1 of Schedule 4.

Note: These agencies are collectively referred to as “telecommunications agencies” in the code – see clause 3.

Part 2: Telecommunications Information Privacy Rules

5. Telecommunications information privacy rules

In accordance with the Act, the following rules modify the application of the information privacy principles, prescribe how the principles are to be applied or complied with and apply some principles without modification:

Rule 1 Purpose of Collection of Telecommunications Information

Telecommunications information must not be collected by a telecommunications agency unless:

- (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and
- (b) the collection of the information is necessary for that purpose.

Note: Except where it is itself a party to a communication, a telecommunications agency will rarely have a lawful purpose to collect the content of any telecommunication. Indeed, it is unlawful to intercept the content of a private communication in most cases (Crimes Act 1961, Part 9A). There are some limited exceptional circumstances relevant to telecommunications agencies (e.g. where acting pursuant to an interception warrant to assist the Police or SIS). Employees of network operators can, in the course of their duties, intercept telecommunications for maintenance purposes but it is an offence for an employee of a network operator to use or disclose information so obtained for unauthorised purposes – Crimes Act 1961, sections 216B and 216C).

Note: An action is not in breach of this rule if it is authorised or required by or under law- Privacy Act, section 7(4). Furthermore, this rule and rules 2-4 apply only to the collection of information on or after the commencement of this code.

Rule 2 Source of Telecommunications Information

- (1) Where a telecommunications agency collects telecommunications information, it must collect the information directly from the individual concerned.
- (2) It is not necessary for a telecommunications agency to comply with subrule (1) if the agency believes on reasonable grounds:
- (a) that the information is publicly available information;

Note: "Publicly available information" is defined in the Act to include information in a "publicly available publication" (which is also defined).

- (b) that the individual concerned authorises the collection of the information from another source;
- (c) that non-compliance would not prejudice the interests of the individual concerned;
- (d) that non-compliance is necessary:
- (i) to avoid prejudice to the maintenance of the law by any public sector agency including the prevention, detection, investigation, prosecution and punishment of offences;
- [(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);
- (iii) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;]

Note: A denial-of-service attack is an example of an action which may compromise network integrity.

Note: Rule 2(2)(d) was amended by Amendment No 3.

- (e) that compliance would prejudice the purpose of collection;
- (f) that compliance is not reasonably practicable in the circumstances of the particular case;
- (g) that the information:
- (i) will not be used in a form in which the individual concerned is identified; or
- (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;
- (h) that the information is traffic information;
- (i) that the collection is an essential element of service provision or the interconnection, wholesaling or similar arrangements between network operators;
- (j) that the information is necessary to deal with a service or billing enquiry and the collection is from:
- (i) a member of the subscriber's household; or
- (ii) a representative of a business subscriber;

Note: Para (j) covers the position where collection is made in the course of a service or billing enquiry. A typical domestic service or billing enquiry may be made orally from the subscriber's own telephone. See rule 11(1)(k) in relation to the release of information in these circumstances.

- (k) that the information is subscriber information and the collection is from a network operator or Internet service provider or any other agency providing telecommunication service to persons outside that agency:
 - (i) by a directory publisher for the purpose of inclusion in a directory in accordance with the requirements of Schedule 2;
 - (ii) by a directory enquiry agency for the purpose of making the information available through a directory enquiry service in accordance with the requirements of Schedule 2; or

Note: See rule 11(1)(m) which is the corresponding provision concerning disclosure of subscriber information for inclusion in a directory or by means of a directory enquiry service. Such information may usually only be disclosed with the authorisation of the individual concerned.

- (l) that the collection is in accordance with an authority granted under section 54 of the Act.

Note: An action is not in breach of this rule if it is authorised or required by or under law Privacy Act, section 7(4). This rule applies only to the collection of information on or after commencement of this code.

Rule 3
Collection of Telecommunications Information from Individual

- (1) Where a telecommunications agency collects telecommunications information directly from the individual concerned, the agency must take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:
- (a) the fact that the information is being collected;
 - (b) the purpose for which the information is being collected;
 - (c) the intended recipients of the information;
 - (d) the name and address of:
 - (i) the agency that is collecting the information; and
 - (ii) the agency that will hold the information;
 - (e) if the collection of the information is authorised or required by or under law:
 - (i) the particular law by or under which the collection is authorised or required; and
 - (ii) whether or not the supply of the information by that individual is voluntary or mandatory;
 - (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
 - (g) the rights of access to, and correction of, telecommunications information provided by rules 6 and 7.

Note: Additional explanations may be required if information collected is to be used or disclosed for direct marketing or to be disclosed in a directory or to a directory enquiry service – see rules 10 and 11 and Schedule 2.

- (2) The steps referred to in subrule (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after it is collected.
- (3) A telecommunications agency is not required to take the steps referred to in subrule (1) in relation to the collection of telecommunications information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.
- (4) It is not necessary for a telecommunications agency to comply with subrule (1) if it believes, on reasonable grounds:
- (a) that non-compliance would not prejudice the interests of the individual concerned;
 - (b) that non-compliance is necessary:
 - (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences;
 - [(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
 - (iii) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;]

Note: Rule 3(4)(b) was amended by Amendment No 3.

- (c) that compliance would prejudice the purposes of collection;
- (d) that compliance is not reasonably practicable in the circumstances of the particular case;
- (e) that the information will not be used in a form in which the individual concerned is identified; or

(f) that the collection is for the purposes of interconnection or the delivery of a CMS.

[(5) Where a network operator participates in the emergency location information system in accordance with Schedule 4, it must ensure that additional steps required by clause 4 of Schedule 4 are taken to meet specific transparency obligations in relation to the system.]

Note: Rule 5(5) was inserted by Amendment No 7. Clause 4 of Schedule 4 requires all location agencies, including network operators, to make general information about the emergency location information system available to the public. Network operators might achieve this by providing a link on their website to general information made available by the relevant government agency.

Note: An action is not a breach of this rule if it is authorised or required by or under law – Privacy Act, section 7(4). This rule applies only to collection of information after the commencement of this code.

Rule 4
Manner of Collection of Telecommunications Information

- (1) Telecommunications information must not be collected by a telecommunications agency:
 - (a) by unlawful means; or
 - (b) by means that, in the circumstances of the case:
 - (i) are unfair; or
 - (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.
- (2) Subject to section 107 of the Telecommunications Act 2001, a network operator or Internet service provider may monitor the call associated data of an individual where necessary for the purpose of investigating an action that may threaten network security or integrity.

Note: Section 107 of the Telecommunications Act prohibits the connection of a telephone analyser (i.e. a device to record call associated data) except:

- (a) *to enable a subscriber to monitor telecommunications between that subscriber and another person (i.e. CLIP);*
- (b) *to maintain the network;*
- (c) *to detect, investigate and prosecute certain offences against the Act (misuse of telephone device, indecent telephone calls for pecuniary gain).*

Note: An action is not a breach of this rule if it is authorised or required by or under law – Privacy Act section 7(4). This rule applies only to the collection of information after the commencement of this code.

Rule 5
Storage and Security of Telecommunications Information

- (1) A telecommunications agency that holds telecommunications information must ensure:
- (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:
 - (i) loss;
 - (ii) access, use, modification, or disclosure, except with the authority of the agency; and
 - (iii) other misuse; and
 - (b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the telecommunications agency, everything reasonably within the power of that agency is done to prevent unauthorised use or unauthorised disclosure of the information.

[(1A) Where a network operator discloses emergency [...] location information in accordance with Schedule 4, it must ensure that additional steps required by clause 6 of Schedule 4 are taken to safeguard that information.]

Note: Subrule (1A) was inserted by Amendment No 5. Clause 6 of Schedule 4 requires particular steps to be taken to safeguard emergency caller location information.

Note: The word "caller" was omitted from subrule (1A) by Amendment No 7.

- (2) This rule applies to telecommunications information obtained before or after the commencement of this code.

Note: An action is not a breach of this rule if it is authorised or required by or under law – Privacy Act, section 7(4).

Rule 6
Access to Telecommunications Information by Individual Concerned

- (1) Where a telecommunications agency holds telecommunications information in such a way that it can readily be retrieved, the individual concerned is entitled:
- (a) to obtain from the agency confirmation of whether or not it holds such information; and
 - (b) to have access to that information.

Note: Section 55(a) of the Act makes it clear that nothing in rule 6 applies to personal information in the course of transmission by telecommunication.

- (2) Where, in accordance with subrule (1)(b), an individual is given access to telecommunications information, the individual must be advised that, under rule 7, the individual may request the correction of that information.
- (3) When a telecommunications agency refuses a request under subrule (1), it must advise the individual of the complaints process available under Schedule 1.

Note: This obligation is in addition to the statutory requirement to give the individual information concerning the right to complain to the Privacy Commissioner, to seek an investigation and a review of the refusal – Privacy Act, section 44(b).

- (4) A network operator (other than a public sector agency) may refuse to disclose to a requester linked traffic information which may reveal the identity of another individual or subscriber.

Note: This provision makes it clear that information can be withheld (i.e. that a caller's number or subscriber information may be deleted from information released). Such information can often be withheld anyway under section 29(1)(a) of the Act where the disclosure "would involve the unwarranted disclosure of the affairs of another individual ...". However, it is debatable as to whether access to details of a single call will always constitute disclosure of the "personal affairs" of another.

Note: This reason for refusing to disclose information is in addition to, and does not limit, other reasons for refusal in Part 4 of the Act – see rule 6(5)(a). Accordingly, an agency can sometimes also withhold other types of subscriber information which is not "linked traffic information". For example, where disclosure might endanger someone or be an unwarranted disclosure of the affairs of another individual.

Note: Even if entitled to refuse access to such information, there will be cases where a telecommunications agency will appropriately disclose details requested. Such disclosures need to conform to rule 11. Examples would include disclosure to a subscriber to resolve a billing dispute (allowed under rule 11(1)(e) or (k)), or where a requester has been subject to harassment and the agency is satisfied that the disclosure of details is necessary to enable the requester to file civil proceedings under the Harassment Act 1997 (rule 11(1)(f)(v)). In cases of harassment or other criminal behaviour an agency may also, of course, disclose information to the Police.

- (5) The application of subrules (1) and (2) is subject to the provisions of:
- (a) Part 4 of the Act (which sets out reasons for refusing access to information); and
 - (b) Part 5 of the Act (which sets out procedural provisions relating to access to information).

Note: See also subrules (3) and (4) which also concern procedures and a reason for refusing access.

- (6) This rule applies to telecommunications information obtained before or after the commencement of this code.

Note: This rule is subject to provisions in enactments which authorise or require personal information to be made available or Acts which prohibit, restrict, or regulate the availability of personal information – Privacy Act, section 7(1) and (2). Under section 7(3) it is also subject to certain regulations which prohibit, restrict or regulate the availability of personal information.

Rule 7
Correction of Telecommunications Information

- (1) Where a telecommunications agency holds telecommunications information, the individual concerned is entitled:
- (a) to request correction of the information; and
 - (b) to request that there be attached to the information a statement of the correction sought but not made.

Note: Section 55(a) of the Act makes it clear that nothing in rule 7 applies to information in the course of transmission by telecommunication.

- (2) Where a telecommunications agency holds telecommunications information it must, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, it is accurate, up to date, complete and not misleading.
- (3) Where a telecommunications agency that holds telecommunications information is not willing to correct the information in accordance with a request by the individual concerned, it must, if so requested, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by the individual of the correction sought.
- (4) Where a telecommunications agency has taken steps under subrules (2) or (3), it must, if reasonably practicable, inform each person or body or agency to whom the information has been disclosed of those steps.
- (5) Where a telecommunications agency receives a request made under subrule (1), it must:
- (a) inform the individual concerned of the action taken as a result of the request; and
 - (b) if it refuses the request, advise the individual of the complaints process available under Schedule 1.

Note: The obligation in paragraph (b) is in addition to the statutory requirement to give the individual information concerning the right to complain to the Privacy Commissioner, to seek an investigation and a review of the refusal – Privacy Act, section 44(b).

- (6) The application of this rule is subject to the provisions of Part 5 of the Act (which sets out procedural provisions relating to correction of information).
- (7) This rule applies to telecommunications information obtained before or after the commencement of this code.

Note: An action is not a breach of this rule if it is authorised or required by or under law - Privacy Act, section 7(4).

Rule 8

Accuracy etc of Telecommunications Information to be checked before use

- (1) A telecommunications agency that holds telecommunications information must not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.
- (2) This rule applies to telecommunications information obtained before or after the commencement of this code.

Note: An action is not in breach of this rule if it is authorised or required by or under law – Privacy Act, section 7(4).

Rule 9
Retention of Telecommunications Information

- (1) A telecommunications agency that holds telecommunications information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.
- (2) This rule applies to telecommunications information obtained before or after the commencement of this code.

Note: An action is not a breach of this rule if it is authorised or required by or under law – Privacy Act section 7(4).

Rule 10
Limits on use of Telecommunications Information

- (1) A telecommunications agency that holds telecommunications information that was obtained in connection with one purpose must not use the information for any other purpose unless the agency believes on reasonable grounds:
- (a) that the source of the information is a publicly available publication [and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information];

Note: Rule 10(1)(a) was amended by Amendment No 4.

- (b) that the use of the information for that other purpose is authorised by the individual concerned, provided that if the other purpose is for direct marketing the individual has been advised that he or she may withdraw such authorisation at any time;
- (c) that non-compliance is necessary:
 - (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;
 - [(ii) for the protection of the public revenue;
 - (iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
 - (iv) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;]

Note: Rule 10(1)(c) was amended by Amendment No 3.

- (d) that the use of the information for that other purpose is necessary to prevent or lessen a serious [...] threat to:
 - (i) public health or public safety; or
 - (ii) the life or health of the individual concerned or another individual;

Note: The term "serious threat" is defined in section 2 of the Act as follows:

"serious threat, for the purposes of principle 10(d) or 11(f), means a threat having regards to all of the following:

- (a) the likelihood of the threat being realised; and*
- (b) the severity of the consequences if the threat is realised; and*
- (c) the time at which the threat may be realised"*

Note: the words "and imminent" were omitted from rule 10(1)(d) by Amendment No 4.

- (e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained;
- (f) that the information:
 - (i) is used in a form in which the individual concerned is not identified; or
 - (ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;
- (g) that the use of the information is necessary to investigate a complaint concerning a malicious or nuisance telecommunication and to take appropriate action;
- (h) that the use of the information is necessary for:
 - (i) the provision of a seamless telecommunications service to subscribers;

- (ii) the development or supply of any broadband, intelligent, interactive or multimedia services or other forms of telecommunications service;
 - (iii) the provision of a CMS; or
 - (iv) the purpose of interconnection, wholesaling or similar arrangements between network operators; or
 - (i) that the use of the information is in accordance with an authority granted under section 54 of the Act.
- (2) A telecommunications agency must not use traffic information obtained as a result of interconnection, wholesaling or similar arrangements between network operators for the purposes of direct marketing to an individual who is not a subscriber of the agency without the authorisation of that individual.
- (3) This rule does not apply to telecommunications information obtained before 1 July 1993.

Note: An action is not a breach of this rule if it is authorised or required by or under law – Privacy Act, section 7(4).

Rule 11
Limits on Disclosure of Telecommunications Information

- (1) A telecommunications agency that holds telecommunications information must not disclose the information unless the agency believes, on reasonable grounds:
- (a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained;
 - (b) that the source of the information is a publicly available publication [and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information];

Note: Rule 11(1)(b) was amended by Amendment No 4.

Note: A “directory” is an example of a “publicly available publication”.

- (c) that the disclosure is to the individual concerned;
- (d) that the disclosure is authorised by the individual concerned;
- (e) that the disclosure is to a subscriber for billing purposes and the information identifies the details of a call for which a specific charge is made, such as a toll call, collect call, or an 0800 or 0900 (or equivalent) call;

Note: Details of an 0800 call may appear on the statement of the subscriber being called whereas details of a 0900 call will appear on the calling subscriber’s statement.

- (f) that non-compliance is necessary:
 - (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences;
 - [(ii) for the enforcement of a law imposing a pecuniary penalty;
 - (iii) for the protection of the public revenue;
 - (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
 - (v) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;]

Note: Rule 11(1)(f) was amended by Amendment No 3.

- (g) that the disclosure of the information is necessary to prevent or lessen a serious [...] threat to:
 - (i) public health or public safety; or
 - (ii) the life or health of the individual concerned or another individual;

Note: The term “serious threat” is defined in section 2 of the Act as follows:

“serious threat, for the purposes of principle 10(d) or 11(f), means a threat having regards to all of the following:

- (a) *the likelihood of the threat being realised; and*
- (b) *the severity of the consequences if the threat is realised; and*
- (c) *the time at which the threat may be realised”*

Note: the words “and imminent” were omitted from rule 11(1)(g) by Amendment No 4.

- [(ga) except where the disclosure of the information may be sought in accordance with a business records direction under Part 5(4) of the Intelligence and Security Act 2017, that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions;]

Note: See Intelligence and Security Act 2017, ss 10-16, for the functions of intelligence and security agencies.

Note: Privacy Act, s 7(1) and (2), provides that rule 11 does not derogate from any provision in another enactment that requires or regulates the disclosure of personal information. Intelligence and Security Act 2017, Part 5(4), which enables an intelligence and security agency to obtain business records of telecommunications network operators is such a provision and therefore it prevails over the code. Rule 11(1)(ga) provides for disclosures outside the scope of Part 5(4).

Note: Intelligence and Security Act, section 122(3) provides that the Director-General of an intelligence and security agency may certify that he or she believes on reasonable grounds that the disclosure is necessary, for the purpose of enabling an agency to decide whether to disclose the information.

(h) that the disclosure is necessary to enable emergency services to respond to a potential threat to the life or health of the individual concerned or another individual;

[(ha) that the disclosure is [to the relevant government agency for the purposes] of Schedule 4;]

Note: Rule 11(1)(ha) was inserted by Amendment No 5 and further amended by Amendment No 7. Rule 11(1)(ha) provides network operators with the lawful basis to disclose location information to the relevant government agency for the purposes of Schedule 4.

(i) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern;

(j) that the information:

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;

(k) that the disclosure is necessary to deal with a service or billing enquiry and the disclosure is to:

(i) a member of a subscriber's household; or

(ii) a representative of a business subscriber;

who appear to be acting on behalf of the subscriber;

(l) that the disclosure of the information is necessary for:

(i) the provision of a seamless telecommunications service to subscribers;

(ii) the development or supply of any broadband, intelligent, interactive or multimedia services or other forms of telecommunications service;

(iii) the provision of a CMS; or

(iv) interconnection, wholesaling or similar arrangements between network operators;

Note: CLIP is a type of CMS and is subject to the more particular regime in paragraph (n) and Schedule 3.

(m) that the information is information enabling a subscriber to be identified and contacted and the disclosure is by inclusion in a directory or directory enquiry service, or by disclosure to a directory publisher or directory enquiry agency for inclusion in a directory or directory enquiry service, and the disclosure is authorised by the subscriber concerned and in accordance with the requirements of Schedule 2;

(n) that the disclosure is by means of CLIP and is in accordance with the requirements of Schedule 3; or

(o) that the disclosure of the information is in accordance with an authority granted under section 54 of the Act.

(2) This rule applies to telecommunications information obtained before or after the commencement of this code.

Note: Nothing in this rule derogates from any provision in an enactment which authorises or requires information to be made available, prohibits or restricts the availability of information or regulates the manner in which information may be obtained or made available – Privacy Act, section 7.

Rule 12
Unique Identifiers

- (1) A telecommunications agency must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.
- (2) A telecommunications agency must not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless:
 - (a) both agencies are associated persons within the meaning of [subpart YB of the Income Tax Act 2007]; or
 - (b) it is permitted by subrule (5).

Note: Rule 12(2)(a) was amended by Amendment No 4.

- (3) A telecommunications agency that assigns unique identifiers to individuals must take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.
- (4) A telecommunications agency must not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.
- (5) Notwithstanding subrules (2) and (3), a telecommunications agency may identify a telephone installation or an individual associated with that installation by reference to a number or identifier generated or assigned by another telecommunications agency where that is necessary for interconnection, wholesaling or similar arrangements between telecommunications agencies or between a telecommunications agency and another agency providing telecommunications service.

Note: Telecommunications agencies use a variety of identifiers such as automatic number generation (ANI), telephone or directory number, portable number, ISDN mobile subscriber identifier.

- (6) Subrules (1), (2), (3) and (5) do not apply in relation to the assignment of unique identifiers before the commencement of this code.
- (7) Subrule (4) applies to any unique identifier, whether assigned before or after the commencement of this code.

Note: An action is not a breach of this rule if it is authorised or required by or under law – Privacy Act, section 7(4).

Schedule 1

Complaints of breach of code

1. Each telecommunications agency must designate a person or persons to deal with complaints alleging a breach of this code and facilitate the fair, simple, speedy and efficient resolution of complaints.
2. Each telecommunications agency must have a complaints procedure which provides that:
 - (a) when a complaint of a breach of this code is received:
 - (i) the complaint is acknowledged within 5 working days of receipt, unless it has been resolved to the satisfaction of the complainant within that period;
 - (ii) the complainant is informed of any relevant internal and external complaints procedures; and
 - (iii) the complaint and the actions of the agency regarding that complaint are documented;
 - (b) within 10 working days of acknowledging the complaint, the agency must:
 - (i) decide whether it:
 - (A) accepts that the complaint is justified;
 - (B) not accept that the complaint is justified; or
 - (ii) if it decides that more time is needed to investigate the complaint:
 - (A) determine how much additional time is needed; and
 - (B) if that additional time is more than 20 working days, inform the complainant of that determination and of the reasons for it; and
 - (c) as soon as practicable after the agency decides whether or not it accepts that a complaint is justified, it must inform the complainant of:
 - (i) the reasons for the decision;
 - (ii) any actions the agency proposes to take; and
 - (iii) the right to complain to the Privacy Commissioner.
3. Nothing in this Schedule limits or restricts any provision of the Act.

Note: Any person may complain directly to the Privacy Commissioner about an interference with his or her privacy (or complain on someone else's behalf). However, there are advantages for both the complainant and the agency if the complainant first approaches the agency and asks for the matter to be considered. The Schedule imposes standards on internal complaints handling with the intention that most complaints be sorted out internally without Privacy Commissioner involvement.

Note: Failure by a telecommunications agency to comply with Schedule 1 is deemed by the Act to be a breach of an information privacy principle even though that failure would not otherwise be a breach of any principle (Privacy Act, section 53(b)). If some harm has resulted from that failure it may constitute an interference with privacy for which the Act provides remedies (Privacy Act, section 66).

Schedule 2

Directories and directory enquiry services

1. Any disclosure made under rule 11(1)(m) must be in accordance with:
 - (a) the agency's policy notified generally or to the subscriber concerned;

Note: See clauses 6 and 7 below.

- (b) any authorisation given by the subscriber; and
 - (c) clauses 2, 3, 7, 8 and 9.

Note: See also rule 2(2)(k).

2. A network operator or Internet service provider must not make it a condition of supply of telecommunications services that subscriber information be published in a directory or be made available through a directory enquiries service.

3. Unless the subscriber concerned explicitly authorises to the contrary, a directory publisher or directory enquiry agency must arrange a directory or operate a directory enquiry service so that:

- (a) [to search for a subscriber's telephone number:
 - (i) using a directory enquiry service, an enquirer is required to provide both the approximate name and approximate address of the subscriber being sought;
 - (ii) using an electronic directory, a searcher is required to provide the approximate name of the subscriber being sought;]

Note: Clause 3(a) was substituted by Amendment No 3.

- (b) where a subscriber's name, address and telephone number is published or displayed in printed or electronic form it is ordered alphabetically by the name of the subscriber concerned;
 - (c) where a subscriber's name, address and telephone number is published or displayed in a directory it is not ordered to allow searches by address only;
 - (d) subscriber information is not disclosed by way of a reverse search facility;
 - (e) where a subscriber has expressed a preference for his or her name to appear in the directory in a certain form, the name is not published in any other form;

Note: For example, subscribers may prefer to be listed using initials and surname, first name and surname, or the form of name by which they are most commonly known. The directory publisher may adopt policies as to acceptable entries (e.g. in relation to length, decency or to avoid confusion) and may refuse to publish non-conforming entries or names that differ entirely from the subscriber's name. However, the agency may not publish a name in a form that differs from an expressed preference without the individual's authorisation.

- (f) where a subscriber requests that only part of his or her address is included in a directory, his or her full address is not published.

Note: Clause 3 is modelled upon clause 13 of the Code of Practice on Telecommunications Directory Information Covering the Fair Processing of Personal Data, UK, 1998.

4. Clauses 3(a), (b), (c) and (d) do not apply in relation to a business subscriber.

Note: The code applies only to telecommunications information about individuals and not to information solely about corporate bodies (such as companies and incorporated societies). The business subscribers to which this clause refers are therefore individuals who are business subscribers (e.g. sole traders or some professionals).

5. Notwithstanding clauses 3(e) and (f), a telecommunications agency is not required to seek explicit authorisation from an existing subscriber as to the form in which that subscriber's name or address is to appear in a directory (including a reprinted or re-issued directory) or a directory enquiry service, but must act upon any request received.
6. For the purposes of clause 5, an **existing subscriber** means a subscriber who has, [as at 1 April 2005], authorised a telecommunications agency to include his or her details in a published or compiled directory.

Note: Clause 6 was amended by Amendment No 3.

7. Where a telecommunications agency discloses subscriber information to a directory agency or a directory enquiry agency for the purposes of inclusion in a directory or directory enquiry service, the agency must do everything reasonably within its power to ensure that the directory publisher or directory enquiry agency will comply with the requirements of this code in relation to the publication or release of the subscriber information.
8. Where an agency intends to seek explicit authorisation from a subscriber for a practice that would otherwise be contrary to clause 3, it must:
 - (a) notify the subscriber concerned directly of the agency's policy and the available options before obtaining the authorisation;
 - (b) advise the subscriber that it is not mandatory for the information to be disclosed in the directory or directory enquiry service; and
 - (c) inform the subscriber that the authorisation may in the future be withdrawn and explain how this may be done.
9. A telecommunications agency must take such steps as are, in the circumstances, reasonable to ensure that subscribers are aware of the agency's practices in relation to directories and directory enquiry services and of the options available concerning the fact and form of publication, release or withholding of subscriber details in full or in part.
- [10. Without limiting clause 9, a telecommunications agency that publishes a directory on the Internet must:
 - (a) take such steps as are, in the circumstances, reasonable to ensure that affected subscribers are aware that information about them is published in this manner and the implications for the accessibility of the information by other people (for example, any significant differences from the way in which the information may otherwise be made available in non-electronic directories);
 - (b) promptly act to remove information relating to a subscriber from the Internet directory where that subscriber withdraws his or her authorisation for inclusion.]

Note: Clause 10 was inserted by amendment No 3.

Schedule 3

Caller line information presentation

1. A telecommunications agency may disclose telecommunications information by means of CLIP, provided that:
 - (a) subscribers are given the option to block the display of calling line identity on a per-line basis for both incoming and outgoing calls;
 - (b) callers are given the means to block the display of calling line identity on a per-call basis for outbound calls; and
 - (c) the agency takes reasonable steps to ensure that:
 - (i) subscribers are made aware of the option to have per-line blocking; and
 - (ii) users of the network are made aware of the ability to utilise per-call blocking;
 - (d) simple means are available for:
 - (i) obtaining per-line blocking;
 - (ii) exercising per-call blocking; and
 - (iii) ascertaining whether an outgoing line is blocked; and
 - (e) the option to obtain per-line blocking, and the means to obtain per-call blocking and to ascertain whether an outgoing line is blocked, are made available free of charge.

Note: Blocking prevents the identification of the calling line to the ultimate recipient of the call. Some information will necessarily be transmitted to intermediaries (i.e. between network operators) as is allowed for in rule 11(1)(l)(iii).

2. A telecommunications agency may override any block applied pursuant to clauses 1(a) or (b) if the call is [to the 111 emergency call service (including a call to any other number that connects to that service)].

Note: Clause (2) was amended by Amendment No 5.

3. A telecommunications agency is not required to provide the options in clauses 1(a) and (b) in respect of a particular subscriber's line where it believes, on reasonable grounds, that:
 - (a) the line is used for direct marketing purposes; or
 - (b) the line has been misused for the purpose of disturbing, annoying or irritating any person,and the agency advises the subscriber that blocking will not be, or is no longer to be, provided on that line.

Note: The exceptions in clause 3 provide a discretion to a telecommunications agency to withhold per line or per-call blocking where a particular line is used for telemarketing or has been misused. It does not oblige agencies to withhold those options.

4. A telecommunications agency is not required to provide the options and means referred to in clauses 1(a) and (b) where the availability of an answer-back function is inherent in the nature of the service being provided to the subscriber concerned.

Schedule 4

Emergency location information

Schedule 4 enables the disclosure of emergency [...] location information (“[ELI]”) by network operators to emergency service providers, and the collection and use of [ELI] by emergency service providers, for the purpose of establishing the location of an individual who has made an emergency call, in order to facilitate a response to that call[; or to prevent or lessen a serious threat to an individual’s life or health].

The Schedule regulates location information which is automatically generated [...] when making an emergency call. [It also regulates the use of technology that enables the collection of location information about cellular devices in the absence of an emergency call from the individual concerned, where this is necessary to prevent or lessen a serious threat to individual life or health.]

The Schedule limits the collection, retention, use and disclosure of [ELI] to ensure that the sharing and use of this information is at all times connected with responding to an emergency [...].

This Schedule applies only to location agencies, as defined in clause 1.

1. Interpretation

In this Schedule:

[cellular device] means a telecommunication device capable of connecting to a cellular network]

Note: The definition of cellular device was inserted by Amendment No 7. Cellular device includes a mobile phone, or any other device fitted with a SIM or eSIM. Telecommunication device is also defined.

[Device Location Information (DLI)] means location information that is:

- (a) derived from a DLI source; and
- (b) not generated by an emergency call

DLI source means:

- (a) a cellular device; or
- (b) in relation to a cellular device, a network operator]

Note: The definitions of device location information and DLI source were inserted by Amendment No 7.

emergency call means any telecommunication from a [telecommunication] device to a specified emergency number

Note: The definition of emergency call was amended by Amendment No 7.

[...]

Note: The definition of emergency caller was omitted by Amendment No 7, as this definition is no longer used in Schedule 4.

Emergency Caller Location Information (ECLI) means [location information] that is:

- (a) derived from an ECLI source; and
- (b) generated by an emergency call

Note: The definition of ECLI was amended by Amendment No 7.

ECLI source means:

- (a) a [telecommunication] device enabled automatically to send ECLI to the [Emergency Location Information System (ELIS)] when an emergency call is made; or
- (b) [in relation to a telecommunication device,] a network operator

Note: the definition of ECLI source was amended by Amendment No 7.

[Emergency Location Information (ELI)] means:

- (a) DLI;
- (b) ECLI]

Note: The definition of emergency location information was inserted by Amendment No 7.

[Emergency Location Information System (ELIS)] means the system which receives and processes [ELI] and makes [ELI] available to emergency service providers for the permitted primary purpose and permitted secondary purpose

Note: The definition of ELIS was amended by Amendment No 7. The ELIS is operated by the relevant government agency, which is defined below.

emergency service provider means:

- (a) New Zealand Police;
- (b) [Fire and Emergency New Zealand];
- (c) The Priory in NZ of the Most Venerable Order of the Hospital of St John of Jerusalem (St John);
- (d) Wellington Free Ambulance Service (Incorporated);
- [(da) New Zealand Search and Rescue;
- (db) Maritime New Zealand;]
- (e) any other agency authorised by the relevant government agency under clause 2 to receive [ELI] from the [ELIS]

Note: The definition of emergency service provider was amended by Amendment No 7.

location agency means:

- (a) an emergency service provider;
- (b) a network operator;
- (c) the relevant government agency

[location information] means personal information indicating the approximate geographical position of a device, which may include the latitude, longitude, altitude and direction of travel of that device]

Note: The definition of location information was inserted by Amendment No 7.

[permitted primary purpose] means:

- (a) in relation to ECLI, to enable an emergency service provider to facilitate a response to an emergency call; or
- (b) in relation to DLI, to enable an emergency service provider to prevent or lessen a serious threat to the life or health of the individual concerned or another individual]

Note: The definition of permitted primary purpose was replaced by Amendment No 7. This definition now includes the collection, use and disclosure of DLI in limited situations where it is necessary to prevent or lessen a serious threat.

permitted secondary purpose means the following purposes that are directly related to the permitted primary purpose:

- (a) maintaining a record of the information used to establish the location of an emergency [...] by an emergency service provider; and
- (b) monitoring and auditing the operation of the [ELIS] by the relevant government agency

Note: The definition of permitted secondary purpose was amended by Amendment No 7.

Note: The permitted primary and secondary purposes restrict the use of ELI and the ELIS. An agency may use personal information sourced from outside the ELIS for other purposes where permitted by law (refer clause 3(4)).

relevant government agency means the government agency responsible for the [ELIS]

Note: The definition of relevant government agency was amended by Amendment No 7. At the date Amendment No 7 commenced, the relevant government agency was the Ministry of Business, Innovation and Employment.

[serious threat] has the same meaning as in section 2(1) of the Act]

Note: The definition of serious threat inserted by Amendment No 7.

specified emergency number means 111 or any other emergency number, agreed by the location agencies from time to time, that connects to the 111 emergency call service

[telecommunication device—

- (a) means any terminal device capable of being used for transmitting or receiving a telecommunication over a network; and
- (b) includes a cellular device].

Note: The definition of telecommunication device was inserted by Amendment No 7. Cellular device is also defined.

2. Additional agencies authorised to receive [ELI] from the [ELIS]

For the purposes of paragraph (e) of the definition of emergency service provider, the relevant government agency may[, after consulting the Commissioner,] authorise an agency to receive [ELI] from the [ELIS] where that agency:

- (a) provides emergency services to the public; and
- (b) requires [ELI] from the [ELIS] for the permitted primary purpose.

[...]

Note: Clause 2(1) was amended, and clause 2(2) was omitted, by Amendment No 7.

Note: Before authorising an agency under clause 2, the relevant government agency is required by clause 7(1) to seek and obtain an assurance that the new agency will take the steps required by clause 6 to safeguard the ELI it receives.

3. [Collection, use, disclosure and accuracy of ELI]

- (1) A location agency may collect, use or disclose [ELI] if it believes on reasonable grounds that:

- (a) the collection, use or disclosure is [necessary] for a permitted primary purpose or permitted secondary purpose; and
- (b) in the case of a disclosure – the disclosure is to another location agency.

Note: Clause 3(1) was amended by Amendment No 7.

- (2) The relevant government agency may collect [ELI] in compliance with subclause (1)(a) either:
 - (a) [directly from the relevant telecommunication device]; or
 - (b) from the relevant network operator.

Note: Clause 3(2), which was amended by Amendment No 7, permits the relevant government agency – as the agency responsible for the ELIS – to collect ELI directly from a device or from a network operator. In either case, consent of the individual concerned is not required.

- [(2A) New Zealand Search and Rescue, Maritime New Zealand, or any agency authorised under clause 2 to receive ELI, must not collect ELI directly from the relevant government agency.

Note: Clause 3(2A) was inserted by Amendment No 7, to limit the agencies that may have direct access to the ELIS. Only Police, Fire and Ambulance may initiate location requests via ELIS.

- (2B) Before collecting, using or disclosing DLI in relation to a cellular device, an emergency service provider must take all reasonable steps to ensure that the device relates to the individual whose location is necessary for the purpose of responding to the serious threat.

Note: Clause 3(2B) was inserted by Amendment No 7, to ensure that reasonable steps are taken to connect a device to the relevant individual.

- (2C) Where an emergency service provider collects ELI, it must ensure that the frequency and duration of the collection is limited to that which is necessary for the permitted primary purpose.]

Note: Clause 3(2C) was inserted by Amendment No 7, to reflect the requirements of rule 1 of the Code and principle 1 of the Act, to limit the collection of personal information to that which is necessary for a lawful purpose.

- (3) A location agency may combine [ELI] with other information – such as aggregated geolocation information – in order to improve the accuracy of [ELI] for the permitted primary purpose.
- (4) A network operator or emergency service provider is restricted by this clause in its collection, use or disclosure of [ELI] only to the extent that the information is sourced from the [ELIS].

Note: Network operators and emergency service providers may collect or generate location information about emergency callers in other ways as permitted by the code or Privacy Act. This Schedule regulates only the way location agencies may use location information derived from the LAS system.

Note: Clauses 3(3) and 3(4) were amended by Amendment No 7.

Note: Clause 3 does not affect any action that is authorised or required by an enactment – Privacy Act 1993, section 7.

[3A. Notice of collection

- (1) An emergency service provider, or the relevant government agency on its behalf, must, as soon as reasonably practicable after collecting DLI pursuant to clause 3(1)(a), notify the individual concerned of:
 - (a) the date and time the information was collected;
 - (b) the type of information collected;
 - (c) the duration of the collection; and
 - (d) the purpose for the collection.
- (2) An emergency service provider is not required to take the steps referred to in subclause (1) if it believes, on reasonable grounds, that doing so would be likely to prejudice the physical or mental health of the individual concerned or another individual.
- (3) Within 7 days of making a decision under subclause (2), an emergency service provider must:
 - (a) review that decision to determine whether subclause (2) still applies; and
 - (b) if subclause (2) no longer applies, take the steps referred to in subclause (1).
- (4) Subject to the general transparency requirements set out at clause 4, a location agency is not required to notify an individual of the collection of ECLI.]

Note: Clause 3A was inserted by Amendment No 7. Clause 3A(2) recognises that there will be circumstances in which notifying an individual that location information has been collected could in itself increase the likelihood of harm to that individual or another individual. Clause 3A(4) carries over clause 4(3), which was omitted by Amendment No 7, and reflects that the collection of ECLI is less intrusive than the collection of DLI.

4. General duty of transparency

- (1) Location agencies should apply a general policy of openness and transparency in respect of the [ELIS] that enables individuals to understand and have confidence in the system.
- (2) Without limiting subclause (1), the information made available by location agencies in an appropriate way, such as on the agency's website or a shared website, should include:
 - (a) a general explanation of the [ELIS], including:
 - (i) how [ELI] is generated [or collected,] and shared;
 - (ii) how [ELI] will be used and the benefits to the public of the system;
 - (iii) where [ELI] will be stored and for how long;
 - (iv) the current agencies participating in the system and their roles; and
 - (v) that the system is permitted by this Schedule; and
 - (b) guidance about individual access, correction and complaint rights in respect of the system.

[...]

Note: Clauses 4(1) and 4(2) were amended, and clause 4(3) was omitted, by Amendment No 7.

5. Retention of [ELI]

- (1) A location agency must not keep [ELI sourced from the ELIS] for longer than is required for a permitted primary purpose or permitted secondary purpose.

- (2) Where the relevant government agency retains [ELI] for the purpose of monitoring or auditing the operation of the [ELIS], reasonable steps must be taken to ensure that the information is not retained in a form that is capable of identifying [the individual to whom the information relates].

Note: Clause 5 was amended by Amendment No 7. The retention limitation in clause 5(2) applies only to information retained by the relevant government agency for auditing purposes; it does not prevent an emergency service provider from retaining an identifiable record of the collection of ELI.

6. Safeguards to ensure compliance

- (1) A location agency must take reasonable steps to ensure that it collects, retains, uses and discloses [ELI] in compliance with the requirements of this Schedule.
- (2) Without limiting subclause (1), a location agency must:
 - (a) develop and maintain written policies and procedures in respect of the collection, retention, [accuracy,] use and disclosure of [ELI];
 - (b) provide information and training to relevant employees or agents to ensure compliance with these policies and procedures;
 - (c) monitor usage and regularly check compliance with the requirements of the Schedule and, in particular, with the limitations on the retention of [ELI]; and
 - (d) take prompt and effective action in respect of any failure to comply with the requirements of the Schedule.
- [(3) The relevant government agency must maintain a log of all disclosures of DLI (**disclosure log**), which includes:
 - (a) whether the disclosure was in reliance on the permitted primary purpose, permitted secondary purpose, or another purpose;
 - (b) where the disclosure was in reliance on the permitted primary purpose, the grounds for believing that it was necessary;
 - (c) where the disclosure was in reliance on another purpose, a description of this other purpose and the statutory authority on which it was based;
 - (d) the date of the disclosure and the duration for which ELI was collected; and
 - (e) whether or not the individual concerned was notified in accordance with clause 3A(1).]

Note: Clause 6(3) was inserted by Amendment No 7. The disclosure log must be reported to the Commissioner every 3 months (see clause 7(3)).

Note: The requirements of clause 6 are in addition to, and do not replace, the general obligations to keep personal information secure (refer rule 5 of the code and principle 5 of the Privacy Act 1993).

7. Assurance of compliance

- (1) The relevant government agency must, before authorising an agency under clause 2 to receive [ELI] from the [ELIS], seek and obtain an assurance that the agency will take the steps required by clause 6.
- (2) A location agency – including the relevant government agency – must, on request from the Commissioner, provide a written assurance that the steps required by clause 6 have been taken.
- [(3) The relevant government agency must provide to the Commissioner, every three months, the disclosure log for the preceding three month period.]

Note: Clause 7(1) was amended, and clause 7(3) was inserted, by Amendment No 7.

Note: Schedule 4 was inserted by Amendment No 5.

Appendix 1
Telecommunications Information Privacy Code 2003
Amendment No 2 (Temporary)

Telecommunications Information Privacy Code 2003 Amendment No 2 (Temporary)

I, MARIE SHROFF, Privacy Commissioner, now issue under section 51 of the Privacy Act 1993, and in accordance with section 52 of the Act, this amendment to the Telecommunications Information Privacy Code 2003.

Issued by me at Wellington on 8 October 2003

The seal of the Privacy Commissioner)
was affixed to this amendment to the) [L.S.]
Telecommunications Information Privacy)
Code 2003 by the Privacy Commissioner)

Marie Shroff
Privacy Commissioner

1. Title

This amendment may be referred to as the Telecommunications Information Privacy Code 2003 Amendment No 2 (Temporary).

2. Commencement and expiry

- (1) Clause 3 will come into force on 9 October 2003.
- (2) The rest of this amendment will come into force on 1 November 2003.
- (3) This amendment will expire on 24 September 2004.

3. Revocation of Amendment No 1 (Temporary)

Amendment No 1 (Temporary) is revoked.

4. Amendment to clause 1

Clause 1 is amended in the following manner:

Omit: Telecommunications Privacy Code 2003
Substitute: Telecommunications Information Privacy Code 2003

5. Amendment to clause 3

The definition of "foreign telecommunications law" is omitted.

6. Amendment to rule 2(2)(d)

Rule 2(2)(d) is amended in the following manner:

Omit: subparagraphs (ii), (iii) and (iv)

Substitute: (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(iii) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;

7. Amendment to rule 3(4)(b)

Rule 3(4)(b) is amended in the following manner:

Omit: subparagraphs (ii), (iii) and (iv)

Substitute: (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(iii) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;

8. Amendment to rule 10(1)(c)

Rule 10(1)(c) is amended in the following manner:

Omit: subparagraphs (ii), (iii), (iv) and (v)

Substitute: (ii) for the protection of the public revenue;
(iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(iv) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;

9. Amendment to rule 11(1)(f)

Rule 11(1)(f) is amended in the following manner:

Omit: subparagraphs (ii), (iii), (iv), (v) and (vi)

Substitute: (ii) for the enforcement of a law imposing a pecuniary penalty;
(iii) for the protection of the public revenue;
(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(v) for the purpose of preventing or investigating an action or threat that may compromise network or service security or integrity;

10. Amendment to Schedule 2

Paragraph (a) of clause 3 of Schedule 2 is amended by inserting after the word "address" the following:

(or, in the case of an electronic directory, the approximate name and the region)

Legislative history of Amendment No 2 (Temporary)

8 October 2003 – amendment issued

9 October 2003 – commencement of clause 3 only (revoking Amendment No 1 (Temporary)) 1

November 2003 – commencement of the balance of the amendment (the date on which the code itself commences)

24 September 2004 – expiry of the amendment.

Explanatory note

This amendment:

- *revokes Telecommunications Information Privacy Code 2003 Amendment No 1 (Temporary); and*
- *amends the Telecommunications Information Privacy Code 2003.*

Amendment No 1 is revoked because it contained an error in the expiry date. This amendment is, in all material respects, the same as Amendment No 1 except that it has an earlier expiry date. The amendments are made in reliance upon Privacy Act 1993, s.52, which specifies requirements in relation to expiry dates for temporary amendments.

The substantive effect of the amendment is to:

- *omit four subparagraphs from the rules (rules 2(2)(d)(ii), 3(4)(b)(ii), 10(1)(c)(ii) and 11(1)(f)(ii)) – several following subparagraphs are omitted and reinserted in sequential order for stylistic reasons;*
- *insert a new parenthetical provision into clause 3(a) of Schedule 2.*

Legislative history

2 May 2003	Code issued
25 September 2003	Amendment No 1 (Temporary) issued (revoked 9 October 2003 by Amendment No 2 (Temporary))
8 October 2003	Amendment No 2 (Temporary) issued (revoked 1 August 2004 by Amendment No 3)
1 November 2003	Commencement date (except for clauses 3(e) and (f) of Schedule 2)
3 June 2004	Amendment No 3 issued
1 August 2004	Commencement of Amendment No 3
1 April 2005	Commencement of clauses 3(e) and (f) of Schedule 2
9 September 2015	Amendment No 4 issued
15 October 2015	Commencement of Amendment No 4
26 January 2017	Amendment No 5 issued
2 March 2017	Commencement of Amendment No 5
25 August 2017	Amendment No 6 issued
28 September 2017	Commencement of Amendment No 6
8 April 2020	Amendment No 7 issued
7 May 2020	Commencement of Amendment No 7

Telecommunications Information Privacy Code 2003

*This consolidation: May 2020
Available to download at www.privacy.org.nz*

*Office of the Privacy Commissioner
PO Box 10094
Wellington 6143
0800 803 909*