Privacy Commissioner
Te Mana Matapono Matatapu

ISSUE OF TELECOMMUNICATIONS INFORMATION PRIVACY CODE 2003

INFORMATION PAPER ON CHANGES TO NOTIFIED CODE

The proposed Telecommunications Information Privacy Code was publicly notified, and released for public consultation, in December 2001. Submissions were sought by 22 March 2002. More than 35 written submissions were received. Consultation meetings were held in Auckland and Wellington. The Commissioner refined the proposed code as a result. In May 2003 the Telecommunications Information Privacy Code was issued. This note outlines aspects of the consultation process and explains changes incorporated in the issued code.

In this note:

- **notified code** means the version dated 13 December 2001 headed "Draft for consultation: Telecommunications Information Privacy Code 2002" which was publicly notified in December 2001
- **issued code** means the Telecommunications Information Privacy Code 2003 issued in March 2003.

CONSULTATION PRIOR TO ISSUE OF CODE

During 2001 a draft code was prepared, building upon work in earlier years. Industry comment was sought on working drafts. Views were sought from the public by placing a draft on the office website and by including it as a topic in a privacy forum held in Wellington in November 2001. Considerable changes were made to these early drafts as a result of comments received in writing and at meetings.

In mid-December 2001 the Commissioner publicly notified his intention to issue the Telecommunications Information Privacy Code (the notified code). Public notices were placed in newspapers in the main centres and in *Infotech Weekly*. An information paper was prepared and made available with the proposed code on the Commissioner's website and in response to public enquiries. Copies were distributed to organisations that might be interested.

Formal written submissions were received from some 35 organisations and individuals. A number of these people later made supplementary submissions with some major telecommunications companies making 6 or 7 additional submissions. During April and May a series of meetings were held in Wellington and Auckland with those who made submissions.

A number of submissions focused upon just one aspect of the code: proposals concerning the retention of traffic information. The Commissioner took a position on

that issue in May 2002 and advised those that made submissions on the matter. The substantive issues, and the position the Commissioner took, are mentioned below.

During the rest of 2002 and in early 2003 the Commissioner continued to consider the submissions made. In a number of cases, clarification was sought from those that had made submissions on particular points. For the most part, this involved discussions with the major network operators who made a number of suggestions for drafting changes.

On 2 May 2003 the Commissioner issued the code (the issued code).

COMMENCEMENT OF THE CODE

The code will come into force on 1 November 2003. The 6 month delay in commencement is to enable time for telecommunications agencies to prepare. Some parts of the code, affecting directories, are delayed until 1 April 2005. The extended period is to take into account the long lead-in time needed for any changes to telephone directories.

It is intended that a version of the code be published with a full explanatory commentary to assist with compliance. This edition is in preparation and will be available well before the code comes into effect.

CHANGES MADE TO THE PUBLICLY NOTIFIED CODE

This note does not seek to describe and explain all the various changes to the proposed code, a number of which addressed stylistic or small drafting matters. It draws attention to the major changes as well as mentioning a selection of less significant ones.

Coverage of the code (clause 4)

The coverage of information by the code remains as in the notified code.

The classes of agency covered remains the same as publicly notified although expressed slightly differently. The changes have resulted from the adoption, as signalled in the notified code, of definitions in the Telecommunications Act 2001. (The Telecommunications Bill was pending enactment at the time the code was notified.) "Telecommunications service provider" was one such definition which has altered substantively. The elements of "telecommunications service provider", as defined in the notified code, have been carried forward in the issued code by stating explicitly the agencies which would have been within the former definition. In particular, the issued code explicitly states it applies to:

- an Internet service provider;
- a call centre which provides call centre services on contract to another agency;
- a mobile telephone retailer.

These classes of agency fell within the former definition of telecommunications service provider.

Definitions (clause 3)

Several definitions which were in the notified code have been dropped where terms are not used in the issued code (business directory, business directory enquiry service, opt-out, preference scheme, reverse directory).

Two new definitions are included (Internet service provider, reverse search facility).

A few definitions have been changed. Some, as already noted, have been altered to take account of the enactment of the Telecommunications Act 2001 (generally without substantive change). Two changed definitions ("direct marketing" and "telecommunications service provider") are mentioned elsewhere in this note.

Anonymity principle (rule 1(2) in the notified code, omitted from the issued code)

The notified code included a subrule 1(2) that:

> "Whenever it is lawful and practicable, individuals must have the option of not identifying themselves when dealing with a telecommunications agency."

This has been omitted from the issued code. While the provision had merit, and was particularly relevant to telecommunications privacy issues, it was concluded the rule would not have achieved much more than subrule 1(1) given the application of the code to a limited class of telecommunications agencies. The particular issue of enabling individuals to maintain their anonymity when communicating by telecommunications through the medium of a telecommunications network would not have been effectively addressed by the subrule. The code elsewhere obliges telecommunications agencies to provide blocking facilities if offering CLIP.

The issue of an anonymity or pseudonymity principle could usefully be revisited at a future point when consideration is given to extending the coverage to agencies using telecommunications.

International law enforcement, network security and integrity

The notified code included exceptions in rule 2, 3, 10 and 11 which are not found in the corresponding information privacy principles in the Act. These allow for non-compliance with the relevant rules where the agency believes on reasonable grounds that the non-compliance is necessary:

- to assist a foreign law enforcement organisation in the prevention, detection, investigation and prosecution of a breach of a foreign telecommunications law; and
- for the purpose of preventing or investigating an action that may compromise network security or integrity.

These exceptions recognise the trans-border aspects of telecommunications and the need to protect networks which we all rely upon.

The provisions have been retained but some changes were made including:

- substituting "foreign law enforcement authority" for "foreign law enforcement organisation" (to avoid a statutory interpretation difficulty given that the Privacy Act defines "organisation" in a manner limited to New Zealand entities);
- extending the exceptions to an "action *or threat*";

- extending the exceptions to actions or threats that may compromise network "or service" security or integrity (this specific example being a denial of service attack which might compromise service to a particular subscriber while leaving a network uncompromised).

A provision is included to explicitly allow the lifting per-line or per-call blocking in relation to 111 calls (see Schedule 3, clause 2).

Participant monitoring of calls for service quality and contract formation (subrules 4(2) and (3) in the notified code, omitted from the issued code)

The notified code contained two subrules concerning the monitoring of the content of telephone calls involving telecommunication agency staff for the purposes of staff training, checking service standards and for the establishment or varying of subscriber contracts. These provisions have been omitted from the issued code.

The provisions did not, for the most part, seek to exempt any practice from information privacy principle 4 nor prohibit any existing practice. Rather, the proposed subrules were intended to assist agencies by prescribing how the principle could be complied with in the circumstances. However, in consultation it became apparent that major telecommunications companies did not particularly welcome the framework suggested in the subrules. An effort was made to further refine the subrules. However, as the specificity diminished the usefulness of the subrules became open to question and it was ultimately decided, for the meantime, to simply leave it to individual agencies to comply with the general obligations in subrule 4(1) if they intend to undertake monitoring.

The issues of call monitoring are not specific to telecommunications agencies which *provide* telecommunications services but can arise for any agencies which *use* telecommunications services. This is a telecommunications privacy issue which may well worth revisiting in the event that the code is extended to a wider range of agencies which use telecommunications. In doing so it may be possible to build upon significant policy work undertaken in Hong Kong and the UK, since the code was notified, concerning best practice approaches on employee monitoring issues.

Access to identity of another individual or subscriber (rule 6)

The notified code created a new reason for withholding information in response to an information privacy request. This allowed a telecommunications agency (other than a public sector agency) to refuse to disclose to a requester linked traffic information which may reveal the identity of another individual or subscriber. This provision was included as a result of experience with some complaints, during the period in which the Privacy Act has been in operation, whereby the identity of callers has been sought from network operators. The individual right of access is fundamental to any set of information privacy principles and therefore great caution must be exercised in limiting such rights. This is a case where the privacy rights of two individuals are set against each other. The rule seeks to allow a clear discretion to withhold information albeit that the price of clarity comes at the cost of favouring one individual's interests over another (rather than leaving it for a case by case balancing). Submissions were made to extend the provision in various ways. However, the issued code actually narrows the provision so that it applies only to network operators, where the original issue was identified, and not all telecommunications agencies.

The operation of this new provision will be watched carefully in practice and it may need to be revisited at a later date to narrow, clarify or extend it. In doing so, there will always be a significant dilemma about narrowing existing statutory access rights.

Retention of traffic information (rule 9)

The information paper accompanying the notified code recorded that retention of traffic information has been a contentious privacy issue overseas. This proved to be the case in this consultation as well. Subrules 9(2) and (3) in the notified code provided simply that:

> "(2) Traffic information not required for billing must be erased, or rendered such that it cannot be associated with information about an identifiable individual, on termination of the telecommunication or promptly thereafter.
> "(3) Notwithstanding subrule 9(2), it is not a breach of this rule if traffic information is retained for no longer than six months from its generation."

The proposal was in keeping with rule 9(1) and was essentially compatible with, although a highly relaxed version of, the approach taken in Europe. A number of submissions expressed concern about the provision. They can be grouped into three categories:

- community groups and individuals favouring surveillance of people's use of the Internet to track use of pornography;
- law enforcement and intelligence agencies who want access to records of traffic information in relation to unlawful trading of objectionable images and the investigation of crimes more generally;
- telecommunications agencies concerned that the requirements might prejudice certain uses that they might wish to put traffic information to.

A significant reason for including the six month grace period in rule 9(3) was the recognition of law enforcement needs. Six months considerably exceeded the period generally being seen in Europe, at the time the code was notified, as being reasonable for retention for law enforcement purposes (typically 0-3 months). Had the decision not been taken to omit subrules (2) and (3) entirely, a new provision could have been developed to allow for the retention of traffic information where a specific request had been received from an appropriate law enforcement body. This would be akin to the "preservation order" approach taken in the United States.

However, it was the submissions from the telecommunications agencies which lead to the omission, rather than reworking, of the proposed subrules. Information was provided in relation to the existing use of the traffic information for statistical analysis and the difficulties that might be encountered in seeking to undertake such work with information that had been rendered unidentifiable.

The Commissioner took a decision not to proceed with rules 9(2) and (3) in May 2002 and communicated this in a four-page memorandum to those who made a submission on rule 9. The memorandum is available on request.

The issues relating to traffic information will likely need to be revisited. At the moment, rule 9(1) continues to govern the matter. This simply replicates what has been the law since 1993. A number of promising suggestions were made during the consultation as to how the issues might be handled. Examples included requiring data warehouses to be

held "off-line" in encrypted form available only for telecommunications agency data analysis (and not, for example, direct marketing) with access by the police pursuant to search warrants only. However, since the development of such an approach markedly differs from that originally notified, it is more appropriate to develop any new proposal and notify it as an amendment at a future time with the ability for fresh consultation and consideration.

Direct marketing and telemarketing (rules 10, 11 in notified code, rule 10 in issued code)

As noted below, in relation to discussion of directories and directory enquiry services, the proposal for requiring telemarketing opt-out indicators in directories has been omitted from the issued code.

Essentially a telecommunications agency may only disclose subscriber information to another agency for that agency's direct marketing purposes with the authorisation of the individual concerned. This was the requirement of the notified code and remains the same for the issued code (see rule 11).

The requirements in relation to a telecommunications agency's marketing to its own customers remains broadly similar although a number of specific requirements of the notified code have been relaxed or omitted in the issued code (see rule 10).

The first change is in the definition of "direct marketing". This now expressly excludes:

- information sent by a telecommunications agency to a subscriber advising of a rate or service change to an existing service (this probably did not amount to direct marketing in any case but has been included for the avoidance of doubt);
- 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.

The basic premise of the code is that the use of telecommunications information by a telecommunications agency for direct marketing be done with the authorisation of the individual concerned. The issued code continues the requirement of the notified code that where the individual is asked to authorise use for direct marketing that the individual must also be advised that he or she may withdraw such authorisation at any time.

However, most of the other requirements of the notified code with respect to the use of information for direct marketing have been omitted (except in relation to traffic information mentioned below). The requirements that were in rule 10(3) of the notified code that a telecommunications agency maintain a preference scheme and check any readily available industry preference scheme (such as the NZDMA registers) have been dropped. The proposals contained in the notified code for the checking of preference schemes had considerable merit but it was concluded that these requirements should not form part of the issued code. A key consideration was the fact that telecommunications agencies were similar to other businesses in respect of marketing to non-customers and therefore if special rules were to be imposed these should perhaps be done more widely. This matter might usefully be considered again if the code were to be extended to a wider group of agencies.

One area where telecommunications companies are not in the same position as other businesses is in relation to access to traffic information. The issued code continues the requirement in rule 10(3)(e) of the notified code that 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 (see rule 10(2) of the issued code). However, the issued code modifies the requirement to provide that the use is allowed with the authorisation of the individual.

Directories and directory enquiry services (rule 11 in the notified code, rules 2(2) and 11(1) and Schedule 2 in the issued code)

The notified code dealt with the release of subscriber details for inclusion in directories or through directory enquiry services in rule 11(3). This material has been moved into its own Schedule 2 with explicit links to rules 2 and 11 (see rule 2(2)(k) and 11(1)(m)). The drafting has changed considerably while remaining similar in substance. Rewritten parts of Schedule 2 have drawn substantially upon the Code of Practice on Telecommunications Directory Information covering the Fair Processing of Personal Data, UK, 1998.

The notified code proposed that subscribers have the right to have an opt-out indicator placed against entries in directories showing that they did not wish to be telemarketed. Essentially, the opt-out indicator would have adapted telephone books to operate as telemarketing "do not call" lists and the agencies subject to the code, including certain call centres, would have been bound to respect those instructions. Concerns were expressed by the publisher of the main telephone directories. Various refinements of the proposal were explored including explicitly permitting telecommunications agencies to use their customer opt-out lists for the purposes of cleansing others' telemarketing lists. However, the provision was ultimately omitted from the issued code. The key consideration was the limited application of the code to telemarketers. While the code will cover call centres that provide call centre services on contract to other agencies, it would not cover businesses that simply market their own goods and services using the telephone directory. It was considered appropriate to leave this idea for reconsideration at a later date at which point the relevant provisions of the code could be applied to all agencies which use directories displaying such opt-out indicators.

The notified code contains a rule against the inclusion of details in a reverse directory except with a subscriber's authorisation. This has been altered in the issued code to refer to a "reverse search facility" (a newly defined term) to also cover, as with other aspects of the directory rules, release of information from a directory enquiry service.

Calling line identification presentation (CLIP) (rule 11 in the notified code, rule 11(1)(n) and Schedule 3 in the issued code)

To make the rules on CLIP easier to find and use, the relevant provisions have been moved from rule 11 to their own Schedule 3. The substance of the CLIP rules remains the same as in the notified code but three new exceptions to the obligation to provide blocking have been introduced:

- where there is a 111 call;

- where it is believed that a subscriber is using a line for direct marketing purposes or has misused the line for the purpose of disturbing, annoying or irritating any person;
- where the availability of an answer-back function is inherent in the nature of the service being provided (see Schedule 3, clauses 2, 3 and 4).

Internal complaints processes (clause 6 in the notified code, Schedule 1 in the issued code)

The provisions concerning the internal handling of complaints has not altered in substance but has been moved from clause 6 into a new Schedule 1. An obligation to inform individuals of the complaints procedure has been included in the correction rule to match the one in the access rule (see rule 7(5)(b)).

Service or billing enquiries (rule 2(2) in the notified code, rules 2(2) and 11 in the issued code)

The notified code included an exception to rule 2, which is not found in the equivalent information privacy principle 2, where the information collected from a source other than the individual "is from a member of a subscriber's household and the information is necessary to deal with a service or billing enquiry".

The issued code has retained this exception but widened it slightly to include a collection from "a representative of a business subscriber". Noting that the resolution of service or billing enquiries often involve a conversation in which there is often both a collection and disclosure of personal information, a corresponding new exception has been included in rule 11(1)(k). However, care needs to be taken in the disclosure of details to a person who is not actually the subscriber, and therefore the disclosure exception includes the additional qualification that the person "appears to be acting on behalf of the subscriber".

Office of the Privacy Commissioner
May 2003