To:
Office of the Privacy Commissioner
By email: privacy.code@privacy.org.nz

13 March 2020

Dear Sir/Madam,

Telecommunications Information Privacy Code – Response to Information Paper regarding proposed amendments

Thank you for the opportunity to respond to the proposed amendments to the Telecommunications Information Privacy TIPC 2003 (**TIPC**) as set out in the Information Paper dated 30 January 2020 (**Amendments**).

TCF members consider that in principle the Amendments offer benefits to improve access to location information where the emergency services are involved in a life-threatening emergency situation. However, this must be carefully balanced against the increased risk around the misuse of personal information and who bears ultimate responsibility for this. Our members support the Commissioner considering the appropriate collection and use of this information and how it might strengthen the boundaries around the extended ELIS system.

Our members have raised significant concerns detailed below that need to be considered and addressed before the industry could support the changes and before a revised Code should be brought into force. This includes concerns that:

- telecommunications companies' obligations in the revised TIPC are not consistent with the limited role the industry plays in the ELIS system;
- the proposals apply to future devices and services that have yet to be identified and therefore any privacy issues that may arise cannot be fully considered; and
- the amended Schedule could apply to scenarios for which there has not been material public consideration and may require specific legislation.

Given the breadth of changes and issues they pose, plus the technical nature of the TIPC, we urge OPC to consider a further targeted consultation and a further set of amendments for consideration before the revised TIPC is formalised.

Control and liability for release of Personal Information

Telecommunications companies have a responsibility to only release personal information for the specified exceptions in Rule 11 of the TIPC. Our members take this requirement very seriously, as stepping outside of these exemptions would not only breach the code, it would also damage consumer trust and the reputation of the company.

New Zealand Telecommunications Forum Incorporated (TCF)
PO Box 302469, North Harbour, Auckland
Tel: + 64 9 475 0203 Fax: + 64 9 479 4530
Email: info@tcf.org.nz Web: www.tcf.org.nz

C2 General

Currently, the only way personal data is disclosed under the emergency caller location information (**ECLI**) system is if a customer makes a 111-call seeking help for themselves. Telecommunications companies are permitted to provide ECLI where they believe on reasonable grounds that the collection and use of information is necessary to enable an emergency service provider to facilitate a response to an emergency call.

Our members do not oversee or filter the data in any way, nor do they have the capability to do so, as it is automatically drawn from their systems. However, the ECLI technical limitation that prevents personal data from being collected except in relation to a 111 call gives operators confidence that the information is necessary to facilitate a response to an emergency call. Under the current arrangements our members consider this to be sufficient.

The expanded ELIS system extends the capability to Device Location Information (**DLI**) whereby a customer's information can be collected and accessed "automatically" via the ELIS in the absence of an emergency call. Under the amended Schedule 4, telecommunications companies can only allow access to DLI personal information to "prevent or lessen a serious threat to life or health". However, the automatic nature of the system means that there will often not be the direct consent of the individual to disclose their personal data and telecommunications companies are not able to determine whether there is a serious threat to the life or health of an individual on a case by case basis.

The emergency service provider assesses whether the data is required to "prevent or lessen a serious threat to the life or health of an individual". Therefore, while telecommunication companies are obliged under the TIPC, as drafted, to assess whether there is a serious threat, in an automated system they must rely in practice on the requesting agency's assessment of the situation.

The current ECLI approach resolves this conundrum by providing an exemption whereby a telecommunications company may provide customer information to facilitate a response to an emergency call[1]. We believe that, for telecommunications companies to participate in the ELIS system, a similar enabling provision to ECLI is required that authorises telecommunications companies to provide DLI information to the ELIS system without the telecommunications company applying general Rule 11 considerations. For example, by adding a further class of information to the definition of permitted primary purpose so that for telecommunications companies, including ISPs, a permitted primary purpose is to provide information to the ELIS system.

Extension to other location devices

The proposed extension of the TIPC to "other location devices" beyond smart phones is very broad. Given the extension appears to cover any device capable of transmitting, it presents an additional set of complexities that will need to be worked through and, as the technical design and relevant service providers are not yet known, it is unclear whether there are any privacy concerns or how these can be mitigated.

For example, many connected devices will not be in the same location as the targeted individual calling into question the utility of such a broadly worded clause. Would the agencies collect all device data or only those of users who have opted into the system? In

[1] i.e. and not be required to consider whether the information is necessary to prevent or lessen a serious threat to the life or health of an individual on a case by case basis.

addition, how will agencies ensure that the device belongs to the targeted individual? Would the proposal be consistent with an opt-in consent process, in which case this is already a permitted activity in the existing TIPC?

Extended Scope of ELIS and Consumer Protection

Our members are concerned about the broadened scope that extends Schedule 4 beyond emergency caller assistance and search and rescue scenarios. The second limb of the definition of "permitted primary purpose" states:

> *In relation to Device Location Information, 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.*

Such access would seem to present the potential for circumvention of the current controls (e.g. requiring a production order) applied by our members to protect a highly sensitive customer data set from unwarranted access.

In another example, the Information Paper, states that a "disclosure log" will be maintained of all disclosures of location information in order to keep a record of any information shared from the Emergency Location Information System (**ELIS**) system "for purposes other than responding to an emergency". The use of a reactive reporting log cannot be an effective means of determining the acceptable scope to which this capability and data can be put. Furthermore, there is no indication as to whether or what action could be taken against an agency for non-compliance with the TIPC in such circumstances (where the disclosure was not permitted by other legislation).

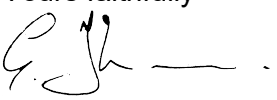
We believe that further consideration would be required prior to extending the scope beyond emergency 111 call and search and rescue related purposes, considering issues such what should constitute a serious threat (this is left to agencies to determine and risks different considerations being applied).

If these concerns are not addressed, this creates privacy risks for consumers, as well as potential reputational risks for emergency services agencies as well as telecommunications providers from such broad purpose. The connection of any system to our members' networks that can access our customers' data is a significant concern for our members.

In summary therefore, our members request changes to the TIPC that ensure legal responsibility and liability for release of information resting with the appropriate agencies, not telecommunications companies, and that further consideration be given to the wording and safeguards of the extended scope of the ELIS system to prevent unintended use.

The TCF and its members would welcome further discussion and information on the issues raised above. Please contact Geoff Thorn (Geoff.thorn@tcf.org.nz) in the first instance.

Yours faithfully



Geoff Thorn
TCF CEO

New Zealand Telecommunications Forum Incorporated (TCF)
PO Box 302469, North Harbour, Auckland
Tel: + 64 9 475 0203 Fax: + 64 9 479 4530
Email: info@tcf.org.nz Web: www.tcf.org.nz