

26 October 2022

Mason

[fyi-request-20617-689164dd@requests.fyi.org.nz](mailto:fyi-request-20617-689164dd@requests.fyi.org.nz)

Dear Mason

### **Request for information**

Thank you for Official Information Act 1982 (OIA) request, dated 19 September 2022, in which you requested information about Police use of polling data. You wrote:

*In the Telecommunication investigations Manual, a Polling Information Request, through a Comms Centre Polling request, is stated to be sent to the Network Operations Centre (NOC) of the three telcos. It is described as relating to a "single" polling request. "A query is done on the Home Location Register (HLR) which is a record of only the last tower a phone polled off ... There are no historic records and it is constantly overwritten .... It is not possible to continually 'track' from this system as it requires constant manual queries."*

You then asked a number of questions. My response to each of your questions can be found below.

1. *Please provide the full Telecommunication investigations chapter.*

The Telecommunications chapter has been provided, however some information has been withheld pursuant to section 6(c) of the OIA, as the making available of that information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial.

2. *Do the New Zealand Police have the access to conduct "manual queries" themselves, or are these relayed to the Telco providers.*

Police does not have the ability to conduct these queries and they must be relayed to the relevant Telecommunications provider.

3. *Is it practically possible to conduct several consecutive manual queries or are there safeguards in place to prevent this? You state that it is not possible to "continually track" but is there anything preventing a bombardment of manual queries as suggested*

Each query made to the telecommunications providers is assessed on its merits and legislative compliance by authorised Police approvers and the telecommunications company themselves.

The main legislation (available to view at [www.legislation.govt.nz](http://www.legislation.govt.nz)) that informs Police accessing polling information, as described in your OIA request are:

- 1) Privacy Act 2020
- 2) Human Rights Act 1993

- 3) New Zealand Bill of Rights Act 1990
- 4) Search and Surveillance Act 2012.

There is also the Code of Practice issued by the Privacy Commissioner under section 32 of the Privacy Act 2020 which specifically relates to the telecommunications industry and is relevant to your request. Information relating to this Code can be found on the Privacy Commissioner's website:

<https://privacy.org.nz/privacy-act-2020/codes-of-practice/tipc2020/>

### **Internal Police Controls**

All requests for polling as described in your request must either go through the Police Communications Centres or an authorised approver who is generally a non-commissioned officer or above.

Police staff are guided by and need to adhere to:

- The Police Code of conduct
- Police 'Our Values'.

Both documents are available on the Police website: <http://www.police.govt.nz/about-us>

#### *4. What is the Warrant / Production Order requirement for single polling requests?*

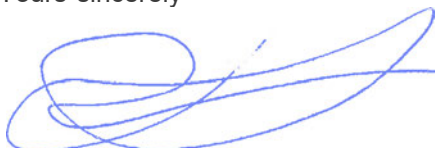
Unless circumstances justify the release of information under the Telecommunications Privacy Code, a production order is required to obtain polling information. Relevant circumstances are generally where there is a genuine risk to life of the individual subject to the request or another and an urgent response is necessary to mitigate this risk.

*For questions 2-4, please provide all manuals, guidance materials, or otherwise held up to date information held by the police.*

The Telecommunications chapter has been provided as per question one and relevant links to material are contained within question two.

I trust this information satisfies your request. You have the right to ask the Ombudsman to review this decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: [www.ombudsman.parliament.nz](http://www.ombudsman.parliament.nz).

Yours sincerely



Dave Lankshear  
Detective Senior Sergeant  
Manager: Telecommunications, Capability and  
Compliance Police National Headquarters

# **Telecommunication investigations**

# Table of Contents

Table of Contents	3
Policy statement and principles	5
What	5
[Redacted]	5
[Redacted]	5
Overview	6
[Redacted]	6
[Redacted]	6
[Redacted]	6
Related information	9
Responsibilities	10
[Redacted]	10
[Redacted]	10
[Redacted]	10
[Redacted]	11
Forensic analysis of devices	12
[Redacted]	12
[Redacted]	12
[Redacted]	12
[Redacted]	13
Evidential integrity of data	14
[Redacted]	14
[Redacted]	14
[Redacted]	15
[Redacted]	16
[Redacted]	16
[Redacted]	16
[Redacted]	16
[Redacted]	17
[Redacted]	17
[Redacted]	17
[Redacted]	18
[Redacted]	18
[Redacted]	18
Disclosure and briefing telco evidence	19
[Redacted]	19
[Redacted]	19
[Redacted]	20
Obtaining telecommunications data	21
[Redacted]	21
[Redacted]	22
[Redacted]	22

Obtaining telco records for a missing person	22
[REDACTED]	22
[REDACTED]	23
[REDACTED]	23
Retention period of records held by telcos	25
[REDACTED]	25
Emergency requests for telecommunications data	26
Emergency requests under the 'Telecommunications Information Privacy Code 2003'	26
Annex 1: Suggested wording for production orders	27
[REDACTED]	31
[REDACTED]	31
[REDACTED]	31

[Redacted]

[Redacted]

## What

Properly obtained evidential material is crucial to a criminal prosecution. **s.6(c) OIA** [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

# Overview

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

s.8(c) OIA

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



b6(c) OR

[Redacted text block containing multiple lines of blacked-out information]

s.8(c) OIA	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

## Related information

See the following related documents:

s.8(c) OIA

[Redacted]

[Criminal Disclosure](#) chapter

s.8(c) OIA

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

s.8(c) OIA

[Redacted]

[Telecommunications Information Privacy Code 2020](#) and [Emergency Caller Location Information \(ECLI\)](#) in the [Information security](#) chapter for emergency requests to identify the location of an emergency caller when making a 111 call/text to the Communications Centre (COMMS) on their mobile phone

s.8(c) OIA

[Redacted]

# Responsibilities

[Redacted]

## Responsibilities of the OC Phones

s.6(c) OIA [Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

s.6(c) OIA

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

# Forensic analysis of devices

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

s.6(c) OIA

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

## Evidential integrity of data

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted text]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
<p>[REDACTED]</p>		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]



§ 87(2)(g)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

s.6(c) OIA

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

SECRET

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## Disclosure and briefing telco evidence

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

§ 87(2)(g)  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]

§ 87(2)(g)  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

[Redacted]

[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

§ 87(2)(g)  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

## Obtaining telecommunications data

[Redacted]

In most cases a Production Order is required to be executed on the telco provider to obtain telecommunications records

Guidance on applying for Production Orders is found in [Part 9 - Production orders](#) of the 'Search' chapter.

### Call associated data (CAD) process

The Search and Surveillance Act 2012 allows for the obtaining of call associated data (CAD) either as a historic process using a section [74](#) production order or on a continuing basis through a surveillance device warrant issued under section [53](#) of the Act. **s.6(c) OIA**

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

s.6(c) OIA

## Obtaining telco records pursuant to other enactments

Police may obtain telco records under other enactments, for example:

- a written notice under section 120 of the Coroners Act
- a production order under Section 105 of the Criminal Proceeds (Recovery) Act 2009.

## Obtaining telco records by consent

An individual can consent to Police obtaining their telco records. s.6(c) OIA

## Obtaining telco records for a missing person

In the case of a missing person investigation where no offence has been identified Police may request telcos to consider disclosing the missing person's telco records using the Information Request Form. Police need to outline the legal basis why they think disclosing the information is justified under the Privacy Act 2020. In any event no requests made under the Privacy Act compel the telcos to make the disclosure.

The seriousness of the investigation will dictate how and when you receive information. **LIFE and DEATH** incidents will take priority at telcos. s.6(c) OIA

**Comms Centre Polling request** - this is sent to the Network Operations Centre (NOC) of the three telcos. It relates to a single polling request. A query is done on the Home Location Register (HLR) which is a record of only the last tower a phone polled off. The HLR is what assists the telco to route calls. There are **no** historic records and it is constantly overwritten with only the latest value. It is not possible to continually 'track' from this system as it requires constant manual queries. The NOCs are not set up to provide ongoing tracking information.

s.6(c) OIA

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



§ 87(2)(b)

[REDACTED]

## Retention period of records held by telcos

[Redacted]

[Redacted]

[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]

[Redacted]

## Emergency requests for telecommunications data

### Emergency requests under the 'Telecommunications Information Privacy Code 2003'

To prevent or lessen a serious threat to public health or public safety, or the life or health of the individual concerned or another individual, principle 11(g) of the [Telecommunications Information Privacy Code 2003](#) allows Police Communications Centres to obtain the following:

- subscriber information
- last outbound activity
- polling location information

**Note:** Emergency requests are limited to identifying the location of an emergency caller when making a 111 call/text to the Communications Centre (COMMS) on their mobile phone

See the section '[Emergency Caller Location Information \(ECLI\)](#)' in the '[Information security](#)' chapter for further information about facilitating a response to an emergency call/text (111).

Disclosure of telecommunications information is limited to:

Rule 11(1)(g) to prevent or lessen a serious threat to:

- public health or public safety
- the life or health of the individual concerned or another individual.

**Note:** 'serious threat' is defined in section 2(1) of the Privacy Act 2020, as:

- the likelihood of the threat being realised, and
- the severity of the consequences if the threat is realised, and
- the time at which the threat may be realised.

- Rule 11(1)(h) - to enable emergency services to respond to a potential threat to life or health of the individual concerned or another individual.

## Annex 1: Suggested wording for production orders

[Redacted]

[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

s.6(c) OIA

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]			[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Annex 2 - s.6(c) OIA

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item 1]
- [Redacted list item 2]
- [Redacted list item 3]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item 1]
- [Redacted list item 2]





---

Printed on : 01/02/2022

Printed from : <https://tenone.police.govt.nz/pi/telecommunication-investigations>