



Police National Headquarters
PO Box 3017,
Wellington
Phone: 04 474 9949

12 September 2017

Misha

Email: [Misha <fyi-request-6466-c05ba87@requests.fyi.org.nz>](mailto:Misha<fyi-request-6466-c05ba87@requests.fyi.org.nz>)

Dear Misha

REQUEST FOR INFORMATION

I refer to your online enquiry to New Zealand Police of 22 August 2017, in which you request pursuant to the Official Information Act:

- *Information as to the Police protocol surrounding the obtaining, handling, storing, and return/disposal of CCTV security footage obtained from 3rd parties in the course of a police investigation.*

Please find attached copies of parts of relevant chapters of the NZ Police Manual:

- 'Passive data generators in homicide or serious crime investigations' – 10 pages
- 'Crime in the retail sector' – 5 pages
- Letter of agreement with Retail New Zealand (Schedule 3 - Protocol regarding disclosure of information held by Retail NZ or its members to the Police and Schedule 4 - Protocol regarding release and use of CCTV images held by Retail NZ and members to the Police) - 4 pages

You will notice that some of the text in the sections provided is in underlined blue type. This text links to other information in the Police Manual, which has not been provided to you.

I also refer you to the documents:

- Crime prevention cameras (CCTV) in public places (2010)
- 2013 Australia and New Zealand Guidelines for Digital Imaging Processes
- 2013 Guidelines for Using Digital CCTV Evidence in Law Enforcement.

These documents are publicly available on the Internet, and therefore release is refused pursuant to Section 18(d) of the Official Information Act 1982.

Any redactions in the material released to you relate to information that is either not relevant to your request or is refused pursuant to Section 6(c) of the Official Information Act 1982, in that the release would be likely to prejudice the maintenance of the law, including the prevention, investigation and detection of offences.

If you are not satisfied with my response to your request you have the right to complain to the Office of the Ombudsman and seek an investigation and review of my decision.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'CS', is written over the typed name 'Craig Scott'.

Craig Scott
Detective Inspector
National Criminal Investigations Group
Police National Headquarters

Part 11 - Passive data generators in homicide or serious crime investigations

CAUTION

This is an operational Police document and some of its content may not be suitable for external dissemination or disclosure. If in doubt contact the National Manager: NCIG for guidance.

This chapter contains these topics:

[Summary](#)

[Passive data strategy](#)

[Methods of gathering electronic evidence](#)

[Closed Circuit Television \(CCTV\)](#)



Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

Summary

CAUTION

This is an operational Police document and some of its content may not be suitable for external dissemination or disclosure. If in doubt contact the National Manager: NCIG for guidance.

Introduction

The development of an electronic world and the use of widespread automated systems such as computers, the Internet and cellular telephones has become increasingly common place in society. As technology continues to develop it is the responsibility of Police to ensure their understanding and investigative processes keep pace with these changes.

Passive data generators are automated systems that gather and collate information for various purposes. Many are not directly associated to persons involved in the investigation but if the relevant systems are identified and accessed by investigators, they can provide crucial information about the movements of the victim, offenders and/or witnesses, movement of particular vehicles and about an individual's lifestyle and relationships.

Other reading

This chapter provides an overview of passive data generators. It also provides specific advice regarding Closed Circuit Television (CCTV) and sales receipt enquiries but does not seek to duplicate existing guidance provided by Police instructions for these subjects:

- Telephone investigation - Refer to: '[Electronic interception](#)' (note that access is restricted).
- Electronic crime - Refer to: (ECL) '[Electronic Crime](#)'.
- Management of digital images - Refer to Photography under:
 - '[Australasian Guidelines on Digital Imaging](#)' and where appropriate,
 - Police '[Digital imaging guidelines](#)'.

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

Passive data strategy

CAUTION

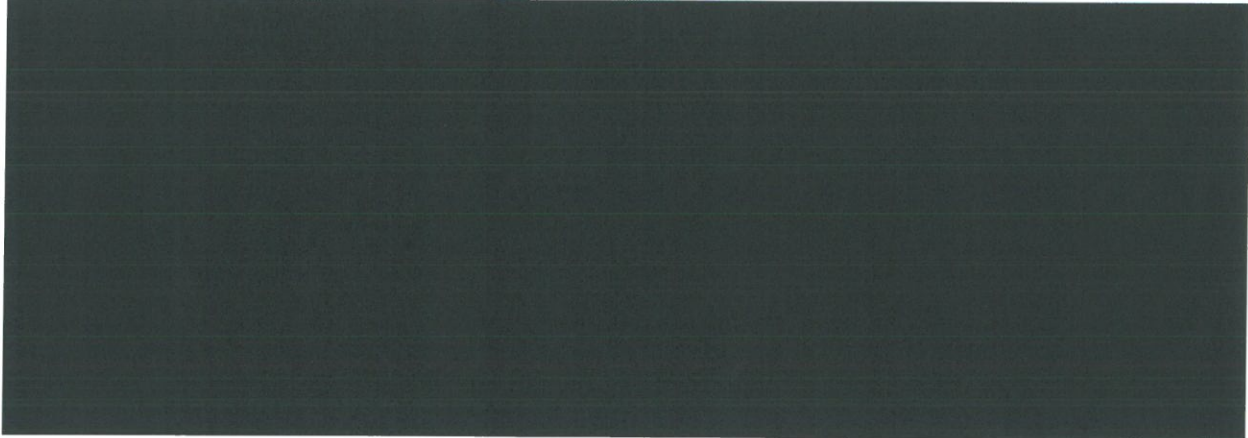
This is an operational Police document and some of its content may not be suitable for external dissemination or disclosure. If in doubt contact the National Manager: NCIG for guidance.

The OC Investigation must develop and implement a strategy to manage the identification, collection, storage, analysis and presentation of data from passive generators using well considered time and location parameters for investigators to follow. Refer to the 'Passive Data Generators' section in ['Part 2 - Role of the OC Investigation in homicide and serious crime investigations'](#).

Sources of electronic evidence

Potential sources of electronic data may include:

- closed Circuit Television (CCTV) systems





In many cases, data generated by these systems is periodically downloaded, archived and/or deleted. Therefore prompt action is required to identify and secure the material otherwise it may be lost to the enquiry.

Legal considerations

Material generated by passive data generators may be subject to legal constraint in which case a lawful authority will be required to seize and use the data. This will usually be a Production Order pursuant to the [Search and Surveillance Act 2012](#).

Before seizing such data, it should be established whether any protocols exist between the source owner and Police that govern how such material can be obtained, e.g.

In such cases, the protocol should be followed.

Integrity of evidence

It is the responsibility of all investigators to acknowledge that the rules of evidence apply equally to computer-based electronic evidence as they do to evidence obtained from any other source.

When access is obtained to material created by passive data generators, investigators must establish how that material was created. This is necessary to demonstrate the integrity and accuracy of the material, if it is later to be used as evidence.

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

Where technical difficulties are encountered the OC Phase, in consultation with the OC Investigation may seek expert advice or arrange for a forensic examination of the material in order to confirm its authenticity and accuracy.

The four principles in the table below will ensure investigators recover electronic evidence safely.

Principle 1	No action taken by Police or persons acting on Police instructions should change data held on a computer or storage media which may subsequently be relied upon in court. Computer based electronic evidence must be regarded in the same way as text contained within a document and it is subject to the same rules and laws that apply to documentary evidence.
Principle 2	In circumstances where it is necessary to access original data held on a computer or on storage media, that person doing so must be competent and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3	An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4	The OC Investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Exhibit management

Audio, CCTV, video recordings or other passive data are original exhibits and must be handled in the approved manner - refer to [Part 16 - Exhibit management in homicide or serious crime investigations](#), and the OC Exhibit desk file in the [Serious Crime Template](#).

When a recording is seized from any source the original recording must be immediately sealed, labelled and a unique exhibit number allocated to it, regardless of whether the data is stored on a tape, CD, DVD, USB or other medium. Tapes must not be stored close to strong electro-magnetic fields. The responsibility for making copies of the original should be determined at an early stage to ensure uniformity in the chain of evidence.

Technical issues

There is a high degree of variation in the types of storage system used to store electronic data. Consideration should be given, in consultation with the OC Investigation, to the technical resources required, firstly in obtaining the data and subsequently in storing, analysing and presenting it. Methods used by data owners to analyse their own data should be established as these may be adequate for investigative purposes and will likely produce faster results than alternative methods.

Where necessary, technical advice is available from:

- **Police Photography Unit:** Photography Sections have expertise in converting images into a useable format, court presentation of images, and editing and enhancement of images (eg. merging two or three cameras onto one screen).
- **Electronic Crime Lab:** The [ECL](#) has experts who can provide technical advice on all aspects of electronic evidence. This will be particularly useful in cases where the recording has been damaged, the data has been deleted or corrupted, or where the suspect has had access to the equipment or data.
- **Private companies,** particularly the service provider who installed or maintains the recording equipment who may provide this service without cost.

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

Cost

Obtaining and analysing large volumes of passive data can result significant costs in terms of financial, human and technical resources for both the owners of the data and police. It is therefore essential the OC Phase and OC Investigation are kept informed throughout so they can decide whether data will be obtained and stored and/or analysed. The authority of the OC Investigation must be obtained before expenditure is incurred.

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

Methods of gathering electronic evidence

CAUTION

This is an operational Police document and some of its content may not be suitable for external dissemination or disclosure. If in doubt contact the National Manager: NCIG for guidance.

The method used to gather electronic evidence will depend on whether general or specific evidential material is being sought.

General material

Passive data may be gathered in a general way where the content of the material sought is unknown and no specific material is expected to feature within it, but where it is nonetheless anticipated that the data will contain information which will be relevant to the investigation. This is achieved by focussing on either a particular location or on the victim, as detailed below:

- Locating, gathering and viewing images captured within a specified geographic location between particular times, for the purpose of identifying any people and/or vehicles present that may later become significant to the investigation. Such images are captured by cameras of CCTV systems operated by organisations, eg. local authorities, banks, garages and shops etc.
- The OC Investigation may consider an area canvass phase specifically for the purpose of identifying premises, businesses and vehicles that are operating CCTV cameras that could provide evidential material.

Note: Any such material may later become evidence when a specific suspect is identified.

Specific material

Passive data may be gathered to assist an investigation for a specific purpose, i.e. to establish or corroborate information about specific circumstances that are relevant to the incident such as:

- confirming the presence and actions of a victim, witness, suspect, vehicle or telephone at a particular location, and confirming the time they were there
- establishing the relationship between particular individuals
- establishing the nature and times of contact between particular individuals
- identifying the lifestyle of a particular individual.

Information or data already gathered by the investigation will determine to a large extent, how the OC Investigation will go about defining the parameters of these enquiries.

Enquiries without a clearly defined focus will likely generate large quantities of passive data which need to be analysed in order to locate the specific material sought to drive the investigation. Therefore it is essential the OC Investigation sets tight parameters in this phase of the investigation.

OC Investigations should also think widely about the type of data sources that may be useful in the particular circumstances of the case. Technical innovations mean that new data generating systems are continually becoming available and it is sometimes difficult to recognise when a particular lifestyle or activity has the potential to generate such

**Part 11 – Passive data generators in
homicide or serious crime
investigations, Continued...**

data. This makes it important to consult those who are knowledgeable about the relevant activity or lifestyle, to identify opportunities that may exist.

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

Closed Circuit Television (CCTV)

CAUTION

This is an operational Police document and some of its content may not be suitable for external dissemination or disclosure. If in doubt contact the National Manager: NCIG for guidance.

All CCTV images must be downloaded, stored, etc according to the [Australasian Guidelines on Digital Imaging](#) and where appropriate, the Police [Digital Imaging Guidelines](#).

CCTV footage can be critical in relation to:

- identifying vehicles, victims, witnesses, suspects and their associates
- identifying and locating items of interest
- following the movements of persons and/or vehicles
- creating a timeline
- confirming or disputing an alibi.

A 2008 report by a law enforcement agency overseas where CCTV is prevalent, concluded only 3% of crimes were solved by CCTV. The OC Investigation must weigh up the costs in terms of financial, human and technical resources involved in collecting, storing and analysing large volumes of footage against the potential benefit to the investigation, before deciding whether data will be:

- obtained and analysed, or
- obtained and stored pending further information coming to light, or
- not obtained.

Co-ordinator

Where large quantities of CCTV footage are to be seized, a CCTV Co-ordinator should be appointed at the outset. For consistency, the CCTV Co-ordinator should remain in that role for the duration of the investigation.

The role of the CCTV Co-ordinator is not to collect all footage personally but rather to manage all aspects of CCTV evidence, including providing advice and guidance to investigation staff regarding targeting and prioritisation of data collection and providing technical assistance as required.

A CCTV Co-ordinator will be particularly helpful where images from different cameras are viewed, as selection of the criteria used to confirm identification of individuals can prove problematic. This can prove particularly difficult where image quality is low.

Where CCTV systems are located that are complex in nature and downloading footage from them is beyond the technical ability of general investigative staff, the proprietor or installation technician, the CCTV Co-ordinator must provide assistance to complete this task where possible. The CCTV Co-ordinator can advise what equipment is required and in most cases this will extend to a USB or external drive that can be used for the duration of the investigation.

Responsibility for the retrieval and management of CCTV and other photographic images sits with Police Photographers and not with ECL. However ECL can advise on specialist equipment requirements. Refer '[Technical issues](#)' in this part.

Parameters

Once the OC Investigation has set time and location parameters within which staff should search for this type of material, every effort must be made to secure the

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

information before it is lost, e.g. CCTV systems often work on a twenty four hour loop before overwriting the recording, so time is of the essence.

Given the proliferation of CCTV systems and the volume of CCTV footage being recorded it has become necessary to take a targeted approach when considering CCTV systems as evidential sources in relation to major crime investigations. Sometimes too many systems record too much information for everything to be seized within a certain radius of a crime scene. Any attempt to adopt such an approach may carry an inherent risk that material may be overwritten before Police can access it.

A targeted and prioritised approach will ensure appropriate resources are deployed in the right area to optimise opportunities to obtain critical evidence.

Targeting

The first task is to determine where CCTV footage should be obtained from. By targeting specific sites or particular locations investigative staff will maximise the likelihood of relevant information being gathered and minimise the risk of wasting time gathering irrelevant information.

This targeted approach will be dictated by:

- Where has the person been?
- Where is it likely they have been?
- Where is it possible they have been?

These parameters will be guided by natural geographic boundaries, timescales, and should be under constant review. The parameters will include considerations such as:

- Location of the primary scene
- Secondary scenes
- Known offender(s)
- Possible suspect(s)
- Victim(s)
- Witness(es)
- Vehicle(s)
- Route(s)
- Timescales
- Forensic opportunities.

Environmental scan

A brief environmental scan of places where a person is known to have been will identify locations of premises and cameras that require targeting as a high priority.

The environmental scan will subsequently extend to other sites or locations where the targeted person is likely to have been or has possibly been, depending on prioritisation. Environmental scanning requires constant review.

CCTV timings

When CCTV data is seized, the time displayed by the CCTV system must be compared to actual time. The correct time can be ascertained by calling the automated World Clock service on 0800 000 000 then dial 7614. Any discrepancy between the system time and real time should be noted and compensated for when downloading the data. This will ensure the correct section of data is obtained, establish the actual time of events captured and assist with synchronisation of timings on different CCTV systems.

Part 11 – Passive data generators in homicide or serious crime investigations, Continued...

To ensure the review of CCTV data and exhibiting of still images from it are conducted systematically, investigators should utilise the CCTV results Excel spreadsheet contained within the [Serious Crime Template](#).

Crime in the retail sector

This chapter contains the following topics:

Summary

- [Introduction](#)
- [Health and safety duties](#)
 - [Maximising safety and minimising risk](#)
 - [Health and safety should be an everyday conversation](#)

Police response to retail crime

Retailers investigating retail crime

- [Investigation process](#)
- [Priority one and two](#)
- [Failure to acknowledge a complaint](#)
- [Rejecting complaints from retailers](#)

Disclosing information held by the retail sector

- [Principle](#)
- [Request for personal information](#)
- [Seeking information](#)
- [Withholding information requested](#)
 - [Search warrant](#)

Request for release of CCTV images

- [Purpose of CCTV](#)
- [Privacy obligations](#)
- [Release and use of CCTV images](#)
- [Release of information to third parties](#)
- [Confidentiality](#)

Appendix 1 - Sample list of questions to ask retailers reporting crime

Crime in the retail sector, Continued...

Summary

This section contains the following topics:

- [Introduction](#)
- [Health and safety duties](#)
 - [Maximising safety and minimising risk](#)
 - [Health and safety should be an everyday conversation](#)

Introduction

This chapter provides procedures and guidelines for Police employees involved in responding, investigating and solving crime that takes place at the retail sector (retailers).

Note: In these instructions, 'retailers' means those who are registered members of the New Zealand Retailers Association.

It should be read in conjunction with the [Letter of Agreement](#) (LOA) signed between the New Zealand Police and the [New Zealand Retailers Association](#) (NZRA) and published on the Police Instructions intranet site.

Health and safety duties

Maximising safety and minimising risk

Maximising safety and eliminating or minimising risk at work is the responsibility of all Police employees and persons engaged by Police to provide a service including contractors and their employees, trainees, interns and volunteers. It is delivered through meeting the obligations under the [Health and Safety at Work Act 2015](#) and Police safety policies.

A key enabler is the application of the [TENR-Operational threat assessment](#) in the workplace.

The expectation of the Commissioner and the Act is that persons in the workplace will take reasonable care to ensure that their acts or omissions do not adversely affect the health and safety of other persons, comply as far as they are reasonably able to with any reasonable instruction that is given in order to comply with the [Health and Safety at Work Act 2015](#) or regulations under that Act. They will co-operate with any reasonable policy or procedure relating to health or safety at the workplace that has been notified to them and take immediate action to stop any perceived or potential breach of the act or if impractical, immediately report the matter to a supervisor.

Health and safety should be an everyday conversation

Relevant Police instructions include:

- [Hazard management](#)
- [Health and safety](#)
- [Wellness and safety](#)
- this chapter in relation to the safe response and investigation with solving crime that takes place at the retail sector (retailers).

Crime in the retail sector, Continued...

Disclosing information held by the retail sector

This section contains the following topics:

- [Principle](#)
- [Request for personal information](#)
- [Seeking information](#)
- [Withholding information requested](#)
 - [Search warrant](#)

Principle

Police need detailed information to carry out the investigation and may request information held by the retailer. The need to achieve the desired outcomes as set out in the [LOA](#) must be balanced by Police and the retailer with the need to protect the rights of individuals and their rights to privacy.

Request for personal information

Police should make a request for personal information only if it is not possible to obtain the information directly from the individual concerned because:

- it is not reasonably practicable to do so
- it would prejudice:
 - the purpose of the collection of such information
 - the maintenance of the law.

Seeking information

If Police seek information that is not in the public domain, the retailer will release that information, including [CCTV images](#), to Police upon mutual agreement that the request is:

- lawful and reasonable
- compliant with the privacy and confidentiality obligations of the retailer to their customers.

Conditions include:

- certification that the request is made in terms of one of the exceptions to principles [10](#) or [11](#) of the Privacy Act 1993 and specifies the exception relied on
- provision of clear details of the information requested
- a written agreement, unless agreed otherwise
- a verbal agreement where the time taken in managing a written request would cause a delay that would prejudice the maintenance of the law
- any verbal requests that may be required to be committed into a written request as soon as practicable after the verbal request has been made.

Withholding information requested

The retailer, as the owner of the information, has the right to withhold information from Police. If the retailer considers there may be grounds for withholding requested information, Police must be told those grounds and asked for their views. The retailer must consider these prior to any final decision on disclosure.

Note: The retailer can request that a search warrant be presented for the requested information.

Search warrant

Where a search warrant is necessary to facilitate the disclosure of requested information, the information request form must be accompanied by a properly issued and signed [search warrant](#).

Crime in the retail sector, Continued...

The retailer will accept that a good facsimile copy of a search warrant addressed to the retailer will be sufficient to consider the warrant executed. The retailer may refuse to process a request if it is not made in the format described in '[Seeking information](#)'.

Crime in the retail sector, Continued...

Request for release of CCTV images

This section contains the following topics:

- [Purpose of CCTV](#)
- [Privacy obligations](#)
- [Release and use of CCTV images](#)
- [Release of information to third parties](#)
- [Confidentiality](#)

Purpose of CCTV

CCTV images (single or a sequence of images) are captured by retailers to:

- ensure the security of their premises and equipment
- ensure the safety of customers and employees
- deter and provide evidence of unlawful or criminal activities.

Privacy obligations

Retailers and Police must recognise the legal and privacy obligations of sharing personal information contained in these images and the associated operational issues.

Release and use of CCTV images

Retailers:

- will in most instances release images to Police voluntarily on the basis that they are:
 - supplied for limited lawful use
 - not intended to be supplied to [third parties](#) without their prior consent
- recognise that the voluntary supply of the images:
 - negates the need to obtain such information by compulsion
 - facilitates the investigation and prosecution of unlawful or criminal activity.

Release of information to third parties

Retailers acknowledge that in the pursuit of law and order Police may need to release these images to third parties including the media. Refer to '[Releasing information to the media](#)' chapter of the Police Manual.

Police must bear in mind the privacy implications to the retailers when releasing information. Obtain prior written consent of the retailers which should not be withheld unreasonably. Refer '[Community disclosure of offender information](#)' chapter of the Police Manual.

Confidentiality

The identity of retailers, customers, and internal security measures must be kept confidential from any suspect or offender during the investigation and prosecution captured on the images.

Retail New Zealand – Letter of Agreement, Continued...

Schedule 3 - Protocol regarding the disclosure of information held by Retail NZ or its members to the Police

1. Sharing information

1.1 When requesting or disclosing information the parties will balance the need to achieve the desired outcomes as set out in the Letter of Agreement (LOA) with the need to protect the rights of individuals and their rights to privacy.

1.2. The parties to this LOA agree that only sufficient information to achieve the respective agency's purpose will be requested or disclosed by one party to the other party.

1.3. The parties are primarily responsible for ensuring that the intent of this LOA is followed by their employees.

1.4. The Police will make a request for personal information only if it is not possible to obtain the information directly from the individual concerned, either because it is not reasonably practicable to do so; or collection from the individual concerned would prejudice the purpose of the collection of such information; or collection of the information from the individual concerned would prejudice the maintenance of the law.

2. Process

2.1. Where the Police seek information that is not in the public domain while conducting an investigation into a crime, however serious, or are gathering intelligence about the activity of any known or suspected criminal(s), the member will release that information upon mutual agreement, that it is lawful and reasonable to do so and is compliant with the privacy and confidentiality obligations of the member to their customers, to the Police (except as provided in paragraph 2.3 of this protocol) only upon receipt of a request from the Police that:

- certifies that the request is made in terms of one of the exceptions to Principle 10 or Principle 11 of the [Privacy Act 1993](#) and specifies the exception relied on
- provides clear details of the information requested
- is in writing unless agreed otherwise
- may be made verbally under urgency where the time taken in managing a written request would cause a delay that would prejudice the maintenance of the law
- any verbal requests may be required to be committed into a written request as soon as practicable after the verbal request has been made.

2.2. If the member considers there may be grounds for withholding the requested information those grounds will be advised to the Police and the views of the Police will be requested and considered prior to any final decision on disclosure. In any event the member has the right to request that the Police obtain a production order or search warrant for the information requested.

2.3. Where a production order or search warrant is necessary to facilitate the disclosure of requested information the information request form shall be accompanied by a properly issued and signed production order or search warrant.

2.4. The retail member will accept that a good facsimile or electronic copy of a production order or search warrant addressed to the member will be sufficient to require the member to provide the evidence referred to in the production order or search warrant.

Retail New Zealand – Letter of Agreement, Continued...

2.5. The member may refuse to process a request if it is not made in the format described in paragraph 2.1.

2.6. Parties agree to respond to requests for information as soon as is practicable.
Signed for and behalf of Retail NZ

Signed for and behalf of Retail NZ

Scott Fisher
Chief Executive of Retail NZ

Signed for and on behalf of the New Zealand
Police

Mike Clement
Deputy Commissioner of Police

Retail New Zealand – Letter of Agreement, Continued...

Schedule 4 - Protocol regarding the release and use of CCTV images held by Retail NZ and members to the Police

1. Purpose

1.1. CCTV images (single or a sequence of images) are made available to the Police from time to time by Retail NZ members, at the request of the Police or as part of a complaint by a retail member, to enable Police to investigate and/or prosecute any unlawful or criminal activity.

1.2. These images are captured by the retail members to ensure the security of their premises and equipment, the safety of customers and employees and to deter and provide evidence of unlawful or criminal activities.

1.3. This schedule is intended to recognise the legal and privacy obligations of both parties in sharing the personal information contained in these images and the associated operational issues.

2. Request for release of images

2.1. The retail members will in most instances release images to the Police voluntarily on the basis that they are supplied for limited lawful use and not intended to be supplied to third parties without the prior consent of the retail member or as required by law.

2.2. Retail members recognise that the voluntary supply of the images negates the need to obtain such information by compulsion and facilitates the investigation and prosecution of offences.

2.3. In addition the process for seeking information outlined in schedule 3 (Protocol regarding disclosure of information to the Police) is applicable in respect of request for CCTV images.

2.4. The Police acknowledge that the images are provided in confidence.

2.5. Retail members agree to provide images for simple requests from the Police free of charge but may be used in a prosecution and be subject to the [Criminal Disclosure Act 2008](#).

4. Release of information to third parties

4.1. The retail members acknowledge that, in order to carry out Police functions, Police may need to release images provided by the members to third parties including the media.

4.2. The Police acknowledge that they will be cognisant of the privacy implications to Retail NZ members when releasing information to third parties and where possible obtain the prior written consent of the retail member, which will not be withheld unreasonably.

4.3. In particular the Police should take reasonable measures to obscure the personal details of retail member staff and customers unrelated to the investigation or prosecution captured on the images.

4.4. Police should also obscure any information that compromises internal security measures.

5. Use of images for investigation and prosecution

Retail New Zealand – Letter of Agreement, Continued...

5.1. Police should take reasonable measures to keep the identity of retail staff members and customers confidential from any suspect or offender during investigation and prosecution.

5.2. Police should take reasonable measures to keep internal security measures confidential during investigation and prosecution.

Signed for and behalf of Retail NZ

Signed for and behalf of Retail NZ

Scott Fisher
Chief Executive of Retail NZ

Signed for and on behalf of the New Zealand

Police
Mike Clement
Deputy Commissioner of Police