

Our Ref: D101100018
Your Ref:

24 January 2011

Mr Justin O'Brien
C/- NT News
GPO Box 1300
DARWIN NT 0801

Dear Mr O'Brien

RE: Complaint against Police

I refer to your written complaint to this Office dated 11 November 2010, regarding the Northern Territory Police accessing your mobile phone records without your permission or knowledge and your request to investigate whether that conduct was unlawful or not.

I accepted your request not to have the Ethical and Professional Standards Command (EPSC) deal with your complaint and my office made enquiries.

BACKGROUND

Law Enforcement Agencies (LEA) are required to report to the Commonwealth Attorney General on the number of authorisations made for access to existing information or documents. This information is tabled in the *Telecommunications (Interception and Access) Act 1979* ("TIAA") Annual Report (copy attached). The authorisations are given by the Commissioner of Police and other officers in NT Police who have been delegated the power to authorise access to telecommunication records.

In the 07/08 period NT Police made 979 authorisations for existing information or documents in the enforcement of criminal law (Section 178) and in the 08/09 period the NT Police made 807 authorisations. The records the subject of the authorisations are requested from a telecommunications provider/carrier. The provider usually has an agreement with an LEA to provide information and a fee is usually charged by the carrier.

As you are aware on 20 October 2010 the Northern Territory Police executed a search warrant at a house situated in Wagaman. An NT News article written by you about this search, published on 21 October 2010, stated that information had been provided to the media by a *police source*. That information included the identity of the owner of the house at Wagaman which was information not released to the media by NT Police.

The Police received a complaint from the home owner dated 27 October 2010 regarding *leaked* information. The EPSC had prior to that date launched an investigation to find the

Police Officer responsible. The Ombudsman was notified of the complaint from the homeowner on 5 November 2010.

The actions of a police officer providing information to you was a breach of Section 155 of the *Police Administration Act*. It was also potentially an offence under Section 76 of the *Criminal Code*:

'76 (1) Any person who, being employed in the public service or engaged to do any work for or render any service to the government of the Territory or any department or statutory body thereof, unlawfully communicates confidential information coming to his knowledge because of such position is guilty of a crime and is liable to imprisonment for 3 years.

(2) If he does so for purposes of gain he is liable to imprisonment for 5 years.'

If an offence was committed by a police officer providing information to the NT News the person obtaining that information could also have been guilty of the same offence as an accomplice, inciter, abettor or procurer. There are several sections of the *Criminal Code* creating such secondary offences. I cite Section 12 but Sections 43BG (complicity and common purpose) 43BH, 43BI (incitement) and Section 104 (compounding crimes) might also have had some relevance to the publication by the NT News of confidential information which was reported to have come from a police officer who specified anonymity as a condition of providing information.

Section 12 of the *Criminal Code* provides:

'12 Abettors and accessories before the fact

(1) When an offence is committed, the following persons also are deemed to have taken part in committing the offence and may be charged with actually committing it:

- (a) every person who aids another in committing the offence;*
- (b) every person who does or omits to do any act for the purpose of enabling or aiding another to commit the offence; and*
- (c) every person who counsels or procures another to commit the offence.*

(2) A person who counsels or procures another to commit an offence may be charged with committing the offence or counselling or procuring its commission.

(3) A finding of guilt of counselling or procuring the commission of an offence entails the same consequences in all respects as a finding of guilt of committing the offence.'

INVESTIGATIVE AUTHORITY

Section 86 of the *Ombudsman Act 2009* ("OA") states when the Ombudsman may decide a Police complaint is to be investigated by the Ombudsman. In this matter the Ombudsman considered that section 86(1)(c) and Section 86(3)(b) applied to your complaint and decided to deal with it under Section 86.

Section 100 of the *Ombudsman Act* refers to adverse comments to be made by the Ombudsman. In this matter subsection 2 is applicable - *The Ombudsman must not make the proposed comment unless, before the report on the investigation is finalised, the*

Ombudsman gives the Commissioner, police officer or other person a reasonable opportunity to make a submission about the report. A copy of this report was provided in draft to the Commissioner of Police on 9 December 2010. Due to an error in the Ombudsman's Office a copy of the draft was sent to you. I thank you for returning it. You may notice differences between the draft and this report. Those arise from my discussions with the Deputy Commissioner, correspondence with the Commissioner and the provision of further information which I have taken into account in fairness to the Commissioner.

Section 101 of the OA *Assessments and recommendations* sets out the matters I am required to consider with respect to a complaint.

(1) For preparing a report for section 97(1) or 99(1), the Ombudsman must:

(a) consider whether the following apply:

(i) conduct of a police officer constituted an offence or breach of discipline or was contrary to law;

(ii) conduct of a police officer was **unreasonable**, unjust, oppressive or improperly discriminatory;

(iii) conduct of a police officer was in accordance with an Act or a practice, procedure or policy that is or may be unreasonable, unjust, oppressive or improperly discriminatory;

(iv) conduct of a police officer was based either wholly or partly on a mistake of law or of fact;

(v) conduct of a police officer was otherwise wrong in the circumstances; and

(b) consider whether a police officer exercised a power for an improper purpose or on irrelevant grounds; and

(c) if the investigation relates to conduct comprising or including a decision by a police officer to exercise a power in a particular way or to refuse to exercise a power, consider whether the following apply:

(i) irrelevant considerations were taken into account in the course of reaching the decision to exercise the power in that way or to refuse to exercise the power;

(ii) a person was entitled at law to have been given, but was not given, the reasons for deciding to exercise the power in that way or to refuse to exercise the power.

(2) The report may include the Ombudsman's assessment about a matter mentioned in subsection (1).

(3) The Ombudsman may, in the report, recommend:

(a) stated action should be taken in relation to the conduct the subject of the investigation; or

(b) no action should be taken in relation to the conduct the subject of the investigation.

(4) Without limiting subsection (3), the Ombudsman may recommend 1 or more of the following actions be taken:

- (a) a police officer be charged with an offence;
- (b) disciplinary action be taken against a police officer for a breach of discipline;
- (c) conciliation in relation to the conduct the subject of the investigation be conducted;
- (d) a decision be reconsidered, varied or reversed or reasons be given for a decision;
- (e) the effects of a decision, act or omission be rectified, mitigated or altered;
- (f) an Act, practice, procedure or policy on which a decision, act or omission was based be amended.

DEFINITIONS

*Call Charge Record*¹ (CCR) – a record of calls made from a service number derived from billing system records.

Reverse Call Charge Records (RCCR) a record of calls received from a service number.

*Historical or existing data*² is data which came into existence before the time the person (telecommunications carrier) from whom the disclosure is sought received notification of the authorisation. It does not include information which came into existence after notification was received but before the authorisation was executed. The disclosure of historical or existing data may be authorised by an enforcement agency when it is considered reasonably necessary, by an authorising officer, for the enforcement of a criminal law or a law imposing a pecuniary penalty or for the protection of public revenue.

*Prospective data*³ is data that comes into existence during the period for which the authorisations is in force. It does not include data that came into existence before the authorisation was in force.

EXHIBITS EXAMINED AND INFORMATION ASSESSED

The following information or exhibits were obtained and considered:

- Your letter of complaint dated 11 November 2010;
- Legal advice regarding Commissioner of Police - Power of Delegation;
- Whether application under the *Telecommunications (Interception and Access) Act 1979* was undertaken by an *authorised person*;
- A copy of the 2007 *Authorisation and Schedule* signed by Mr Paul White;

¹ Reference: Police Integrity Commission

² Reference: Telecommunications (Interception and Access) Act 1979 Annual Report for the year ending 30 June 2009.

³ Reference: Telecommunications (Interception and Access) Act 1979 Annual Report for the year ending 30 June 2009.

- NTPFES 'Request Processing System' documents;
- NTPFES 'Provide Request Details' documents;
- Requests to your telecommunications carrier (Optus);
- Advice from the Commonwealth Attorney General's Office on the *Telecommunications (Interception and Access) Act*;
- Call Charge Records (CCR) and Reverse Call Charge Records (RCCR) for your mobile phone 19 October 2010 to 22 October 2010;
- Call Charge Records (CCR) for your mobile phone 22 September 2010 to 27 October 2010;
- Correspondence from the Commander of Ethical & Professional Standards Command (EPSC);
- Emails between the Deputy Ombudsman and the Commander of Police Crime & Specialist Support Command;
- Conversation between the Commissioner of Police and the Ombudsman;
- Conversation between the Commissioner of Police and the Deputy Ombudsman;
- Two meetings with the Commander of Police Crime & Specialist Support Command;
- Police Roster for the period 14/10/10 to 10/11/10;
- Emails between the Assistant Ombudsman and the Attorney General's Department (Commonwealth);
- Meeting between the Deputy Commissioner and the Ombudsman and Deputy Ombudsman to discuss the draft of this report 14/12/10;
- Correspondence from the Commissioner of Police dated 30 December 2010.

LEGISLATION AND POLICE GENERAL ORDERS

The *Telecommunications (Interception and Access) Act 1979* regulates the circumstances and conditions on which the *privacy of individuals who use the Australian telecommunications system*⁴ can be infringed. It is legislation of the Commonwealth of Australia, not the Northern Territory.

*Agencies are able to authorise the disclosure of telecommunications data if they are an enforcement agency. An enforcement agency is an agency responsible for the administration of legislation which enables them to enforce a criminal law, impose pecuniary penalties or protect the public revenue. An authorised officer of an enforcement agency is able to make the authorisation*⁵.

Sections 174-180 of the *Telecommunications (Interception and Access) Act 1979* allows authorisations for the release of telecommunications data under certain circumstances.

Apart from a requirement for Police to adhere to legislation, the Police are also required to adhere to *General Orders* which contains their *Code of Conduct and Ethics*. This Code states *the purpose of this order is to provide instruction, guidance and advice and make explicit certain behaviours that are unacceptable for all Police staff regardless of rank, and to provide an ethical framework for member's decisions and actions. If a member is in any*

⁴ Reference: *Telecommunications (Interception and Access) Act 1979 Annual Report for the year ending 30 June 2009*.

⁵ Reference: *Telecommunications (Interception and Access) Act 1979 Annual Report for the year ending 30 June 2009*.

doubt about the application or meaning of any section of this General Order the member must consult a supervisor or manager for guidance. Whatever their position, a Police member may not act beyond the powers the law gives them.

Within this *General Order* under the heading of *media relations* it is written:

Members may only release information to the media in compliance with NTPFES Media Policy.

Information published in the media that appears to be from a police communication or source that is not in accordance with the NTPFES Media Policy will not be tolerated. Such information can include, but is not limited to, police operational or administrative issues. All such unauthorised releases of information will be subject to investigation and oversight by the Ethical and Professional Standards Command. If provisions of the Information Act or Criminal Code relating to the access or communication of information have been breached the matter may be referred for criminal investigation.

Section 155 of the *Police Administration Act* states the following:

155 Communication of information

(1) A member shall not, without reasonable cause, publish or communicate any fact or document to any other person which comes to the knowledge or into the possession of the member in the course of his duties as a member and which the member has not been authorised to disclose.

Penalty: \$1,000 or imprisonment for 6 months or both

Section 14C of the *Police Administration Act* sets out the disciplinary procedures applicable to members:

14C Disciplinary procedures

The Commissioner may, for the purposes of the general control and management of the Police Force, issue instructions relating to the counselling and cautioning of members (including the issuing of written cautions to members) who commit breaches of discipline that are of such minor nature as not to warrant action being taken under Part IV.

This investigation has not included whether or not any particular Police officer breached legislation or the Police Code of Conduct and Ethics by providing information to the NT News.

On 19 November 2007 Mr Keith Holland, Communications Access Co-ordinator (Commonwealth) made a *determination*⁶ under subsection 183(2) of the *Telecommunications (Interception and Access) Act 1979*. This determination commenced on 1 December 2007. This *determination* is in respect to subsection 178(2), the section used by Police to obtain your phone records. This determination specifies that an *Authorisation* must include:

⁶ Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2007.

1. *The identity of the enforcement agency;*
2. *The basis on which the enforcement agency is an enforcement agency;*
3. *The identity of the authorized officer who is making the authorization;*
4. *The basis on which the authorized officer is an authorized officer;*
5. *The relevant provision(s) of the Act under which the authorization is made;*
6. *The name of the person from whom disclosure is sought;*
7. *Details of the information or documents to be disclosed;*
8. *A statement that the authorized officer is satisfied that the disclosure of the information or documents is reasonably necessary for the enforcement of the criminal law,...*
9. *The date on which the authorization is made.*

An Authorisation, whether in written or electronic form, must be signed by its maker. Section 5AB – *Authorised Officers* – states that the head of an enforcement agency may, by writing, authorize a management office or management position in the agency for the purposes of paragraph (c) of the definition of authorized officer in subsection 5(1). A copy of an authorization must be given to the Communications Access Co-ordinator. The Authorisations sighted by this Office to obtain your CCR's and RCCR's complied with the above determination.

Attorney Generals Department – Commonwealth

The view of the Commonwealth Attorney Generals (AG's) Office (Telecommunications and Surveillance Law Branch) was sought as part of this investigation. My Office was advised that if the Police accessed information under S178 (ie existing data) then the limitations referred to in section 180(4) of the *Telecommunications Interception Act* are not relevant.

The AG's department also set out the definitions of existing and prospective data as follows:

Existing and prospective telecommunications data

Telecommunications data (metadata) is information about a telecommunication but does not include the content or substance of the communication. For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration.

The disclosure of telecommunications data by eligible persons (ie carriers) is prohibited under s 276 of the Telecommunications Act 1997. Since 2007 however, the TIA Act contained an exception to the general prohibition on the disclosure and use of metadata. Access to metadata may now be allowed under s 178, 179 and 180 of the TIA Act.

The new provisions distinguish between access to historical metadata, which is data that is already in existence at the time of the request, and prospective metadata, which is data that is collected as it is created and forwarded to the agency in near real time.

Sections 178 and 179 are provisions that provide an exception for the prohibition on the use of historical metadata. Section 178 provides for the access of historical metadata for the purpose of the enforcement of the criminal law whereas s 179 provides for the access of historical metadata for the purpose of the enforcement of laws imposing pecuniary penalties or the protection of the public revenue.

Section 180 provides an exception for the prohibition on the use of prospective metadata. Where access to historical metadata is available to enforcement agencies, access to prospective telecommunications data is only available to criminal law-enforcement agencies. Access under s 180 is limited to investigations by criminal law enforcement agencies of offences which attract a maximum term of imprisonment of at least 3 years. Regard must also be had to the privacy of the person or persons likely to be interfered with by the disclosure.

Our view is that the reason for the extra limitations in s 180 is because of the higher impact on privacy where metadata is being disclosed in near real-time as opposed to historical metadata. Our view is supported by the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007 which inserted the access to telecommunications data provisions into the TIA Act. This is available on ComLaw (<http://www.comlaw.gov.au/ComLaw/legislation/bills1.nsf/bills/bytitle/99290269428E090BCA2572FB00241212?OpenDocument&VIEWCAT=attachment&COUNT=999&START=1>).

With reference to the identity of the person to be notified of access under Section 184 my Office was advised:

The reference to the 'person' to be notified of authorisation for access to telecommunications data in s 184 of the TIA Act is the same person from whom the disclosure is sought. Disclosure of such information is sought from telecommunications carriers. You are right in saying that the provision's reference to 'person' is to the telecommunications carrier and not to the person to whom the records relate.

The AG's concluded:

Accordingly, telecommunications data can be released under s 178, 179 and 180 of the TIA Act which provides access to different types of metadata. Historical metadata access under s 178 and s 179 is allowed where it is reasonably necessary for the enforcement of the criminal law and laws imposing pecuniary penalties respectively. In contrast, prospective metadata under s 180 may only be accessed where it is reasonably necessary for the investigation of offences that are punishable by imprisonment of at least three years. These are distinctive provisions that do not overlap.

First CCR search – 19 October – 22 October

The Telecommunications (Interception and Access) Act 1979 - Section 175 – Authorisations for access to existing information or documents - under subsection (2)(c) states that the

following person is an eligible person – *an officer or employee of the Organisation covered by an approval in force under subsection (4); may authorize the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorization.* Subsection (4) states that the *Director-General of Security*⁷ may, by writing, approve an officer or employee of the Organisation for the purposes of paragraph (2)(c).

On 19 November 2007 Mr Paul Cameron White, then Commissioner of the Northern Territory Police endorsed a document titled 'Authorisation' with a 'Schedule' allowing *each office or position of the Northern Territory Police at or above the rank of Superintendent; the Officer in Charge of the Operational Intelligence Section; the Officer in Charge of the Specialist Crime Section; or the Territory Intelligence Coordinator* to amongst other things *authorize the disclosure of specified information or specified documents under Division 4 of Part 4-1*⁸ of the Act.

On 21 October 2010 a Senior Constable from the Operational Intelligence Section (OIS) completed a *Request* form which was allocated to another Senior Constable from the Drug and Intelligence Division. The Request was for CCR and RCCR records for the period 19/10/2010 to 22/10/2010 for your mobile 0401442440. On 22 October 2010 the acting Officer in Charge of OIS authorised the request.

The Authorisation was electronically sent to Optus on 22 October 2010. Unfortunately the officer completing the electronic request made a clerical error and entered incorrect information into the document citing that the CCR and RCCR information was for an *investigation into offences contrary to the Misuse of Drugs Act*. This incorrect information appears to have no effect on the Police meeting the Commonwealth requirement for *Authorisations*. The request accurately recorded the enabling legislation (Section 178(2)). Subsequently, Police noted their error and corrected their records identifying section 155 of the *Police Administration Act* as the reason for seeking the carrier (Optus) records. They also advised Optus of the mistake to ensure that no record existed linking your phone number as having some connection with the misuse of drugs.

The Police on obtaining your phone records determined the name of a Police officer believed to have breached section 155 of the *Police Administration Act*. Details for phone numbers showing on your records were sought from the carrier to identify the subscriber to that number.

The search of your charge records to this point was limited to a four day period during which it appeared that a Police officer provided information to you. Your records identified a Police officer's phone number. The records showed two calls from your number to the officer's and one call to you from the Police officer. The first call on the records between the two numbers showed that the contact was initiated by you.

⁷ *Director-General of Security* – not defined within the Act however the Deputy Director-General of Security is defined as an officer of the Organisation who holds office as Deputy Director-General of Security.

⁸ Division 4 – *Enforcement Agencies*. Part 4-1 - *Permitted access to telecommunications data*.

I am satisfied that the records and evidence show that the first search of your call charge records was lawful and was reasonably necessary for the investigation of suspected offences. Those offences could have been breaches of Section 155 of the *Police Administration Act*, a breach of Section 76 of the *Criminal Code* and possible breaches of Sections 12, 43BG, 43BH, 43BI or 104 of the *Criminal Code*. Further investigation by NT Police to find out who used the phone sets matching the subscriber numbers was warranted.

The Second CCR search – 22 September 2010 – 27 October 2010

On 28 October 2010 a Senior Constable from OIS, sent another request for your records. The request was only for your CCR records, ie, records of whom you called, not who called you. However the period was expanded seeking records from 22 September 2010 to 27 October 2010. The authorising officer was the Territory Intelligence Coordinator (TIC). The electronic Authorisation for your records was sent on 01/11/2010 to Optus. The Authorisation was given by a Senior Sergeant whom I am satisfied had a lawful delegation under the *Telecommunications (Interception and Access) Act*.

Also on 28 October 2010 the Police applied for and obtained CCR's (22/09/10 to 27/10/10) for a Police officer believed to have been responsible for the information *leak*.

On 5 November 2010 this officer was interviewed and on 8 November 2010 the officer was disciplined (section 14(c) of the *Police Administration Act*) for not reporting contact with you.

Investigation Outcome

This investigation revealed that the Police made two (2) applications to Optus to obtain your CCR's, the initial application included obtaining your RCCR's.

I have seriously considered your view that Section 180(4) of the TIAA - *Authorisations for access to prospective information or documents* - applies to Section 178. Section 178 is the section of the TIAA that Police relied upon to obtain your records.

Prospective information (as referred to in section 180) is not defined within the Act, however it was described by NT Police as *accessing real time data*. In researching a 2007 submission to the *Senate Legal and Constitutional Affairs Committee* I found *prospective data* being described as *information that comes into existence during the life of an authorisation*. The *Telecommunications (Interception and Access) Act 1979 Annual Report* for the year ending 30 June 2009 describes *prospective data* as *data that comes into existence during the period for which the authorisation is in force. It does not include data that came into existence before the authorisation was in force. The disclosure of prospective data may be authorised by a criminal law-enforcement agency when it is considered reasonably necessary, by an authorising officer, for the investigation of an offence with a prison term of at least three years.*

None of the NT Police requests to Optus or the other carrier was for information that came into existence during the life of the authorisations. As such, I must conclude that section 180(4) is not applicable to the existing documents (CCRs and RCCRs) sought by Police under

section 178(2). It is not necessary when seeking past records for a law enforcement agency to be investigating an offence that carries at least a term of imprisonment of 3 years.

The seeking of your phone records in the second instance (starting from 22/09/2010) was in my view unnecessary. At the time of this second request the Police Officer believed to be responsible for the 'leak' had been identified. You had identified yourself in the article you wrote as a possible accomplice.

The Police informed me that the second search of your CCRs was to find out what communication occurred between the Officer and you before and after the calls on 20 October 2010. They said that you and the officer connected to the number you called on 20 October might have been close friends regularly in touch which would tend to dilute anything sinister about the calls on 20 October. I was also told that it was necessary to have the records to be ready to challenge the officer concerned when he was interviewed in case he claimed to be regularly in touch with you as a friend. I reject that latter explanation as a sufficient reason justifying the extent of the records requested. The officer concerned was interviewed three days before Optus provided the CCRs which causes me to discount the "friendship" defence as a sufficient reason. I also consider that even if the CCRs for a five week period showed that your phone and the officer's phone were connected often, such records would not prove who made the calls and what was said. Those records for a five week period were not capable of disclosing anything of probative value beyond what had already been obtained by the first search.

Although I am satisfied that the second search of your CCRs was lawful and authorised under Section 178 of the *Telecommunications (Interception and Access) Act* that search was "unreasonable" within the meaning of Section 101 of the OA. Police have powers and they have a discretion to decide when and how to exercise those powers. They also have a duty to respect the human rights and dignity of the citizens they serve and protect. There must be a balance maintained and intrusive powers ought not to be exercised unless it is reasonably necessary to do so. In the instance of the second search of your CCRs for a period of five weeks it is my opinion that the intrusion into your privacy was not reasonable even though it was lawful.

The Commissioner of Police disagrees with my view. His view is that the second request to Optus was in accord with "standard investigative techniques ... to establish whether contact between parties is an ongoing occurrence and whether there is a pattern to the conduct....". I have not accepted that view in your case because any contact between you and a police officer prior to the execution of the warrant, on 20 October 2010, was of no relevance to an alleged offence of unlawful disclosure of an event which happened on one occasion only, on either 20 or 21 October 2010. I have given the Commissioner of Police my reasons for the view I hold and I include an extract of my letter to him:

"In my opinion to access phone call charge records for a period of three weeks before the event which precipitated the offence under Section 155 of the Police Administration Act was unreasonable. It was in my view unreasonable because any interaction or communication between Mr O'Brien and any police officer prior to the execution of the warrant on the house in question was not capable of producing any evidence that could logically have carried any probative value. Citizens of the Northern Territory have a human right to privacy, recognised by International

Conventions and Declarations, and to some extent recognised by the Common Law. There was no proportionality between the seriousness of the offence being investigated, the value of any information likely to be obtained and the degree of invasion of Mr O'Brien's human right to privacy. It is the failure to balance the value of his rights against the outcome sought or potentially available that amounts to the exercise of the discretion to access his records being, in my view, unreasonable. In many other cases the investigative techniques you describe might well shift the balance and make the needs of law enforcement or prevention of harm reasonably override a person's right to privacy. I do not believe it was reasonable to do so in this instance."

RECOMMENDATIONS

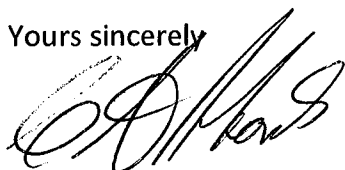
I made four recommendations to the Commissioner of Police. The Commissioner of Police has accepted two of them as follows:

1. The Commissioner of Police will issue a general order to make it patent that access to a person's telephone call records must be authorised by a member of the rank of Superintendent or above.
2. The Commissioner of Police will issue a new authorisation under the *Telecommunications (Interception and Access) Act* replacing the exiting authorisation of Commissioner Paul White authorising only officers of the rank of Superintendent and above only to make requests for telephone call records under the *Telecommunications (Interception and Access) Act*.

I note that you have approached my office concerning a response from NT Police to a request by NT News under the *Information Act* for the release of documents. It is correct that under the *Information Act* documents obtained by EPSC to investigate a complaint against Police that is covered by the *Ombudsman Act* are exempt from disclosure. That exemption arose first when NT Police notified the Ombudsman of the Lord Mayor's complaint on 5 November 2010. No document before that date would be covered by the exemption of documents and information created or obtained under the *Ombudsman Act*. Other exemptions may be applicable but not the exemption created by Section 49C of the *Information Act*. I do not know what documents were requested under the *Information Act* and I cannot investigate any matter arising under the *Information Act* unless it is referred to me by the Information Commissioner.

If you require any further information please contact the Assistant Ombudsman, Bert Hofer. I advise that the notice served relating to disclosure of the draft of this report remains valid. It does not apply to this report.

Yours sincerely



CAROLYN RICHARDS
Ombudsman

Encl.