Submission No 186

Inquiry into potential reforms of National Security Legislation

Name: **The Hon Bruce James QC**
Commissioner

Organisation: **Police Integrity Commission**
GPO Box 3880
Sydney, NSW, 2001

ABN 22 870 745 340

27 August 2012

Our Ref: 3537/94

The Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Sir

Inquiry into potential reforms of national security legislation

Thank you for your letter dated 9 July 2012 inviting the Commission to prepare a submission to the inquiry into potential reforms of national security legislation being conducted by the *Parliamentary Joint Committee on Intelligence and Security.*

I note that the deadline for submissions has been extended by the Committee.

The NSW Government recently made a submission to the inquiry on the issues outlined in the discussion paper published by the Commonwealth Attorney General's Department. The NSW Government submission was drafted in consultation with a number of agencies in NSW, including this Commission. This Commission supports that submission and the recommendations it makes to the Committee.

Given the complex nature of the reforms about which the Committee has been tasked to inquire, this Commission provides the enclosed submission of its own. This submission is provided by way of a particularisation of those issues raised in the submission of the NSW Government which are relevant to the statutory functions of this Commission. It provides the Committee with evidence of how the existing telecommunications interception regime impacts on the operation of bodies, such as the Police Integrity Commission, which are charged with the oversight of law enforcement agencies. The Police Integrity Commission submission also raises issues which the Committee may wish to consider in any inquiry into how a reformed telecommunications interception regime could assist in the strengthening of the oversight, and hence corruption resistance, of law enforcement in NSW. (The NSW Police Force is the largest police force in Australia. This Commission oversights the NSW Police Force and the NSW Crime Commission.)

Should you require any further information please do not hesitate to contact Michelle O'Brien, Commission Solicitor, on 02 9321 6700.

Yours faithfully

The Hon Bruce James QC
Commissioner

LEVEL 3 111 ELIZABETH STREET GPO BOX 3880 SYDNEY NSW 2001 AUSTRALIA
TELEPHONE (61 2) 9321 6700 FACSIMILE (61 2) 9321 6799 FREECALL 1 800 657 079 www.pic.nsw.gov.au

Submission by Police Integrity Commission to Inquiry by PJCIS into potential reforms of national security and TI legislation.

Telecommunications (Interception and Access) Act 1979("the Act")

The establishment of anti-corruption agencies such as the Police Integrity Commission ('PIC') and the Independent Commission Against Corruption ('ICAC') in New South Wales (and thereafter similar agencies in the States and Commonwealth) post-dated the drafting of the original *Telecommunications Interception Act 1979.*[1]

As the number of these agencies grew, the size of the Act also grew with the conferral of interception powers on each new agency. However the legislation did not keep pace with the changing environment by facilitating the smooth and efficient exchange of intercepted information between the anti-corruption agencies and the law enforcement agencies they were oversighting (or between the agencies as joint partners, when they engaged in joint investigations to pursue matters of mutual interest).

Issue 1 – Communication of Intercepted Information between Agencies: section 68

The PIC investigates misconduct by NSW Police Force officers, NSW Police Force administrative employees and NSW Crime Commission officers. The *Police Integrity Commission Act 1996 ('PIC Act')* requires the heads of public authorities, including the NSW Police Force and NSW Crime Commission, to report to the PIC any matter that concerns officer misconduct.

Accordingly the PIC often receives *lawfully intercepted information* containing evidence of officer misconduct which has been recorded pursuant to an interception warrant obtained by another agency. This information is communicated to PIC pursuant to section 68(f) of the Act, being information that relates to a matter that "*may give rise to an investigation by the Police Integrity Commission.*"[2]

On receipt of such intercepted information the PIC may deal with it for a *permitted purpose* pursuant to s67, for example, an investigation of police misconduct.[3] Such use may include further investigation by PIC of the allegations contained in the intercepted information, such as the holding of hearings.

Any outcome from the PIC's investigation is likely to contain, in some form, the original source of the allegations, that is, the intercepted information communicated to the PIC by the other agency. This may include, for example, an intercepted conversation originally communicated to the PIC under section 68 which was then used in evidence in a PIC hearing and formed the basis of a number of questions and answers in the hearing.

Should the PIC resolve that an appropriate outcome at the end of its investigation is to refer the evidence (which contains the original intercepted information) to another agency for appropriate action (i.e. for that other agency's purpose), and the PIC is not the originating agency, the PIC is not permitted to communicate the lawfully intercepted information.

---

[1] For example the Independent Commission Against Corruption was established in 1988, the Police Integrity Commission was established in 1996.
[2] *Telecommunications (Interception and Access) Act* 1979, s 68(f)
[3] See definition of 'permitted purpose' in section 5

Section 68 of the Act only permits the interception agency that "*originally obtained*" the intercepted information to communicate that information to another agency for the purposes of that other agency. As the example below demonstrates, this would prevent the PIC communicating back to the NSW Police Force or the NSW Crime Commission the evidence from a PIC investigation which was initiated as a result of intercepted information communicated to the PIC by the NSW Police Force or the NSW Crime Commission because it concerned misconduct of a NSW Police Force or the NSW Crime Commission officer.

Example 1

In the course of investigating a serious offence the NSW Police Force obtains lawfully intercepted information pursuant to a NSW Police Force warrant which suggests the involvement of a NSW Police Force officer in misconduct. The NSW Police Force communicates this information to the PIC pursuant to s68(f) of the Act.

The PIC conducts hearings and completes an investigation which confirms the officer has engaged in misconduct. PIC resolves to refer its evidence to the NSW Police Force for action against the officer.

However as the evidence which the PIC wants to disseminate to the NSW Police Force contains lawfully intercepted information which originated from the NSW Police Force, and of which the PIC is therefore not the originating agency, the PIC is unable to disseminate the material containing the intercepted information pursuant to s68 of the Act.

Absent the making of a report – which is not conducive to the efficient disposal of matters - there is no other provision in the Act which would allow PIC to communicate the relevant intercepted information back to the NSW Police Force. The NSW Police Force is therefore prevented from using the PIC evidence in dealing with the officer, even though some of that evidence originated from the NSW Police Force's own material.

Recommendation 1 - That the requirement for "*originating agency*" be removed from section 68 in order that agencies can communicate intercepted information between themselves, so long as it is for a *permitted purpose* of the receiving agency. If it is considered that the *originating agency* should retain some control over the subsequent release of its intercepted information - lest prejudice be occasioned to an investigation of the *originating agency* – then the Act could include a provision that the *originating agency's* consent be obtained in such circumstances. This would be preferable to the current restrictive wording of s68.

Issue 2 - Available disciplinary action when intercepted information establishes police or other misconduct

The Act provides that the NSW Police Force and the PIC may use *lawfully intercepted information* for the following permitted purposes (in addition to an investigation of a prescribed offence or a prosecution of same)[4]:

(c) In the case of the Police Force of a State (e.g. NSWPF):

[4] See definition of 'permitted purpose' in section 5

(i) *an investigation of, or an inquiry into, alleged misbehaviour, or alleged improper conduct, of an officer of that State, being an investigation or inquiry under a law of that State or by a person in the person's capacity as an officer of that State; or*

(ii) a report on such an investigation or inquiry; or

(iia) the making by a person of a decision in relation to the appointment, re-appointment, term of appointment , retirement or termination of appointment of an officer or member of staff of that Police Force;

...

(e) In the case of the PIC:

(i) an investigation under the Police Integrity Commission Act of police misconduct (within the meaning of section 5 of that Act) of a police officer (within the meaning of that Act; or

(ia) an investigation under the Police Integrity Commission Act of corrupt conduct (within the meaning of section 5A of that Act) of an administrative officer (within the meaning of that Act); or

(ib) an investigation under the Police Integrity Commission Act of misconduct (within the meaning of section 5B of that Act) of a Crime Commission officer (within the meaning of that Act); or

(ii) a report on an investigation covered by subparagraph (i), (ia) or (ib); or

...

Whilst the above provisions permit the NSW Police Force and the PIC to use intercepted information for the purposes of investigating police misconduct and reporting on same, only the NSW Police Force, as the employer, is in a position to take action against the officer at the conclusion of an investigation. The present wording of the Act provides a limited range of options to the NSW Police Force in cases where the decision to take action relies on evidence sourced from intercepted information. If the investigator is satisfied that misconduct has occurred, but it is not of sufficient seriousness to lead to prosecution for a prescribed offence, then the only other action open to NSW Police Force is that listed in subparagraph (c)(iia) above, i.e. *a decision in relation to the appointment, re-appointment, term of appointment, retirement or termination of appointment* of the officer.

The absence of any other options in subparagraph (c)(iia) means, in effect, that the NSW Police Force is not permitted to use intercepted information to support any form of action which falls short of dismissal, or "*termination of appointment*".

Accordingly, although Part 9 of the *Police Act* 1990 (NSW) sets out a range of disciplinary measures which are open to the NSW Police Force in dealing with a police officer who engages in misconduct, if the evidence supporting that action is from intercepted information, then it would not be a *permitted purpose* under the Act for the NSW Police Force to take any one of the options normally open to it other than termination of appointment or non-renewal of appointment.

If the NSW Police Force was to conduct an investigation and conclude on the basis of intercepted information that misconduct had occurred, and decide, say, to impose a reduction of the officer's rank by way of disciplinary action, the NSW Police Force would be

in breach of the Act, because subsection (c)(iia) does not permit NSW Police Force to use intercepted information in the making of a decision to take such disciplinary action. It would be open to the officer to challenge the decision of the NSW Police Force on those grounds.

This situation leads to the result that many investigations by NSW Police Force and PIC into suspected police misconduct will achieve nothing. This is because if the misconduct is found proved on the basis of intercepted information the New South Wales Police Force will not be able to take any disciplinary action, other than dismissal, and many matters will not reach that threshold.

Accordingly in such matters, where it is clear from the outset that the suspected misconduct under investigation would not, if proved to the requisite standard, result in dismissal, then there is little incentive for the NSW Police Force or the PIC to embark upon such investigations in the first place. This beggars the question of why the Act confers upon both agencies (and their counterparts in other States and the Commonwealth) the power to use intercepted information to investigate police misconduct but ties their hands when they come to take appropriate action at the end of an investigation. The inevitable result is that many investigations do not get off the ground, even if the evidence is strong, because the agency knows it will be a waste of time and resources.

An illustration of such a matter is found in the following 2 case studies.

Example 2

The PIC is investigating allegations that a New South Wales Police Force officer is involved in serious offences. The PIC has a warrant to intercept the officer's mobile telephone for the purpose of investigating those offences.

*The officer is fluent in a foreign language and is sometimes engaged to work as a translator for the New South Wales Police Force. The PIC's intercept has revealed that whilst at work translating calls obtained pursuant to a NSW Police Force interception warrant, the officer played an intercepted call to an associate who was not a police officer by holding his mobile telephone near to the speakers at his work station so that the intercepted information was transmitted via his own mobile telephone to his associate's telephone. This constitutes an unauthorised release of confidential police information as well as an offence against s 63 of the Act. While such an offence could be prosecuted under the Act by virtue of the definition of **prescribed offence** in section 5, it is unlikely that the prosecuting authorities would agree to prosecute in the absence of further evidence, such as hindering an investigation or similar.*

Such conduct should not however go unaddressed. The officer should be disciplined and at the very least transferred out of the position which allows him access to intercepted information. Furthermore the NSW Police Force should be able to take such action immediately (as an officer who has been caught releasing information once may have done it on other occasions and may continue to do it.) Because of the restrictions in subsection (c)(iia) discussed above, however, the NSW Police Force will be unable to use the evidence obtained from the PIC intercept to take any action against the officer. Subsection (c)(iia) only provides for dismissal. Dismissal action involves a lengthy process. In this case, a dismissal based on that incident alone could probably be successfully challenged by the officer as being excessively harsh.

Fortunately, in this case, the PIC subsequently obtained further (non-TI) evidence of other misconduct by the officer which the PIC was able to communicate to the NSW Police Force and which NSWPF was able to use in making the decision to suspend the officer, pending completion of the PIC investigation of the serious offences.

Example 3

The PIC commenced an investigation into allegations that a NSW Police Force officer was releasing confidential police information and had compromised the execution of two NSW Police Force warrants on a person who was suspected of serious firearms and drug offences. The suspect appeared to have prior knowledge that the search warrants were to be executed by police and had taken steps to remove incriminating evidence from the premises. A freelance cameraman also appeared to have been tipped off at one of these compromised search warrants and arrived at one of the premises which was to be searched at the same time the NSW Police Force did.

As a result of these allegations the telecommunication services of both the suspect and the cameraman were intercepted by the PIC to investigate if there was a corrupt relationship between the target and a police officer or between the cameraman and a police officer.

Intercepted communications from the cameraman's mobile phone revealed that he maintained regular contact with several police officers and regularly met with them for lunch and coffee. The interception also revealed that the cameraman obtained information from these officers, mostly about the location of incidents at which the police and other emergency services were attending. Although these incidents were generally of a minor nature, there appeared to be a consistent breach by a number of officers of their code of conduct obligations and the New South Wales Police Force media policy and guidelines.

The relevant intercepted material was communicated to the NSW Police Force however they did not to take any disciplinary action as the material did not support a criminal offence which reached the appropriate threshold or justified dismissal action and, accordingly, the material could not be used for a permitted purpose. Once again, it is likely that there were other releases of police information taking place which were not caught on the PIC intercepts. Nevertheless the NSW Police Force was unable to take any action against the involved officers because of the restrictions on use of intercepted information.

Comment – The above case studies highlight the special position occupied by police officers and the need for special measures in preventing police misconduct.

Police officers exercise a role different to that of most other public officials. They have access to highly confidential information about individuals and organisations, access to detailed knowledge about police investigative methodology, and access to firearms and other weapons. All of these factors create unique opportunities to exploit, intimidate or extort members of the public or organisations. A higher level of accountability must be applied to police officers by virtue of their position, and use of intercepted information is vital in making that accountability effective. The ability to use intercepted information to take appropriate managerial action in all cases where it is indicated is essential in ensuring that police forces are not thwarted in dealing with officers who represent a risk to the integrity and security of police operations.

The NSW Parliament, when replacing the *Listening Devices Act* 1984 (NSW), recognised the need for covertly obtained evidence to be used in managerial decisions involving public officers (not just police). The *Surveillance Devices Act* 2007 (NSW) authorises the NSW Police Force and PIC (and other agencies) to apply for warrants to use listening and other surveillance devices for the purpose of investigating serious offences. Unlike the

Telecommunications (Interception and Access) Act 1979, however, the permitted uses of information obtained pursuant to a warrant under the *Surveillance Devices Act 2007* include the making of a managerial decision in relation to a public officer[5]. Section 40(4)(d) and (e) provides that "*protected information*" (under that Act) may be used, published or communicated if it is necessary to do so for any of the following purposes:

> ...
>
> *(d) an investigation of a complaint against, or the conduct of, a public officer within the meaning of this Act or a public officer within the meaning of a corresponding law and the oversight of such an investigation,*
>
> *(e) the making of a decision in relation to the appointment, re-appointment, term of appointment, promotion or retirement of a person referred to in paragraph (d) or the making of any managerial decision with respect to such a person,*
>
> ...

Recommendation 2 - That the Act be amended so that the permitted options for police forces who find officers engaging in misconduct are not limited to dismissal or prosecution. This would improve the current situation where police forces have to speculate in advance whether a misconduct investigation is worth commencing, on the basis that even if the investigation finds that misconduct had occurred, if it did not reach the threshold of prosecution or dismissal then the police force may be unable to take any action.

Issue 3 - Inconsistency in the use to which "telecommunications data" may be put as opposed to intercepted information, for management and disciplinary purposes

The PIC is authorised to obtain "*telecommunications data*" under Part 4-1 of the Act. The PIC obtains retrospective call associated data under s178(2) and live call associated data under s180(2) of the Act. This data is obtained for the purposes of PIC investigations and may form part of the basis for recommendations arising from such an investigation.

However the PIC is only able to communicate information obtained under Part 4-1 of the Act if the disclosure is "*reasonably necessary for the enforcement of the criminal law.*"[6] Data obtained under s180(2) can also be communicated for the purposes of enforcement of a law imposing a pecuniary penalty or the protection of public revenue.[7]

The threshold test for communication of "*telecommunications data*" is therefore higher than the permitted purpose for communicating "*lawfully intercepted information*", which can be communicated to a police force under section 68 where it relates, or appears to relate, *inter alia,* to an act or omission by a police officer which may give rise to a police disciplinary proceeding against that officer, a decision of the Commissioner to terminate that officer's employment or misbehaviour or improper conduct of an officer.[8]

Recommendation 3 - It is submitted that the purposes for which interception agencies are authorised to communicate "*telecommunications data*" should be made consistent with those of *intercepted information* under the Act.

---

[5] Section 40(4)(c)
[6] Section 178(3) and s182(2)(b)
[7] Section 182(2)(c) and (d)
[8] See section 68(d)(ii), (iia) and (iii)

Issue 4 - Dissemination of intercepted information when in the public interest

The NSW *Surveillances Devices Act 2007* contains the following provision enabling communication of information obtained pursuant to SD warrant:

Section 40(5) – (7) (emphasis added):

> *(5) .. protected information may be communicated or published by a law enforcement officer to any person with the consent of the chief officer of the law enforcement agency of which the officer is a member.*
>
> *(6) A chief officer may consent to the communication of protected information under subsection (5) only if satisfied that it is necessary or desirable in the public interest for the protected information to be communicated to the person concerned and that the public interest in communicating the information outweighs any intrusion on the privacy of the person to whom it relates or of any other person who may be affected by its communication.*
>
> *(7) In deciding whether to give consent the chief officer must take into consideration the manner in which the protected information will be dealt with after it is communicated to the person concerned.*

A similar power also exists in the Victorian *Surveillance Devices Act 1999.* Section 11(2) provides that the general prohibition does not apply to:

> *(b) to a communication or publication that is no more than is reasonably necessary-*
>
> *(i) in the public interest*
> *(ii) ...*

The Act in its present form prescribes the situations in which information obtained under the Act is able to be used. It is noted that the legitimate public interest in the protection of privacy necessitates this strict regime of how, to whom and for what purpose intercepted information may be used and communicated. In authorising the communication of intercepted information in these limited circumstances, however, the Parliament has identified situations where the protection of the privacy of an individual is overcome by another, more pressing, public need. That is, Parliament has acknowledged that there are situations where the privacy of an individual should yield to a greater public interest.

It is trite to observe that legislative drafters are unable to anticipate every situation in which a public interest necessitating disclosure of intercepted information would overcome the public interest in the protection of an individual's privacy. In the PIC's view it would seem doubtful that the legitimate public interest of privacy, sought to be protected by the Act, necessitates inflexibly closing off the use of intercepted information to only the circumstances which are able to be anticipated, and thus included, in the Act.

The PIC considers that in order for the Act to effectively serve the public interest a discretion should be provided which permits the use of intercepted material in situations where a public interest plainly exists in its communication however, due to the idiosyncratic nature of the circumstances, the situation was unable to be anticipated by the drafters of the Act and, as such, no express power to communicate the information was provided (e.g. a situation where an intercept reveals a threat of imminent suicide).

It is acknowledged that such a discretion would be broad and would diverge from the strict protection of privacy embodied in the Act however such a discretionary power would be exercised rarely, in exceptional circumstances and would be tightly controlled. Such controls can be applied by vesting the discretion solely in the chief officer of the agency (or appropriate senior officer of an agency) as has been done in the *Surveillance Devices Act 2007* (NSW). Strict reporting obligations could also be imposed where the chief officer has exercised such a discretion.

Recommendation 4 - It is submitted that such a general power of dissemination be considered. Such a power would permit the dissemination of information where the Chief Officer of an agency deems that there is a public interest in it being so communicated.

It is also submitted that appropriate safeguards should be applied such as ensuring the discretion is exercised only by the Chief Executive Officer and is accompanied by concomitant reporting obligations to the Ombudsman.

Issue 5 - Whether restrictions on communication in the Act override statutory powers of PIC and similar anti-corruption agencies

The PIC's investigative functions require it to oversight the NSW Police Force and the NSW Crime Commission, both interception agencies for the purposes of the current Act. As part of its investigations the PIC may use its statutory powers of investigation to issue notices pursuant to s25 or s26 of the PIC Act. Such notices can require those authorities to produce documents or statements of information within their possession.

Similar notice powers are utilised by other state authorities.[9]

It is anticipated that an issue may arise where:

- the PIC serves a s25 or s26 notice on an agency for the purposes of a PIC investigation;
- the notice requires production of a record that contains "*lawfully intercepted information*" obtained by that agency;
- despite the existence of the PIC investigation, it is the view of that other agency that such material does not "relate" to a matter that may give rise to an investigation by the PIC; and therefore
- the other agency refuses to communicate the information as it is their view that they are unable to do so under section 68(f) of the Act.

It is unclear whether the provisions regulating the communication of information under the Act are intended to override the investigative powers of statutory bodies such as the PIC. The PIC's powers are based in state legislation and therefore would be invalid to the extent of any inconsistency under s109 of the Constitution. A strong argument would seem to exist that the provisions of the Act exhaustively define the circumstances in which intercepted material can be communicated and that, as such, the provisions of s25 or s26 of the PIC Act would yield to section 68 of the Act.

Such an outcome would however frustrate the intentions of the NSW Parliament in establishing the PIC and the intentions of other State Parliaments in establishing their respective anti-corruption agencies. The PIC has been given significant coercive powers to investigate other agencies under its oversight. Such investigations are sometimes unwelcome or viewed unfavourably by those agencies. It is submitted that the obstruction of

[9] See, for example, *Independent Commission Against Corruption Act 1988* s21 & s22

an investigation by a restrictive interpretation of the Act would impede oversight of law enforcement and be contrary to the intention of Parliament.

Recommendation 5 - that consideration be given to including a provision in the Act which clarifies that the provisions of the Act are not intended to prohibit disclosure or use of information if the disclosure or use is required or authorised by law.

It is noted that section 280(1)(b) of the *Telecommunications Act 1997* provides a means by which telecommunications companies can disclose call related data in response to subpoenas issued by state courts (and other legal requirements.)

The section provides:

> *(1) Division 2 does not prohibit a disclosure or use of information or a document if:*
>
> ...
>
> *(b) in any other case—the disclosure or use is required or authorised by or under law.*

It is submitted that a section in similar terms (where the definition of law encompassed state legislation) may be appropriate in order to require to communication of TI records in reply to notices such as those provided for in s25 and s26 of the PIC Act. The effect of such a section should be to compel the production of TI records where that is required by state legislation such as the PIC Act.

Sufficient accountability of the use of such records could be achieved by maintaining the same reporting obligations that exist with other TI material.

Police Integrity Commission
August 2012