Australian Government

Australian Commission for
Law Enforcement Integrity

ALRC Review of Secrecy Laws (Issues Paper 34)

Submission by the Australian Commission for Law Enforcement Integrity (ACLEI)

to the

Australian Law Reform Commission

18 February 2009

1. Introduction

The Australian Commission for Law Enforcement Integrity (ACLEI) welcomes the opportunity to make a submission to the Australian Law Reform Commission (ALRC) in response to Issues Paper 34, *Review of Secrecy Laws*.

The submission is designed to assist the ALRC by providing:

- general information about ACLEI's role in Australian Government administration (Section 2);
- commentary about corruption and the unauthorised access and disclosure of law enforcement information (Section 3); and
- a summary of issues the ALRC might consider when developing its Discussion Paper in the current inquiry (Section 4).

2. Responsibilities and powers of ACLEI

The Role of the Integrity Commissioner

The *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act) commenced on 30 December 2006. The LEIC Act establishes the statutory office of Integrity Commissioner. The Integrity Commissioner is supported by an independent agency, the Australian Commission for Law Enforcement Integrity (ACLEI).

The Integrity Commissioner's role is to:

- detect, investigate and prevent corruption in law enforcement agencies;
- maintain and improve the integrity of staff members of law enforcement agencies; and
- collect and process intelligence on corruption in law enforcement.

The law enforcement agencies, of which the members are subject to the scrutiny of the Integrity Commissioner under the LEIC Act, are the Australian Federal Police (AFP), the Australian Crime Commission (ACC) and the former National Crime Authority (NCA).

Other agencies with a law enforcement function may be added by regulation (s 5, LEIC Act, definition of *law enforcement agency*).

Receiving information about corruption

One important feature of the LEIC Act is that it provides for the mandatory notification, by the relevant law enforcement agency head to the Integrity Commissioner, of information and allegations concerning corruption, irrespective of the source of that information (s 19).

In this way, the LEIC Act establishes an arrangement whereby the Integrity Commissioner and the agency heads, prevent and deal with corruption jointly and cooperatively. The arrangement recognises both the considerable work of the ACC and AFP to introduce internal corruption controls (including detection and deterrence-focussed mechanisms) and the continuing responsibility that the law enforcement agency heads have for the integrity of their staffs.

Also, the LEIC Act provides for the Minister to refer corruption issues to the Integrity Commissioner (s 18), as well as for any other person, including members of the public or other government agencies, to provide information about corruption (s 23).

Further, ACLEI is authorised under the *Telecommunications (Interception and Access) Act 1979* to receive information about any corruption issues involving the AFP or the ACC that may be identified by other integrity agencies or police forces as a result of their telecommunications interception activities.

What are ACLEI's investigative powers?

A challenge facing ACLEI is that law enforcement officers subject to investigation by the Integrity Commissioner are likely to be well-versed in law enforcement methods, and may be skilled at countering them in order to avoid scrutiny. As a consequence, ACLEI has access to a range of special law enforcement powers.

The key investigative powers available to the Integrity Commissioner and ACLEI are:

- coercive information-gathering, including notices to produce evidence or information, or under oath or affirmation in response to a summons;
- telecommunications interception;
- electronic and physical surveillance;
- controlled operations;
- assumed identities;
- search warrants;
- right of entry to law enforcement premises and associated seizure powers;
- arrest;
- scrutiny of financial transactions; and
- access to specialised information databases for law enforcement purposes.

ACLEI may also collect intelligence about corruption in support of its functions.

Certain disclosures to ACLEI are authorised

The LEIC Act, and the AFP and the ACC Acts, include provisions that authorise law enforcement officers to provide information to ACLEI about corruption issues, as follows:

- Subsections 51(2) and (4) of the *Australian Crime Commission Act 2002*, and s 60A(2) of the *Australian Federal Police Act 1979*, permit a serving or former law enforcement officer lawfully to provide to the Integrity Commissioner information and material related to their employment that might disclose a corruption issue.
- Subsection 222(5) of the LEIC Act establishes an immunity from civil proceedings in respect of any information, document or evidence given to the Integrity Commissioner by a law enforcement officer, provided that these were provided in good faith.

One application of these provisions is to enable 'whistleblowers' to bring information directly to ACLEI for independent assessment and investigation. This measure recognises the sensitivities involved in reporting suspicions about corruption from within a law enforcement environment, and the potential for reprisal.

Protecting investigations from compromise, and witnesses from victimisation

Secrecy plays an important role in corruption investigation. The LEIC Act includes special provisions to protect investigations from being compromised:

- Sections 90 and 91 provide for the Integrity Commissioner to direct that particular evidence and information about a hearing, including the fact that a person has given or is about to give evidence at a hearing, be kept confidential. Penalties of up to 12 months imprisonment can apply if a person is found guilty of contravening a confidentiality direction (s 92).
- Section 220 establishes an offence of victimisation in respect of a person who refers a matter, gives information, or produces a document to the Integrity Commissioner.

- In addition, s 104A provides for the Integrity Commissioner to make such arrangements as are necessary to protect the safety of witnesses and intended witnesses (and of others whose safety may be prejudiced as the result of another person giving evidence), and to protect them from intimidation and harassment.

What can be done with evidence?

Where the Integrity Commissioner discovers evidence of an offence, a liability to civil penalty, or evidence that would be admissible in a proceeding under the *Proceeds of Crime Act 2002* (or a State or Territory equivalent), the assembled evidence must be given to the AFP or to any relevant public prosecution agency, or to a relevant State or Territory police force.

With limited exceptions, information provided during a coercive hearing by a witness, who claimed a 'use indemnity', is inadmissible in evidence against the person in criminal proceedings, or any other proceedings for the imposition or recovery of a penalty. Use indemnity applies when a person is not excused from providing information that would incriminate him or her. However, evidence gathered as a result of this information may be admitted in any proceedings against the person, i.e. there is no derivative use immunity.

Evidence about a breach of duty or misconduct that might justify terminating the employment of, or initiating disciplinary proceedings against, a staff member of a law enforcement agency, must be provided to the head of the relevant law enforcement agency. This provision extends also to secondees, and allows the Integrity Commissioner to provide the information to a secondee's home agency. The 'use indemnity' does not apply to disciplinary proceedings.

What are the Integrity Commissioner's other functions?

The Integrity Commissioner must consider the nature and scope of corruption revealed by investigations, and report annually on any patterns and trends in corruption in law enforcement agencies.

Where laws of the Commonwealth or the administrative practices of government agencies might contribute to corrupt practices or prevent their early detection, the Integrity Commissioner may make recommendations for these laws or practices to be changed.

What are the main secrecy provisions that apply to ACLEI?

Appendix One sets out the main secrecy provisions that relate to ACLEI's operational work. The table demonstrates the diversity of regulatory provisions and penalties relating to information handling that apply to ACLEI staff, or that can be imposed upon others as a consequence of their dealing with ACLEI.

3. Unauthorised disclosure of law enforcement information

Protecting and sharing information

As in many other areas of government, collecting, analysing and sharing information is at the heart of law enforcement activity.

Privacy legislation provides some protection against misuse of personal information that has been collected, such as against exposure that would cause embarrassment, impugn reputations, or offend expectations to dignity. Relevant exemptions permit the exchange of some types of personal information for law enforcement purposes.

Freedom of Information legislation further acts to protect key law enforcement information and intelligence from disclosure, for similar reasons to those set out already.

Other legal relationships, such as those that draw on commercial confidence arrangements and appropriate remedy, provide further assurance to those communicating with government.

Accordingly, it is typical to find that well-developed procedures, supervision and IT systems work in concert to regulate the access to, and disclosure of, information held by government agencies. Agencies such as AUSTRAC make it a condition of access that a receiving agency has these sorts of measures in place.

However, once information is accessed or known by a government officer who could disclose it, the effectiveness of control measures ultimately relies upon the professionalism of the officer.

In the case of dealing with official information, secrecy provisions in legislation and the possibility of administrative or criminal sanction, help to determine the professional standards that apply.

Public confidence in law enforcement

In recent decades, digital data storage and retrieval systems have become powerful intelligence aids in the investigation of serious crime. Technology and enhanced cooperation between jurisdictions have enabled unprecedented sharing of information about individuals, groups, property and other assets, and events.

Together, these advances and the legal framework have allowed law enforcement officers to perform their legitimate work more quickly and effectively than has previously been the case.

At the same time, this increase in capability has been accompanied by community concerns about the purposes to which information is put, and the security of that information. These concerns are reflected in legislative protections and other measures, for instance:

- In one State, particular concerns about the collection and secure storage of information by the Victoria Police resulted in the enactment of the *Commissioner for Law Enforcement Data Security Act* 2005 (Victoria).
- In the Commonwealth, it is an offence to gain unauthorised access to data held in a computer that is ‘restricted’ (s 448.1, *Criminal Code Act 1995*, 2 years imprisonment).
- It is also a serious offence to gain unauthorised access to data held in a computer with the intention of committing a serious criminal offence (s 447.1, *Criminal Code Act 1995*).

In short, public confidence is an important factor in the tacit agreement which governments draw upon to authorise, and continue to consent to, the collation and exchange of information by their law enforcement agencies.

Police informers

There are others who may have an interest in the security of law enforcement information. Those who would give information in secret to law enforcement agencies are commonly concerned for their own safety, particularly against reprisals from those whose interests could be adversely affected by the information they provide.

These people seek assurance that their information will not be disclosed, whether through inadvertence or corruption. While the details of the measures law enforcement agencies take to keep information confidential are of little interest to these people, what matters is the reputation of an agency for being able to keep secrets.

The link between corruption and information

There is a long-standing connection between unauthorised information disclosure and police corruption. For example, the value to criminals of obtaining access to confidential law enforcement information has been well noted (see, for example, Royal Commission into the New South Wales Police Service, Final Report, Volume 1, May 1997 – the 'Wood Royal Commission').

The more 'traditional' manifestations of information-centred corruption feature 'tip-offs' ahead of police raids, providing police-held information to private detectives, and disclosing the identity and location of police informers to criminals.

While these apprehensions persist in policing, contemporary concerns also include the unauthorised release of information about counter-surveillance techniques and the exposure of other law enforcement methods used to investigate crime.

Contemporary research in the United Kingdom indicates that unauthorised access and disclosure of police information is more prevalent in that country, relative to other forms of corruption (Miller, 2003. 'Police corruption in England and Wales: An assessment of current evidence'. *Home Office Online Report 11/03. p.13)*.

Unauthorised information access and disclosure can be observed to link with law enforcement corruption risks in several ways:

- Corrupt officers trying to identify whether they are under suspicion;
- Tip-offs of specific police activity, such as an impending raid;
- Spoiling covert operations by alerting targets to surveillance;
- Obtaining specific information from databases to pass to others for private gain; and
- Selling or trading information about police methods and counter-surveillance techniques.

Heightened concern about the seriousness of unauthorised releases of information by police officers is reflected in a recent decision of the Victorian Court of Appeal, upholding convictions for the offence of misconduct in public office:

> *"The accessing of confidential databases held by Victoria Police for the purposes of providing information to [an unauthorised person] must be regarded as most serious. The public is entitled to rely upon the integrity of police officers in investigating and prosecuting agencies. It is entitled to expect*

> *that police officers will not abuse intentionally the trust reposed in them in relation to confidential information."*[1]

Measures taken against unauthorised disclosure

Law enforcement agency heads recognise easily the importance of the flow of information to their agency, whether it comes from other government agencies, from business, from informers, from covert surveillance activities, or from ordinary members of the public. They recognise also the need to share information with other government agencies in appropriate circumstances.

They also recognise that there is a need to protect police methods, particularly those relating to covert operations, especially to protect the personal safety of covert operatives. This same concern extends to protecting the public investment in long-running investigations.

In short, law enforcement agencies have a strong interest in ensuring that information is properly handled, because the impact of their not doing so is great.[2]

Accordingly, it is usual to find that law enforcement agencies have invested in detection systems such as data-access audit trails, 'red-flag' alerts on IT systems, and substantial investment in internal investigation capabilities.

Special enforcement measures

The enforcement of criminal penalties relating to information handling is a key part of the 'detection and deterrence' strategy that seeks to counter corrupt conduct in law enforcement.

Anti-corruption agencies, such as ACLEI, take a central role in government's investment in ensuring that particularly sensitive law enforcement information is not compromised by unauthorised disclosure by individuals as a consequence of their corrupt conduct.

See *Appendix Three* for selected references about investigations that have linked confidential law enforcement information to corrupt disclosure.

The role of penalty provisions

'Confidentiality' or 'secrecy' penalty provisions, howsoever named, are part of this 'detection and deterrence' framework that is designed to control access to government-held information. In Commonwealth law, these provisions include:

- general offence clauses that relate to an employee's duty of confidentiality and fealty, and which prohibit unauthorised disclosure and establish a penalty regime (s 70, *Crimes Act 1914*; s 60A, *Australian Federal Police Act 1979*; s 51, *Australian Crime Commission Act 2002*; s 207, *Law Enforcement Integrity Commissioner Act 2006*);
- targeted deterrence measures, for example Regulation 13B of the *Australian Federal Police Regulations 1979*, which prohibits unauthorised disclosure of information relating to internal investigations of police misconduct; and
- risk-based measures relating to harm and opportunity, for example where harm to a person may eventuate, a higher maximum sentence is sometimes prescribed (s 15XS of the *Crimes Act 1914*, relating to Assumed Identities, is an example).

---

[1] Kellam JA in R v Bunning [2007] VSCA 205 (27 September 2007), cited in Office of Police Integrity (2008) Exposing corruption within senior levels of Victoria Police, Melbourne.

[2] The Wood Royal Commission Report set out the deleterious effects of corruption on the New South Wales Police Force. A common element of many of the corrupt enterprises exposed by the Royal Commission was 'police leaks'. See *Appendix Two*.

The provisions above range from the general to the more specific, matching opportunity and risk to increased regulation and consequence. Legislation in other jurisdictions recognises also the special risks associated with the unauthorised access and disclosure of information by police.

For example, in September 2005, the Director of the Office of Police Integrity recommended to the Parliament of Victoria that the offence and penalty provisions of the *Police Regulation Act 1958* be amended to include a 'with intent' provision relating to the unauthorised disclosure of information, carrying a maximum penalty of ten years imprisonment, where a intentional or reckless disclosure could endanger the safety of a person or prejudice the effective operation of an authorised operation.[3] That recommendation has since been enacted by the amendment of s 127 of the *Police Regulation Act 1958*, proclaimed on 17 October 2007.

This 'special case' approach, may be suited to the Commonwealth regulatory system for protecting official information.

4. Issues for consideration

Since the Integrity Commissioner investigates corruption issues, ACLEI has an interest in the laws that regulate the professional standards of law enforcement agencies and their staff.

In light of the foregoing discussion about the particular corruption risks associated with law enforcement activities, the ALRC may wish to consider the following suggestions in its deliberations.

Law enforcement secrecy as a special case/ class

ACLEI believes that the handling of official information by law enforcement agencies warrants being considered as a special case. The primary reason for this relates to the corruption/ information 'leak' nexus, and the dire consequences for justice and community safety that can result.

Clear, consistent policy messages

ACLEI suggests that this 'special case' approach would result in a refinement of the policy message relating to law enforcement information, namely, that the community consents to the collection, storage and sharing of sensitive information by and with law enforcement agencies, providing that this trust is not betrayed.

This approach would assist to differentiate between the obligation of fealty that an employee would ordinarily owe an employer, and that which ought to accompany the responsibility of handling information that has been collected or acquired for a law enforcement purpose.

Matching penalty to risk

To achieve this aim, ACLEI suggests that consideration be given to the following special measures to protect information against misuse in a law enforcement context:

1. Separate statutes

ACLEI prefers a situation where the main secrecy provisions that apply to law enforcement agencies are retained in each agency's principal statute. An alternative approach could be to create a separate statute that deals specifically with handling law enforcement information, and requisite secrecy/confidentiality arrangements and penalties.

[3] Office of Police Integrity (2005) Investigation into the publication of *One Down, One Missing*. Melbourne.

2. Achieving consistency
Currently, there are differing penalty provisions for unauthorised disclosure of information that apply to staff who work in the ACC and the AFP. As a minimum, the ACC Act secrecy provision pertaining to staff should be made consistent with that which applies under the AFP Act.

3. Higher penalty
One approach may be to also raise the penalty provision in the ACC Act (s 51), the AFP Act (s 60A) and the LEIC Act (s 207) to a level higher than two years imprisonment.

4. Escalation model
Another possibility may be to adopt an escalation model linked to potential harm, adopting the approach recently taken in Victoria (s 127 of the *Police Regulation Act 1958*). This model could equally cover 'intention' and 'recklessness'.

5. Corrupt intent
Another way may be to specify 'corrupt intent' as an aggravating factor relating to penalties. The seriousness of the offence ought to carry a penalty of no less than seven years imprisonment.

6. Special classes of information
Yet another approach could be to provide additional protection to special classes of information. Currently, some Commonwealth legislation recognises that particular types of sensitive information require proportionate protection. This approach may be because of sensitivities related to:

- the source of the information (eg, the AUSTRAC or CRIMTRAC databases);
- the way the information was collected (eg, the intrusive nature of surveillance devices and telecommunications interception); or
- the harm that might be caused by uncontrolled disclosure (eg, s 15XS of the *Crimes Act 1914*, relating to Assumed Identities).

ACLEI suggests that there may be other classes of law enforcement information that could be considered for special protection, namely information relating to:

- the identities of Registered Informants, and
- police covert methods.

7. Strict liability
It may also be that strict liability could apply to certain fault elements of an offence in particular circumstances, including harm related to providing information that could:

- reveal the identity of a Registered Informant or a covert operative;
- reveal covert methods; or
- seriously prejudice the effectiveness of an authorised law enforcement operation.

While this approach could reduce any penalty a court might otherwise consider just, it would overcome many of the barriers to commencing a prosecution, namely that initiating a court case might risk revealing or publicising other confidential information, notwithstanding that public interest immunities are sometimes available.

In ACLEI's observation, it is the prospect of prosecution and imprisonment that would most trouble the mind of a law enforcement officer, and would therefore be an effective deterrent.

8. Subsequent unauthorised disclosure

ACLEI has a concern about inappropriate associations between current and former staff of law enforcement agencies, including where the former officer acts as an intermediary for criminals.[4] ACLEI notes that the same damage, and sometimes more, can result from a secondary disclosure as it can from the primary disclosure.

Accordingly, ACLEI believes that the criminalisation of 'subsequent unauthorised disclosure' would be a valuable deterrent against corrupt (intentional) disclosure.

9. Targeted deterrence: Anti-collusion

ACLEI notes Regulation 13B of the *Australian Federal Police Regulations 1979*, which prohibits unauthorised disclosure of information relating to internal investigations of police misconduct. ACLEI suggests that there may be merit in placing this provision in the AFP Act, and attaching a penalty to it.

A similar approach could be adopted under the ACC Act, which currently does not have a provision of this type.

An alternative approach could be to characterise collusive disclosure in relation to an internal misconduct investigation as an aggravating factor in the 'escalation' model or the 'special class' model discussed above.

[4] Annual Report of the Integrity Commissioner, 2007-2008, p.52.

Appendix One – Main secrecy provisions applying to ACLEI's operational work

Law Enforcement Integrity Commissioner Act 2006			
Section	Type	Effect	Maximum Penalty
s 207	Offence provision	Establishes confidentiality requirements for ACLEI staff.	Imprisonment for 12 months or 60 penalty units, or both.
s 208	Exception provision	Establishes general exceptions to confidentiality requirements.	n/a
s 209	Exception provision	Establishes capacity for the Integrity Commissioner to disclose information publicly , where it is in the public interest.	n/a
s 210	Procedural fairness provision	Sets out a procedural fairness model where a public disclosure under s 209 would involve publication of an opinion or finding that is critical of a government agency or a person.	n/a
s 216	Exception provision	Establishes authority for the Integrity Commissioner to provide information to the Parliamentary Joint Committee on ACLEI.	n/a
s 90	Offence provision	Establishes capacity for the Integrity Commissioner to direct that confidentiality arrangements apply to evidence given at a hearing, to protect reputation or safety, effectiveness of an investigation, fair trial, protection of confidential/sensitive information.	Imprisonment for 12 months.
s 91	Enabling provision	Establishes capacity for the Integrity Commissioner to direct that disclosure of a summons is prohibited.	See s 92.
s 92	Offence provision	Relates to prohibited disclosure in contravention of s 91, including second parties.	Imprisonment for 12 months.

Public Service Regulations 1999			
Section	Type	Effect	Maximum Penalty
Regulation 2.1 (Act s 13)	Conduct requirement	Establishes a 'conduct requirement' or 'duty' not to disclose information, against which an unauthorised disclosure may lead to a breach of the APS Code of Conduct, and consequential administrative/disciplinary sanctions.	Breach of the APS Code of Conduct (see s 15 of the PS Act).

Crimes Act 1914			
Section	Type	Effect	Maximum Penalty
s 70 (re general disclosure)	Offence provision	Establishes confidentiality requirements for all public servants (including ACLEI staff).	Imprisonment for 2 years.
s 15XS (re assumed identities)	Offence provision	Establishes confidentiality requirements where the disclosure endangers or is likely to endanger the health or safety of a person, or prejudices, or is likely to prejudice, the effective conduct of an operation.	Imprisonment for 10 years.
s 23YO (re DNA/NCIDD database)	Offence provision	Establishes offence of reckless disclosure relating to the DNA/NCIDD database, where a person's identity could be revealed.	Imprisonment for 2 years.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 **(the AMLCTF Act)**			
Section	Type	Effect	Maximum Penalty
120	Offence Provision	Prohibits unauthorised disclosures by the Integrity Commissioner.	Imprisonment for 2 years or 120 penalty units, or both.
123	Offence Provision	Prohibits 'tipping-off'.	Imprisonment for 2 years or 120 penalty units, or both.
127	Offence Provision	Prohibits ACLEI from making unauthorised disclosures relating to records from the AUSTRAC database.	Imprisonment for 2 years or 120 penalty units, or both.
128	Exception provision	Exceptions to s 127 (authorised handling/ use).	n/a

Taxation Administration Act 1953			
Section	Type	Effect	Maximum Penalty
s 3E	Offence provision	Requirements relating to secondary handling of taxation information. Includes exceptions.	Imprisonment for 2 years or fine of $10,000, or both.

Income Tax Assessment Act 1936			
Section	Type	Effect	Maximum Penalty
s 16	Offence provision	Information-handling requirements relating to taxation information.	100 penalty units or imprisonment for 2 years, or both.

Surveillance Devices Act 2004			
Section	Type	Effect	Maximum Penalty
s 45	Offence provision	Information-handling requirements relating to protected information. Includes exceptions.	Imprisonment for 12 months, or 10 years if unauthorised handling endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence.

Telecommunications (Interception and Access) Act 1979			
Section	Type	Effect	Maximum Penalty
s 63	Enabling provision (interceptions and warrants)	No dealing in intercepted material or interception warrant information. Exceptions are at s 67 (& 73), 68, 74, 75A.	See s 105.
s 105	Offence provision (interceptions and warrants)	Contravention of s 63.	Imprisonment for 2 years as an indictable offence, or 6 months in a Court of summary jurisdiction.
s 133	Offence provision (stored communications)	Information-handling requirements relating to protected information.	Imprisonment for 2 years or 120 penalty units, or both.
s 182	Offence provision (call charge records, etc)	Prohibits subsequent disclosure of call charge records obtained under Part 4-1, Division 4.	Imprisonment for 2 years.

Appendix Two – The effects of police corruption

2.70 So far as the [New South Wales Police] Service is concerned, the presence of corruption, particularly of a systemic or entrenched kind, means that:

- the security and viability of operations directed at organised crime are threatened by the risk of leaks and compromise, thereby lessening its worth as a law enforcement body;
- the personal safety of informants, undercover officers and dedicated police cannot be guaranteed;
- the trust of the various sections of the community and of government is weakened;
- the reputation of the Service as a protector of the community is diminished;
- the Service is less likely to attract the most able and suitable recruits, or to retain the officers of integrity and skill that it needs;
- the more able and dedicated officers are less likely to seek promotional transfers to areas known to be high risk, thereby entrenching the problem in those commands;
- the Service risks repetitive scandal and increasing external intervention into its affairs;
- the Service is less likely to receive assistance from the community, whether in the form of crime reporting and intelligence, or in the form of assistance of individual officers in need;
- the Service is unlikely to receive a favourable hearing in relation to requests for budget increases, expansion of its resources or improved terms and conditions of service;
- the Service is likely to be denied co-operation on the part of other law enforcement agencies in relation to sharing of intelligence and participation in joint operations;
- the overall confidence of the judiciary, and of jurors, is likely to be diminished, thereby risking the success of prosecutions that were, in fact, based upon sound, honest investigations;
- the innocent may be convicted of crimes which they did not commit, and the guilty may escape justice;
- once officers have succumbed to corruption they are potentially compromised for all time, and become not only vulnerable to blackmail or pressure from other police to ignore their misconduct, but also practised in the art of deception and cover-up; and
- the corrupt who often are the more cunning and forceful members of the Service are likely to gather in powerful cliques, to then use their influence to hijack the promotional opportunities of the more honest, and to resist any attempts at reform.

- Royal Commission into the New South Wales Police Service (1997) Final Report, Volume I: Corruption. Sydney.

Appendix Three – Selected references about protecting confidential law enforcement information.

Information-handing standards:

Commissioner for Law Enforcement Data Security (2007) Standards for Victoria Police law enforcement data security. Melbourne.

Investigation and Research Reports:

Independent Commission Against Corruption (1992) Report on the unauthorised release of government information. Sydney.

Independent Commission Against Corruption (1994) Report on investigations into matters relating to police and confidential information. Sydney.

Royal Commission into the New South Wales Police Service (1997) Final Report, Volume I: Corruption. Sydney.

Queensland Criminal Justice Commission (2000) Protecting Confidential Information: A report on the improper access to, and release of, confidential information from the police computer systems by members of the Queensland Police Service. Brisbane.

Office of Police Integrity (2005) Report on the leak of a sensitive Victoria Police information report. Melbourne.

Office of Police Integrity (2005) Investigation into the publication of *One Down, One Missing*. Melbourne.

Office of Police Integrity (2008) Exposing corruption within senior levels of Victoria Police. Melbourne.

ACLEI (2008) An investigation into an allegation that the Australian Federal Police 'tipped-off' a Federal Member of Parliament about an impending search. Report 02/2008.

Police Integrity Commission (2008) Unauthorised disclosure of confidential information by NSW Police officers. Research and Issues Papers, Number 2. Sydney.

Media Reports:

PC jailed for leaking information. *BBC News*, http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk/3713816.stm, published 4/10/2004.

Conflicting forces hamper police. *The Age*, Nick McKenzie and Richard Baker, http://www.theage.com.au/national/conflicting-forces-hamper-police-20081202-6pso.html, published 3/12/2008.

Officer Amerdeep Johal 'used police files to find blackmail targets'. *The Times,* Adam Fresco, http://www.timesonline.co.uk/tol/news/uk/crime/article5308835.ece, published 9/12/2008.

Long path to a key moment in police history. *The Age*, Nick McKenzie. http://www.theage.com.au/national/long-path-to-a-key-moment-in-police-history-20090213-877i.html, published 14/2/2009.