NSW
Police Integrity
Commission

Research
and Issues
Papers

NUMBER 02

OCTOBER 2008

Police Integrity Commission
Level 3, 111 Elizabeth Street
Sydney NSW 2000

www.pic.nsw.gov.au

Unauthorised Disclosure of Confidential Information by NSW Police Officers

Julie People

Summary

The unauthorised disclosure of confidential information by New South Wales (NSW) police officers is a form of misconduct that can have serious consequences for the police officers involved and the community. Data sourced from complaints was used in this study to describe patterns in the characteristics of unauthorised disclosures of confidential information by NSW police officers. In total, 104 complaints regarding leaks of information received between 1 November 2006 and 30 June 2007 were examined. A number of patterns are described including details of the relationships between police officers and the persons to whom information is allegedly leaked, the source of the alleged leaked information, the benefits and consequences to police officers from allegedly leaking information and the involved officer's attitude regarding the alleged leak of information. Case studies are also presented. The most significant results from this study indicate that there is confusion, misunderstanding and lack of awareness regarding confidential information and its use and dissemination within and outside the NSW Police Force. Implications for management are discussed and finally, a response from the NSW Police Force is presented.

1. Introduction

The New South Wales (NSW) Police Force holds large amounts of confidential information, much of which is readily accessible to police officers. The unauthorised disclosure of confidential information, or the 'leaking' of confidential information, is a form of police misconduct that can have serious consequences for both the police officers involved and the community. Management action can be taken against police officers who leak information and, if the case is particularly serious, they can be charged with an offence and/or dismissed from the NSW Police Force. More importantly, leaks of information also have the potential to cause harm to other persons, the community and/or organisations.

For example, in Queensland, a woman's privacy was breached when a police officer disclosed her silent telephone number to a man who had stalked her for many years (Criminal Justice Commission 2000 p.19). In NSW, information leaked to criminals helped them to continue their activities (Independent Commission Against Corruption 1994). Investigations were jeopardised when police officers disclosed confidential information to suspects in NSW (Police Integrity Commission 2005) and in Victoria (Office of Police Integrity 2008). In a separate case in Victoria, confidential information

leaked to the media included details of facts provided to the police by an informant. Shortly after this information was published, the informant and his wife were murdered (Office of Police Integrity 2005).

It is impossible to know how many leaks of information occur. Estimating the number of instances of leaks of information or of any other type of misconduct by police officers is a very difficult task. Data collected from complaints about police officers is often used as an indicator of the prevalence of misconduct. There are, however, problems associated with using this data as an indicator, particularly for leaks of confidential information.

Not all instances of misconduct will lead to a complaint, especially in the cases where persons are in agreement to conduct corrupt activities (Criminal Justice Commission 1997). Complaints about leaks of information are more likely to be made when there is a victim involved who knows or suspects that information about them has been leaked. This is particularly problematic for leaks of information because victims are often not aware that information about them has been disclosed to other persons, hence they cannot make a complaint (Criminal Justice Commission 2000).

Also, the number of complaints made about police officers can vary over time due to reasons independent of the level of police misconduct, such as changes in public willingness to complain or changes in the amount of contact between police officers and the public (Criminal Justice Commission 1997).

Members of the public may be reluctant to complain about police officers. When asked whether they would complain about an incident involving a police officer, approximately 50 to 75 per cent of people said they were likely to complain (Criminal Justice Commission 1997). The more serious the incident, the more likely they were to complain. When the same people were asked whether or not they had actually made a complaint about a police officer, only 38 per cent of people who felt they had a reason to complain had actually done so (Criminal Justice Commission 1997).

Many complaints are difficult to investigate and substantiate because of a lack of evidence (e.g. Goldsmith 1991; Prenzler 2004). Other complaints are dismissed because of lack of details about the alleged misconduct. Generally, a small proportion of complaints are substantiated. In some cases, the proportion is ten per cent or less (Goldsmith 1996; Criminal Justice Commission 1997; Ede et al. 2002). Therefore, substantiation rates most probably underestimate the true prevalence of misconduct by police officers (Goldsmith 1996; Criminal Justice Commission 2000; Ede et al. 2002).

Another problem with using complaints data as an indicator of prevalence is that complaints do not necessarily indicate that misconduct has occurred. Some complaints are the result of misunderstandings between complainants and police

officers or misunderstandings by the complainant about events that occurred. Some complaints can be fabricated.

For all of the reasons described above, it is clear that data sourced from complaints cannot tell us how many instances of police misconduct occur. This data can, however, provide important information regarding the characteristics of instances of misconduct, including the ways in which they occur, the reasons behind them and their consequences. The data sourced from complaints that are substantiated is particularly useful to help identify problem areas, better manage misconduct and help prevent it.

The data sourced from complaints that are not substantiated is also useful. While some complaints are false or not made in good faith, the proportion of these is unlikely to be large because most complainants genuinely feel they have something to complaint about (Maguire and Corbett 1991). Further, if complaints are obviously false or not made in good faith, they can be declined for investigation by the NSW Police Force (*Police Act 1990*). Complaints that are not substantiated most likely occur because of misunderstandings, confusion regarding procedures used by the police or lack of evidence (Goldsmith 1991, Alpert and Smith 1999, Prenzler 2004).

Data from complaints that are not substantiated can also be used in the management and prevention of misconduct. Patterns obtained from the data can help to identify problem areas where procedures used by the police are unclear, where misunderstandings are common or where finding sufficient evidence to substantiate complaints is difficult. Preventing misunderstandings and clarifying procedures used by the police can also help to reduce the number of complaints made against them.

This study uses data sourced from complaints to describe the characteristics of alleged instances of unauthorised disclosures (or leaks) of confidential information by NSW police officers. Specifically, the information from the allegations made in complaints is used to describe patterns regarding:

- the proportion of complaints that are substantiated;
- the ways that alleged leaks of information are discovered;
- the persons who make complaints regarding leaks of information;
- the number of police officers involved in each alleged leak of information;
- whether police officers are named in the allegations of leaked information;
- whether the complaints include details that the alleged leak of information was an isolated occurrence;
- the relationship between the police officer(s) who allegedly leaked the information and the person(s) to whom information was allegedly leaked;
- the purposes, benefits and consequences of each alleged leak of information;

- the source of alleged leaks of information and whether the complaints include details that the information is obtained specifically by the police officer(s) involved;
- the methods used to allegedly leak information;
- other types of misconduct that are reported in conjunction with complaints regarding leaks of information; and
- police officer's attitudes regarding information they are alleged to have leaked and whether the officers are aware of the NSW Police Force's policies regarding confidential information.

Documenting the patterns regarding the characteristics of unauthorised disclosures of confidential information is an important step in the management of this type of misconduct. Such information is useful to ensure the management of this type of misconduct can be made more specific, focussed and targeted to prevent leaks of information from occurring and to deal with leaks of information once they occur. This study aims to identify the most common characteristics of leaks of information sourced from complaints. Once the characteristics of leaks of information are described, the implications of the patterns detected are discussed. Advice and suggestions to further assist the NSW Police Force with the management and prevention of this type of misconduct are then provided. The final section of this report includes the response from the NSW Police Force regarding the outcomes of this study and of some further work done by the Police Integrity Commission (PIC).

2. Methods

Complaints about NSW police officers are generally made to the NSW Police Force, the NSW Ombudsman's Office or the PIC. Once a complaint is made, it is entered into C@tsi, the NSW Police Force's complaints management system. This system electronically stores and files all documents associated with the complaint and its investigation, including a unique identity number, letters received from complainants, transcripts of interviews with police officers or informants, documents used in the investigation of the complaint, an investigator's report on the complaint and any other relevant documents. Each entry in C@tsi is also given a brief title to describe the subject of the complaint.

Complaints are generally investigated by the NSW Police Force unless they are of a very serious nature, in which case they may be investigated by the PIC. Some complaints are declined for investigation, such as those where the complaint is considered frivolous, vexatious or not made in good faith or the conduct complained of occurred too long ago to justify an investigation (*Police Act 1990*).

Complaints that are investigated are finalised after a decision is made regarding the outcome of the investigation. Once finalised, a report, described as a Section 150

report (*Police Act 1990*) is created and stored in C@tsi. This report may contain copies of the documents described above and details of the outcome of the investigation. Generally, if the misconduct described in the complaint has been proven to occur, the outcome of the investigation is that the complaint is 'sustained'. Complaints are generally 'not sustained' if there is no evidence of misconduct or if the police officer involved in the misconduct cannot be identified.

Complaints recorded in C@tsi and received between 1 November 2006 and 30 June 2007 were used in this study. All complaints with sufficient details available on C@tsi by 15 December 2007 were included. The titles of complaints were manually searched to find those which included a reference to an unauthorised disclosure of confidential information. Complaints with titles similar to unauthorised disclosures of information, ambiguous titles or titles for other types of misconduct which could have included an unauthorised disclosure of information (such as inappropriate associations) were also carefully read to determine if there was any mention of confidential information being disclosed without the authority of the NSW Police Force. Only complaints that included a specific reference to an unauthorised disclosure of information were used in this study. Complaints relating to unauthorised access to the Computerised Operational Policing System (COPS) were not included in the study unless an unauthorised disclosure of information was mentioned.

This method of searching complaints may not find every complaint regarding unauthorised disclosure of confidential information. Although uncommon, it is possible that some complaints with titles unrelated to an unauthorised disclosure of information (e.g. excessive use of force, sexual assault) contain a complaint regarding this type of misconduct.

The details for each complaint included in this study were sought from the Section 150 report within the C@tsi file. Some complaints did not include a Section 150 report, generally because the report was not yet officially finalised. In some of these cases, the C@tsi file included an investigator's report or sufficient details that could be used in this study. When details regarding the investigation of the complaint and the outcome of the investigation were not available, the complaint was not included. Complaints that were declined for investigation were also not included.

The following details of each complaint and its investigation were obtained from the C@tsi files:

- how the alleged leak of information was discovered;
- who made the complaint (type of complainant);
- the number of police officers involved in the alleged leak of information;
- whether a police officer was named in the complaint;

- whether the complaint indicated that the alleged leak of information was an isolated occurrence;
- the relationship between the police officer who allegedly leaked the information and the person to whom information was allegedly leaked;
- the purpose of the alleged leak of information as described by the complainant;
- the benefit (to the police officer) from the alleged leak of information;
- the source of the alleged leaked information;
- whether the complaint included details indicating that the information was obtained specifically by the police officer;
- the method used to allegedly leak the information;
- other types of misconduct that were reported in conjunction with the complaint regarding the leak of information;
- the consequence of the alleged leak of information;
- the involved police officer's attitude regarding the alleged leak of information; and
- whether the police officer involved was aware of the NSW Police Force's policy regarding confidential information.

In addition to the collection of the above details, the PIC assessed each complaint to decide whether a leak of information occurred, independently of the decision made by the NSW Police Force. The assessment of the complaints by the PIC is not intended to replace the outcomes of the investigations or the decisions made by the NSW Police Force. Its purpose is simply to assess whether information was leaked and to classify the complaints of leaks of information in an independent manner. Complaints were classified into two categories; substantiated and not substantiated. The complaint was classified as substantiated when there was an actual unauthorised disclosure of confidential information, regardless of whether it was intentional or not, or whether or not the police officer who leaked the information was identified. In some instances, the police officer involved admitted that he or she leaked information. In other instances, sufficient evidence was found during the investigation of the complaint to substantiate it. Some complaints were classified as substantiated by the PIC when it was obvious that information had been leaked because confidential information that only the NSW Police Force held was made available to persons outside the NSW Police Force. The complaint was classified as not substantiated by the PIC when the investigation showed sufficient evidence that a leak of information did not occur or when there was no sufficient evidence that a leak of information did occur.

Some of the details of the complaint, as described above, were then classified into a number of categories as shown in Table 1.

Table 1. The categories used to classify specific details of the leak of information.

Detail	Categories
How the alleged leak of information was discovered	In the media A complaint was made The information was written in a report Through conversations Through investigations of other matters Detected by the NSW Police Force's security system
Type of complainant	Anonymous Member of the public Police officer Victim of the leak of information
Relationship between police officer and person to whom information was allegedly leaked	Criminal or criminal group Family member Friend or associate Media/journalist Member of the public Other police officer Unknown
Purpose of the alleged leak of information	Accidental (no purpose) Curiosity or gossip Grudge against the NSW Police Force Grudge against a person or organisation other than the NSW Police Force To locate or contact someone Part of the police officer's job Tip offs Other Unknown
Benefit from the alleged leak of information	None Avoided trouble with the law Financial Person located or contacted Personal satisfaction Unknown
Source of the alleged leaked information	Written in a separate complaint COPS Other types of police files Knowledge required for/during an investigation Office knowledge Unknown
Method used to allegedly leak information	Email or electronic Face-to-face Fax Published in a report Written in court papers Media interview Overheard by others Phone Unknown
Consequence of the alleged leak of information	None Criminals evaded the law An investigation was compromised An individual's privacy was compromised The reputation of the NSW Police Force was tarnished Unknown
Involved police officer's attitude regarding the alleged leak of information	Admitted it was wrong Denied it Did not realise it was wrong Claimed it was an accident Claimed it was part of the job Claimed it was the right thing to do Claimed it was necessary to warn someone about criminals Unknown

Data was split according to the outcome of the PIC's assessment of the complaint (i.e. whether the complaint was substantiated or not substantiated). The data presented in this study therefore describe alleged leaks of information where the complaint was not substantiated as well as proven leaks of information where the complaint was substantiated. Data is presented for all complaints used in this study, unless otherwise indicated.

Case studies of incidents of leaks of information were also compiled from the details available in C@tsi. These case studies were chosen to be representative of the types of complaints used in this study.

3. Results

In the eight months between 1 November 2006 and 30 June 2007, 128 complaints were found on C@tsi that mentioned an unauthorised disclosure of confidential information. Of these, 17 were not finalised and did not contain sufficient details to be included in this study. A further seven were declined for investigation by the NSW Police Force. Therefore, 104 complaints were used in this study. One-quarter of these (26) were classified by the PIC as substantiated and the remaining complaints (78) were classified as not substantiated. Interestingly, of the 78 complaints which were not substantiated by the PIC, 35 were given this outcome because there was no evidence that a leak of information had occurred. In some of these cases, this finding occurred because there were insufficient details provided in the complaint to investigate the matter fully.

3.1. Details of the complaint

The vast majority (84 of 104) of leaks or alleged leaks of information were first brought to the attention of the NSW Police Force when a complaint was received. Of these, 18 were substantiated. The remaining 20 (of 104) complaints regarding leaks of information were reported by police officers who discovered them through a variety of methods, as shown in Figure 1.

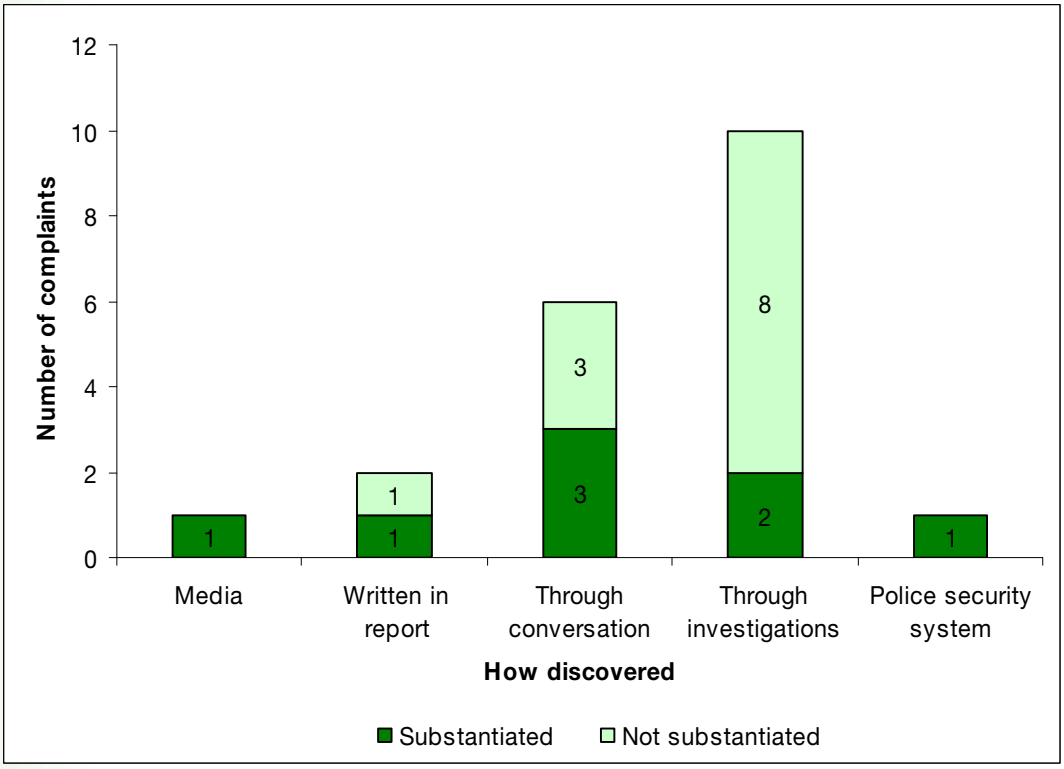


Figure 1. The ways in which alleged leaks of information were discovered (excluding when discovered through complaints) by outcome of the PIC's assessment, n=20.

These 20 complaints were made when a leak or a potential leak of information was discovered via the media (1), written reports, such as those presented to other organisations (2), conversations with other persons (6), other investigations (10) or the NSW Police Force's security system, which detects outgoing emails with certain types of confidential information (1). Eight of the 20 complaints discovered in these ways were substantiated. An example of a complaint where the alleged leak of information was discovered through investigations is given in Case study 1.

Case study 1. An alleged leak of information discovered through a police investigation.

During an investigation, a male suspect revealed that he had spoken to another male who received confidential information about being monitored by the police. The police officer who allegedly disclosed this information was named. An investigation was conducted but there was no evidence that confidential information had been leaked. The complaint was not substantiated.

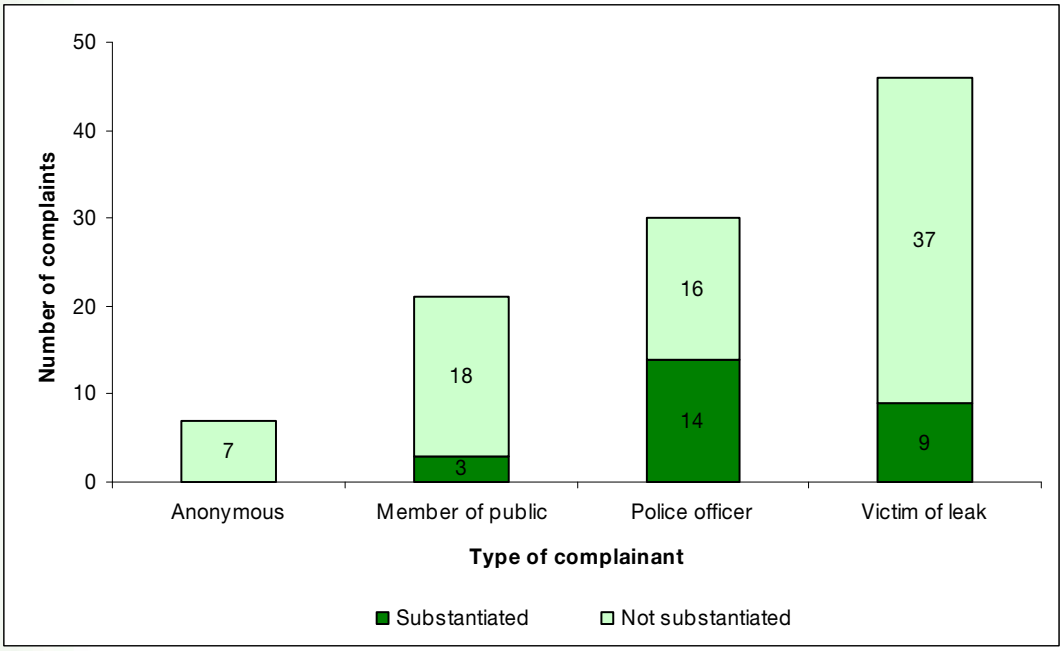


Figure 2. Types of complainant by outcome of the PIC's assessment.

Figure 2 shows the number of complaints made by types of complainants by outcome of the PIC's assessment. Forty-six complaints were made by persons who believed they were victims of information that had been leaked. Of these, nine (20%) were substantiated. Thirty complaints were made by police officers and 14 of these were substantiated (47%). Members of the public made 21 complaints, of which three were substantiated (14%). The smallest number of complaints (7) was made by persons who wished to remain anonymous, none of which were substantiated.

Complaints were therefore most likely to be substantiated when made by police officers (47%) and least likely to be substantiated when made by anonymous persons (0%). There are many reasons to explain this result. One possibility is that complaints made by police officers are most likely to be substantiated because police officers provide the greatest number of details regarding the leak of information compared to other types of complainants. Similarly, it is possible that complaints made by anonymous persons are least likely to be substantiated because they provide the least number of details regarding the leak of information.

To examine this, the number of categories in which details were provided by each of the four types of complainants was compared. Data regarding only the categories that were most likely to assist in investigating a complaint was considered. These were:

- the number of police officers involved in the alleged leak of information;
- whether a police officer was named in the complaint;

- whether the alleged leak of information was an isolated incident;
- the relationship between the police officer alleged to have leaked the information and the person to whom information was allegedly leaked;
- the purpose of the alleged leak of information;
- the benefit from the alleged leak of information;
- the source of the alleged leaked information; and
- the method used to allegedly leak the information.

The number of categories for which each complainant provided details of the leak of information was then calculated. This was done by calculating the number of anonymous complainants who provided details for all eight categories described above, for only seven of the categories described above, for only six categories and so forth. This was repeated for each type of complainant. The results are summarised in Table 2. Cumulative percentages of the total number of complainants that included details for one to eight categories were calculated for ease of comparison.

Table 2. Number of categories for which details were provided and the percentage of complaints that included details for one to eight categories by type of complainant.

Number of categories	Type of complainant							
	Anonymous		Member of the public		Police officer		Victim	
	n	Cumulative %	n	Cumulative %	n	Cumulative %	n	Cumulative %
8	0	0.0	3	14.3	12	40.0	14	30.4
7	0	0.0	2	23.8	3	50.0	13	58.7
6	1	14.3	1	28.6	5	66.7	2	63.0
5	0	14.3	3	42.9	2	73.3	7	78.3
4	1	28.6	8	81.0	4	86.7	5	89.1
3	5	100.0	3	95.2	3	96.7	3	95.7
2	0	100.0	1	100.0	0	96.7	1	97.8
1	0	100.0	0	100.0	1	100.0	1	100.0
Total	7		21		30		46	

As shown in Table 2, none of the anonymous complainants provided details for all eight categories, 14 per cent of members of the public provided details for all eight categories, as did 40 per cent of all police officer complainants and 30 per cent of all victims. When complainants who provided seven of the eight categories were considered, the greatest number of details was provided by victims, followed by police officers, members of the public and anonymous complainants. As the number of categories for which details provided decreased, the percentages of police officers and victims who provided details for the same number of categories was similar. Case study 2 describes an example of details provided by an anonymous complainant.

Table 2 also shows that complaints made by anonymous persons are least likely to include details for more than six categories. Anonymous complainants were most likely to provide details regarding the number of police officers involved in the alleged incident and the relationship between the police officer who allegedly leaked the information and the person to whom the information was allegedly leaked.

Case study 2. Anonymous caller alleged that police officers were involved in tipping off drug dealers.

An anonymous person called crime stoppers and stated that two police officers, whom he named, were involved in tipping off drug dealers in his local area. No other information was provided. The matter was investigated, but there was no evidence that either of those police officers was involved in the alleged misconduct. The complaint was not substantiated.

3.2. Details provided in complaints

Table 3 shows the number of police officers who were alleged to have leaked information in each complaint. The vast majority of complaints (82) indicated that one police officer disclosed confidential information; 23 of these cases were substantiated. Only eight complaints included details that two police officers were involved in the alleged leak of information. Three of these instances were substantiated. In the remaining 14 cases, details were not provided regarding the number of police officers involved in the leak of information. No complaints indicated that more than two police officers were involved in an alleged leak of information.

Table 3. Number of police officers who were alleged to have leaked information in each complaint by outcome of the PIC's assessment.

Number of police officers	Outcome of assessment		Total
	Substantiated	Not substantiated	
1	23	59	82
2	3	5	8
Unknown	0	14	14
Total	26	78	104

Complainants provided the name of the police officer involved in the alleged leak of information for 66 of the 104 complaints. Of these 66 complaints, 24 were substantiated. Police officers were not named in the remaining 38 complaints. For two of these, the complaint was substantiated. Therefore, in these two cases, there was evidence that information was leaked, but the police officer who leaked the information could not be identified.

The majority (58) of complaints indicated that the alleged leak of information was an isolated incident. Twenty of these were substantiated. Nine complaints included details that the alleged leak of information was not an isolated incident. Three of these were substantiated. The remaining 37 complaints (three substantiated) did not specify whether the alleged leak of information was an isolated incident.

Figure 3 shows the relationship between the police officer who allegedly leaked the information and the person to whom information was allegedly leaked by outcome of the PIC's assessment. As shown in this figure, 28 complaints were concerned with leaks of information to members of the public. Of these, ten were substantiated. Twelve of the 28 complaints concerning leaks of information to members of the public were allegedly done so to exchange information to other agencies or persons as part of the police officer's job. Three of these 12 complaints were substantiated. Eleven complaints of leaks of information to members of the public claimed that the information was leaked face-face. Five of these were substantiated. Case study 3 provides an example of a complaint that describes an alleged leak of information to members of the public.

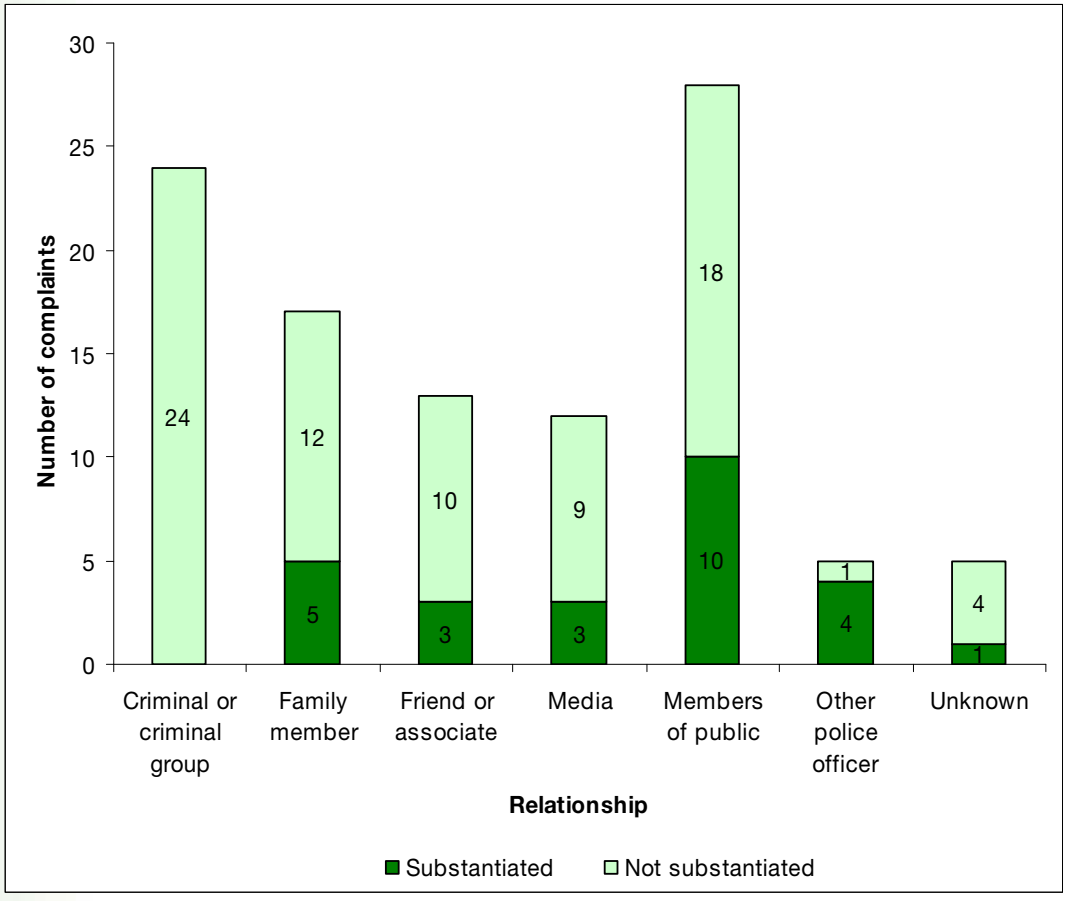


Figure 3. The relationship between the police officer who allegedly leaked the information and the person to whom information was allegedly leaked by outcome of the PIC's assessment.

Five complaints were concerned with information leaked to other police officers. Four of these leaks of information allegedly occurred because of curiosity or gossip and all four were substantiated. The purpose of the alleged leak of information which was not substantiated is not known.

Case study 3. Breach of complainant's privacy.

A member of the public called the police to report a case of child abuse against her neighbours. She later made a complaint to the police that her neighbours were aware she had reported them and they were harassing her. This had caused her much distress and embarrassment. The complainant believed a police officer had disclosed her report to the neighbours. The case was investigated and there was no evidence that any police officer had disclosed the identity of the complainant to her neighbours. The investigator concluded that the complainant and her neighbours had a difficult relationship and the neighbours assumed it was the complainant who had reported them. The complaint was not substantiated.

Other complaints were concerned with information leaked to family members (17), friends or associates (13) and the media (12). Small proportions of these complaints were substantiated. Examples of complaints concerned with alleged leaks of information to family members are provided in Case studies 4 and 5. An example of a complaint regarding an alleged leak of information to the media is provided in Case study 6.

Interestingly, 24 complainants alleged that information was leaked to known criminals or criminal groups, none of which were substantiated by the PIC. Case study 2 is an example of this. The complaints about information leaked to criminals were made by ten members of the public, nine police officers, four anonymous persons and one victim. Seven of these alleged leaks were discovered through police investigations of other matters (and hence reported by police officers) and the remainder were discovered when the complaint was made. Ten of the 24 complaints included the name of the police officer who was alleged to have leaked information. Also, 14 of the 24 complaints were regarding tip offs and one was regarding an accidental or unintentional disclosure of information. The purpose of the other nine leaks of information was not specified in the complaints.

To further understand some of the other details that may have been available for the investigation of the 24 complaints regarding leaks of information to known criminals, these 24 complaint files were searched for details regarding whether the criminals were named in the complaint, whether the complainant was interviewed as part of the investigation and whether call charge records were used as a part of the investigation. Call charge records can be used to determine if there was any

telephone contact between the police officer who was alleged to have leaked information and the person who allegedly received the information.

Case study 4. A member of the public reported that a police officer disclosed information to family members.

A member of the public called his local police station regarding information he had received about a paedophile living in the area. The information had originally come from the wife of a police officer, whom the complainant named. The police officer was interviewed and he stated that while his family was visiting him at work, a person suspected of committing offences against minors attended the police station. He told his wife about the suspected activities of this person as a protective measure for the safety of their children. He did not specifically tell his wife that the information was confidential. His wife divulged this information to other persons in the community. The officer was counselled. The PIC classified this complaint as substantiated.

Almost all (22) of the complaints included the name of the criminal who allegedly received confidential information from police officers. The complainant was interviewed in nine of the 24 investigations. Interviews were not conducted in four investigations because the complainant was anonymous. For five instances the complainant was not interviewed because further details were not required. Interviews were also not conducted for the remaining six investigations because the alleged leak of information was discovered through police investigations and reported by a police officer who did not have any further details. Very few investigations (3) used call charge records. They were not used in some investigations because call charge records would not have provided the necessary evidence to show a leak of information occurred (e.g. if a police officer was known to associate with a person who received the confidential information, then phone calls between them would not be unusual).

Case study 5. Personal details accidentally leaked to family members.

A police officer was entering details of an investigation into the NSW Police Force's computer system when she suspected that one of the persons involved in the investigation might be a family member. She rang her husband to confirm this and disclosed details of the case. The police officer claimed that during the telephone call she did not realise that what she was doing was wrong. Immediately after the telephone conversation, she realised she had disclosed confidential information and reported the matter to her supervisor. She also reported a conflict of interest. The officer was counselled. The PIC classified the complaint as substantiated.

Figure 4 shows the purpose of alleged leaks of information as described in complaints by the outcome of the PIC's assessment. Most complaints (23) did not include details regarding the purpose of alleged leaks of information. For 14 of these, this most likely occurred because the police officer who allegedly leaked the information was not named in the complaint.

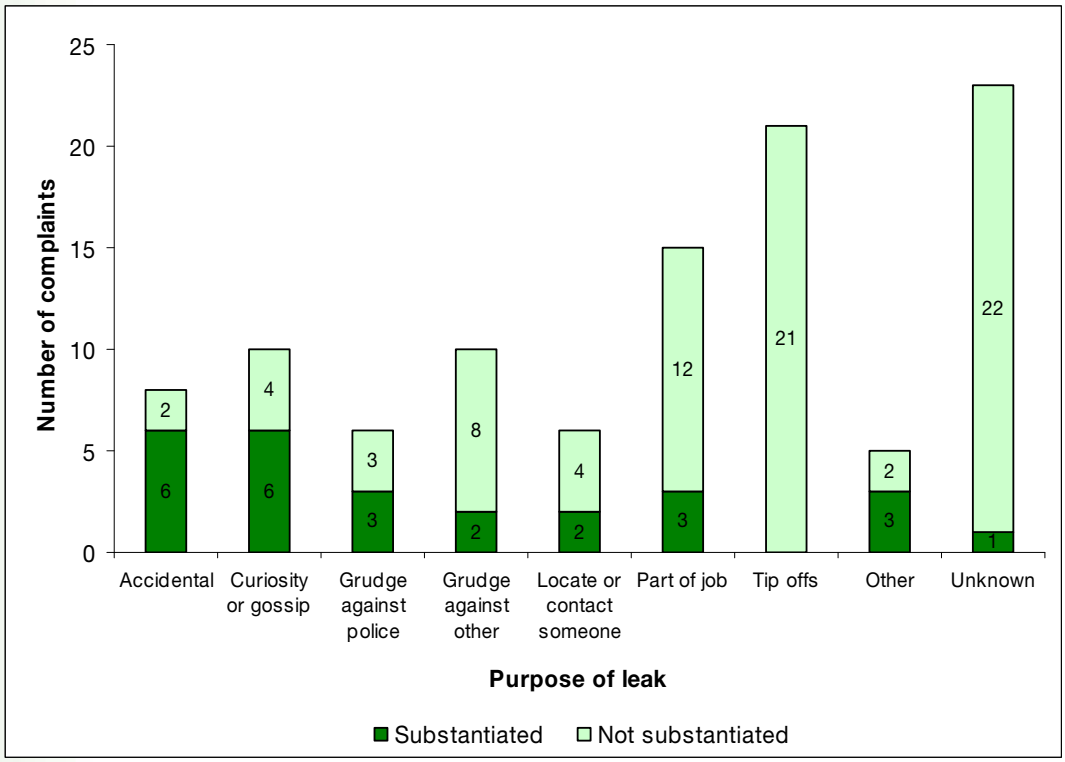


Figure 4. Purpose of the alleged leak by outcome of the PIC's assessment.

The next most common (21) purpose of leaks of information as indicated in the complaints was tip offs or the provision of information regarding police activity, none of which were substantiated. The majority (14) of these alleged leaks of information were to known criminals or criminal groups. For 12 of these, the police officer who allegedly leaked the information was named in the complaint. Four complaints regarding tip offs were discovered through investigations of other matters, the remainder through complaints. Case Study 2 describes an example of a complaint regarding a tip off.

The complaints analysed indicated that the purpose of alleged leaks of information also included disclosures of information as part of the police officer's job (15 complaints, 3 substantiated), grudges (16 complaints, 5 substantiated) and curiosity or gossip (10 complaints, 6 substantiated). Some leaks of information (8 complaints, 6 substantiated) had no purpose, they were accidental or not intentional. Other leaks of information (6 complaints, 2 substantiated) occurred in order to locate or contact someone. Case study 5 describes a complaint regarding an accidental leak of

information. The 'other' category included one leak of information for financial gain (not substantiated), one for political reasons (substantiated) and three to warn someone about becoming involved with criminals or criminal activity (2 substantiated, 1 not substantiated).

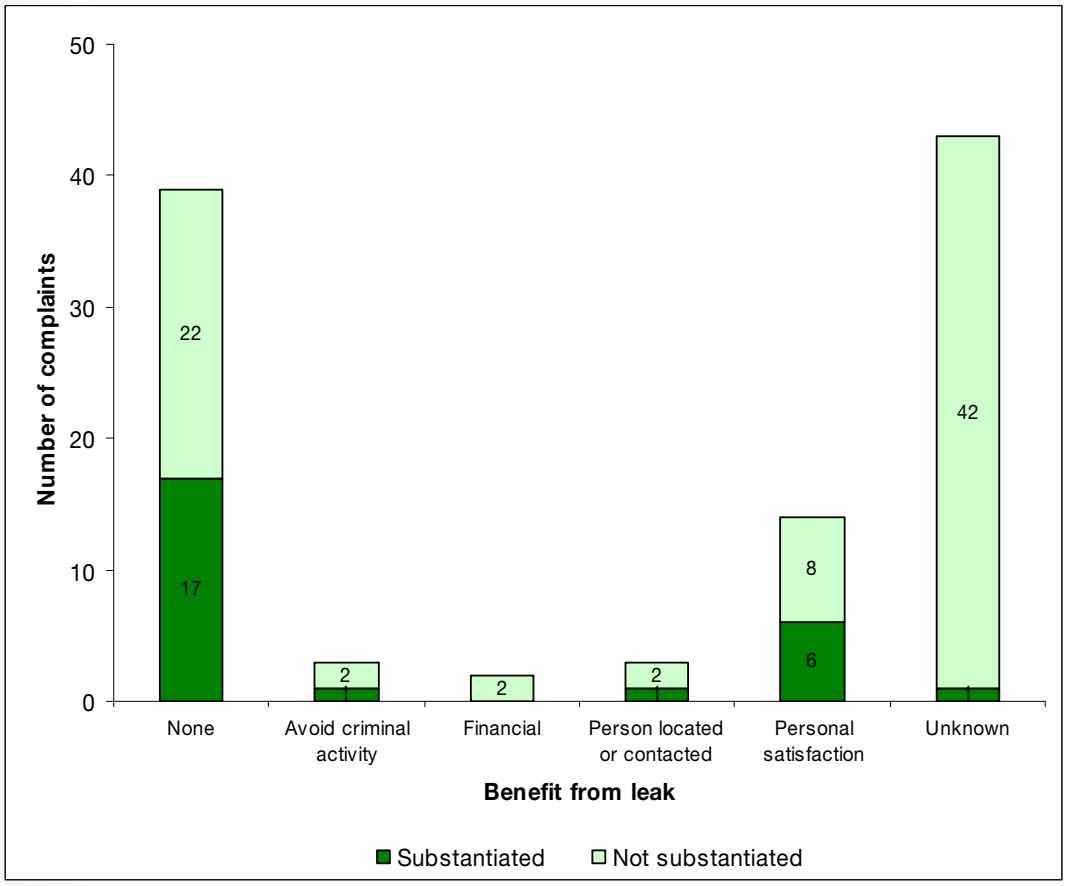


Figure 5. Benefit from the alleged leak of information by outcome of the PIC's assessment.

Data regarding the benefit from the alleged leak of information as described in the complaint by outcome of the PIC's assessment is shown in Figure 5. In the majority of instances (43), the benefit of the alleged leak of information was not indicated in the complaint. For 39 complaints, however, there was no obvious benefit from allegedly leaking information. Of these, 17 were substantiated. Fourteen complaints alleged that the benefit from leaking information was personal satisfaction, usually from a grudge held against the NSW Police Force or another person or institution. Approximately half of these (6) were substantiated. A small number of complaints alleged that a police officer benefited from leaking information by allowing others to avoid becoming involved in criminal activity (3), gaining financially (2) or locating or contacting the person they were seeking (3).

Case study 6. A complainant alleged that details regarding his pending charges were released to the media.

A person who had been granted bail for an offence for which he was due to appear in court complained that his name and the details of his charges were published in a major newspaper and broadcast on a public radio station. He believed that details of his offence were released to the media by police officers. The complaint was investigated but there was no evidence that any police officer had released confidential information about the complainant. The police officer investigating the case suggested that the complainant's details had been sourced from publicly available files. The complaint was not substantiated.

Figure 6 shows the source of the alleged leaked information as described in the complaints by outcome of the PIC's assessment. The source of the alleged leaked information was unknown in most instances (41). A large proportion of the complaints indicated that the alleged leaked information was sourced from COPS (30) or office knowledge (20). Eight alleged leaks of information sourced from COPS were substantiated, while 12 sourced from office knowledge were substantiated. Smaller numbers of complaints indicated that the alleged leaks of information originated from knowledge gathered from investigations (5 complaints, 3 substantiated), information in other files available to the NSW Police Force (5 complaints, 2 substantiated) or information gathered from a complaint about a police officer (3 complaints, none substantiated).

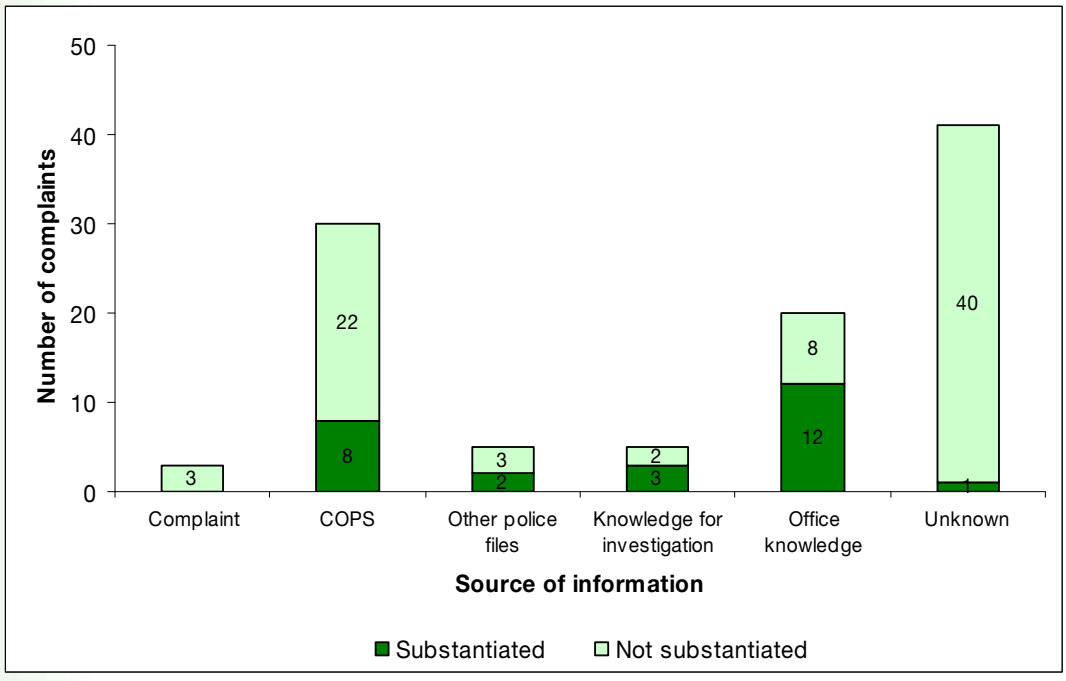


Figure 6. The source of alleged leaked information by outcome of the PIC's assessment.

Thirteen of the 104 complaints indicated that information was obtained specifically in order to disclose it to other persons. Three of these complaints (2 substantiated) indicated that the information was derived from office knowledge and nine of these complaints (4 substantiated) indicated it was derived from COPS. Although one other complaint (which was substantiated), indicated that information was obtained specifically, the source of the information was unknown. In 29 complaints, information was not obtained specifically, 14 of these were substantiated. For the remainder of alleged leaks of information (56), there was no indication whether information was obtained specifically. Six of these complaints were substantiated.

Figure 7 shows the methods used to allegedly leak information as indicated in the complaints by outcome of the PIC's assessment. The vast majority (65) of complaints did not provide details regarding the methods used to allegedly leak information. A very small proportion of these (5) were substantiated. Other noteworthy methods of leaking information as described in the complaints involved face-to-face conversations (21 complaints, 10 substantiated) or by telephone (9 complaints, 4 substantiated). Interestingly, when the method of leaking information was not mentioned in the complaint, the proportion of substantiated complaints (8%) was much lower than when the method was described (46%). Case study 4 describes a complaint where information was leaked face-to-face and Case study 5 describes a complaint where information was leaked by telephone.

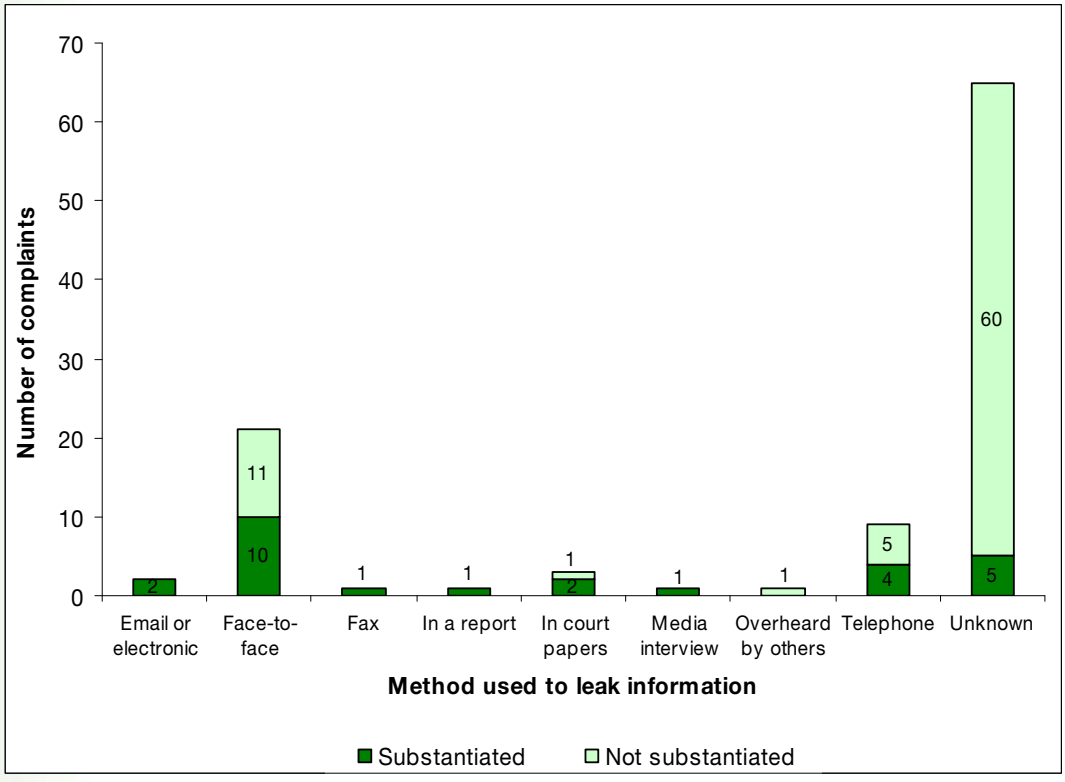


Figure 7. The method used to allegedly leak information by outcome of the PIC's assessment.

Thirty-four of the complaints analysed in this study indicated that several other types of misconduct occurred in conjunction with unauthorised disclosures of information. The most common types included improper associations (8), unauthorised access to COPS (6) and unprofessional conduct (6). Seventy-two of the 104 complaints did not mention any other types of misconduct.

3.3. Details derived from the investigation of the complaint

The following section describes patterns regarding the alleged consequence of the leak of information. When there was no obvious consequence from the alleged leak of information, it was recorded as 'none'. When there was a possibility of a negative consequence from the alleged leak of information, but there was no mention of any consequence, it was recorded as 'unknown'.

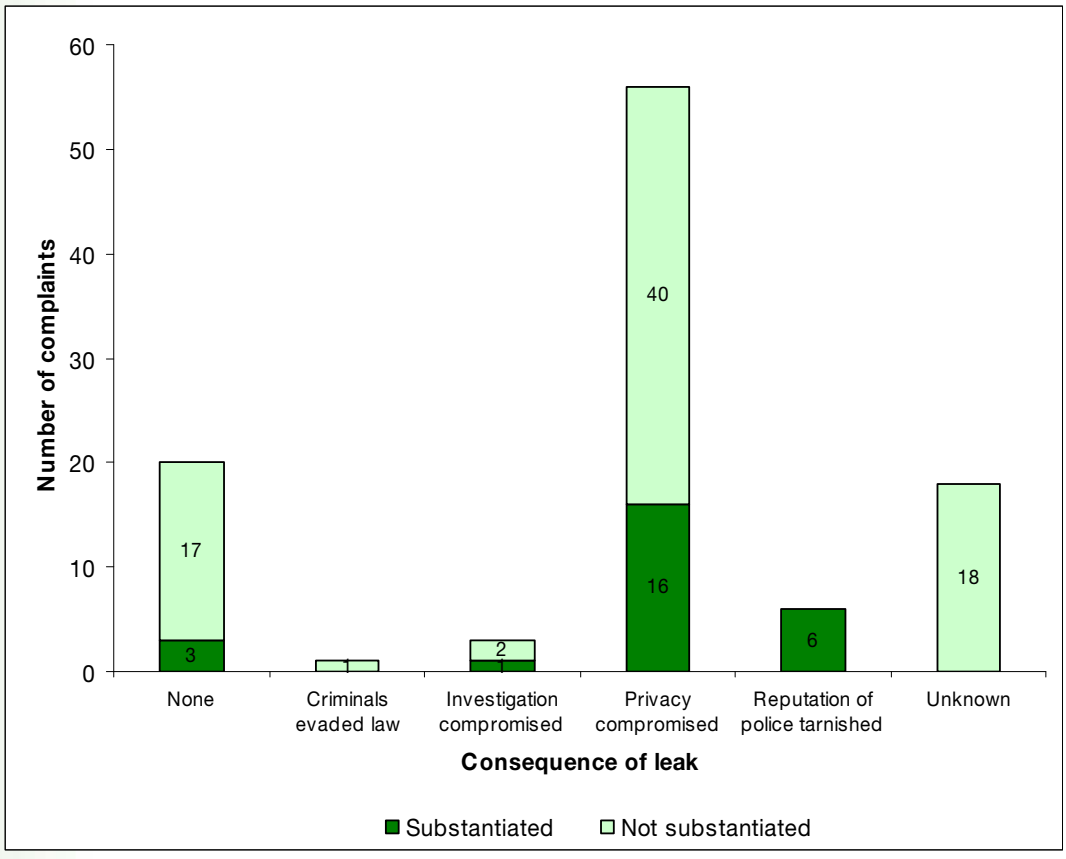


Figure 8. Consequence of the alleged leak of information by outcome of the PIC's assessment.

Figure 8 shows the consequence of the alleged leak of information as described in the complaint or the investigation by the outcome of the PIC's assessment. For 20 complaints, three of which were substantiated, no consequences of allegedly leaking information were identified or mentioned in the complaint or the investigator's report. That is, for 20 cases, there were no obvious negative effects from the alleged leak of

information. Six complaints, all of which were substantiated, resulted in the reputation of the NSW Police Force being tarnished. Only four complaints, of which one was substantiated, were concerned with consequences such as criminals evading the law or investigations being compromised.

For the majority of complaints (56), the consequence of the alleged leak of information was that an individual's privacy was compromised. Sixteen of these were substantiated. The seriousness of this type of disclosure of information can vary. In one instance where a victim's privacy was compromised, an assault occurred against the victim, who sustained serious injuries. Case study 3 provides an example of a complainant who claimed her privacy had been compromised.

Complaint files were further analysed to determine what management action was taken against police officers who compromised an individual's privacy. Only substantiated complaints were considered. For 12 of the 16 substantiated complaints where an individual's privacy was compromised, police officers were counselled, reminded of the correct procedures to follow when dealing with confidential information or directed to undertake training and development with regard to confidential information. In one case, no disciplinary action was taken because the complaint was not sustained by the NSW Police Force. The PIC, however, classified this complaint as substantiated because information was disclosed without the authority of the NSW Police Force. In another two cases, criminal charges were laid and in the remaining case, the police officer who leaked the information was nominated for a section 181D (*Police Act 1990*) removal, a process that indicates the Police Commissioner's loss of confidence in that police officer. This police officer was later dismissed.

The following paragraphs describe the involved police officer's attitude regarding the allegation of the leak of information and whether the officer was aware of the NSW Police Force's policy regarding confidential information. When more than one police officer was named in the allegation, the data recorded for these categories was based on the attitude and knowledge of the police officer who was alleged to have the greatest involvement in leaking the information.

Figure 9 shows the attitude of the police officer involved in the alleged leak of information for the complaints where a police officer was named in the allegation by outcome of the PIC's assessment. For 23 of the 66 complaints, there was no mention of the police officer's attitude in the investigator's report. Seventeen police officers denied leaking confidential information. Two of these were substantiated; the purpose of one of these was to warn someone about becoming involved with criminals and the other was for political reasons. The purpose of the remaining 15 complaints (not substantiated) where the police officer involved denied leaking information were grudges (3), tip offs (4), gossip (2), to locate someone (1), part of the police officer's job (1) or unknown (4).

Fourteen police officers claimed they disclosed information because it was a necessary part of their jobs. Four of the complaints made against them were classified as substantiated, or in other words, information leaks occurred for four of the incidents where police officers claimed they divulged information to other persons because it was necessary to exchange information as part of their duties. The purpose for two of these was to exchange information as part of the police officer's job. In these cases, incorrect procedures were used by the police officers when divulging confidential information. For another of the substantiated complaints where the police officer involved claimed it was necessary to disclose information as part of his duties, the purpose of the leak of information was to locate or contact someone. For the remaining substantiated complaint, the purpose was a grudge; the officer claimed he needed to divulge information as part of his job, but the complaint indicates that he disclosed information because of a grudge. Ten complaints where police officers claimed they disclosed information as part of their jobs were classified by the PIC as not substantiated. For eight of these, it was necessary to release information as part of their jobs. The purpose for one was a tip off and for the other it was to warn someone against becoming involved with criminals.

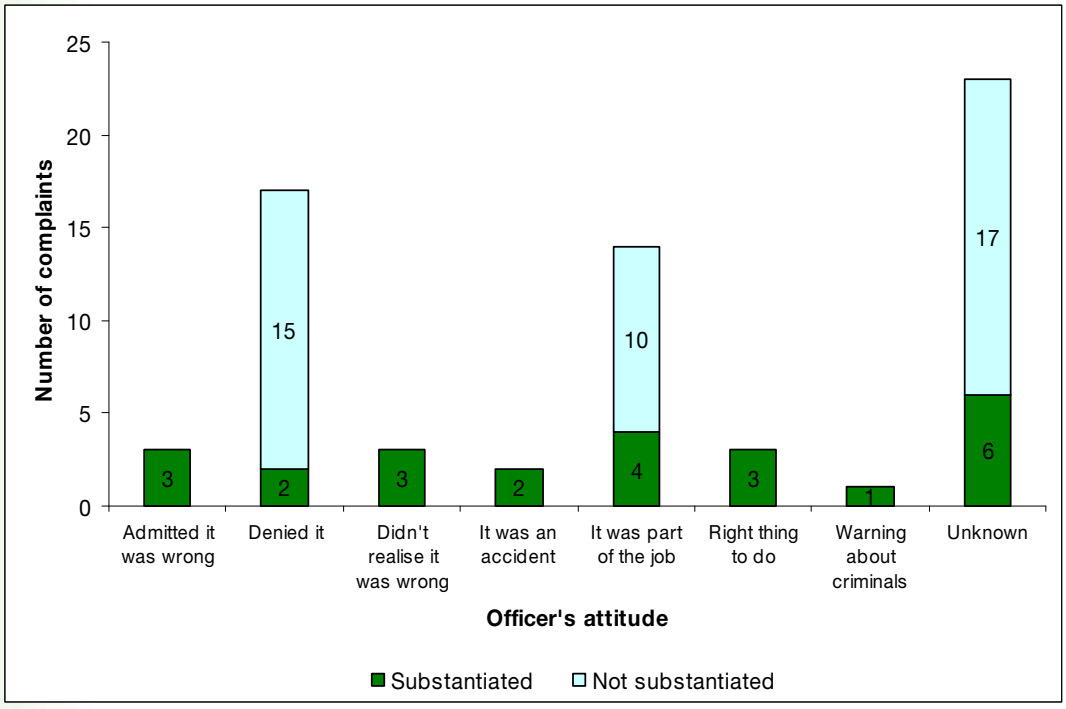


Figure 9. The attitude of the police officer involved in the alleged leak of information for all complaints in which a police officer was named in the allegation by outcome of the PIC's assessment, n=66.

Smaller numbers of police officers admitted that leaking the information was the wrong thing to do (3), claimed that they did not realise that they were doing the wrong thing (3), claimed the leak of information was accidental (2), thought it was the right thing to do (3) or believed they needed to warn someone about criminals or

criminal activity (1). All of these were substantiated. An example of a complaint regarding a leak of information where the police officer claimed they did not realise it was wrong to release information is provided in Case study 5.

In the 66 complaints that included the name of a police officer, only five investigator's reports included details regarding the police officer being aware of policies or training within the NSW Police Force which relate to the disclosure of confidential information; three of the five police officers indicated they were not aware of the training or the policies, while the other two police officers were aware of them.

3.4. Summary of Results

The data provided in this study was sourced from complaints regarding leaks of confidential information by NSW police officers. As explained previously, complaints data can be problematical for measuring the prevalence of misconduct. In this study, however, complaints data was used to identify patterns in the characteristics of unauthorised disclosures of confidential information.

Patterns were identified from complaints that were classified as substantiated as well as those that were classified as not substantiated. Patterns detected from complaints that are classified as substantiated can provide valuable details regarding leaks of information which are useful in the management and prevention of this type of misconduct. Of the 104 complaints of leaks of information that were analysed in this study, 26 were classified as substantiated.

Patterns detected from complaints that are not substantiated can also be useful in the management and prevention of leaks of information. They can be used to identify problem areas where evidence of a leak of information is difficult to obtain. They can also provide valuable details regarding misunderstandings, accidents and problems with procedures used as part of police officer's jobs, which can be used to help reduce the numbers of complaints made about police officers.

In this study, 78 complaints were classified as not substantiated. They included 35 complaints where there was not sufficient evidence that a leak of information occurred and 12 complaints regarding information being exchanged as part of the police officer's job. The remaining 31 complaints that were not substantiated therefore describe alleged leaks of information that most likely occurred due to misunderstandings between the police officer involved and the complainant or misunderstandings by the complainant about events that occurred which led them to believe information was leaked. The complaints may also have been false or frivolous. The number of false complaints should, however, be minimal because generally, people who make a complaint genuinely feel that they have something to complain about (Maguire and Corbett 1991). The number of complaints that are obviously frivolous or not made in good faith are also likely to be minimal because these

complaints can be declined for investigation by the NSW Police Force (*Police Act 1990*) and would not have been included in this study. The majority of those 31 complaints described above are therefore likely to have occurred because of misunderstandings between the police officer involved and the complainant, or misunderstandings by the complainant about events that occurred which led them to believe information was leaked.

The most significant findings of this study are outlined below. Their implications for the management and prevention of leaks of information are discussed in the following section.

- About 20 per cent of complaints of leaks of information were reported by police officers who discovered the alleged leak of information through a variety of methods, including during the investigation of another matter. The remaining alleged leaks of information were discovered when a complaint was made.

- Almost half (44%) of the complainants were victims of alleged leaks of information. This was not surprising because complaints about police officers are most likely to be received when there is a victim involved in an event involving misconduct (Criminal Justice Commission 2000). A number of the other patterns identified in this study reflect this, with some of the strongest patterns relating to victims and personal breaches of privacy.

- Complaints made by police officers were much more likely to be substantiated than complaints made by other persons. It is possible that police officer complainants provide a greater number of details regarding a leak of information than other types of complainants. The data in this study, however, did not support this possibility.

- The majority (79%) of complaints regarding leaks of information mentioned that only one police officer was involved.

- Most complaints (63%) included the name of the police officer who allegedly leaked the information. About one third (36%) of complaints that included the name of a police officer were substantiated.

- Most complaints (56%) described the alleged leak of information as an isolated event.

- Twenty-eight complaints (27%) alleged that information was leaked to members of the public. Twelve of these (43%) allegedly occurred because it was necessary to exchange information as part of the police officer's duties. Only three of these 12 were substantiated.

- Few (12%) allegations regarding leaks of information indicated that confidential information was released to the media. Three of these complaints (25%) were substantiated.

- Approximately one-quarter (23%) of the complaints made alleged that information was leaked to criminals or criminal groups. None of these were substantiated. Almost all of these complaints included the name of the criminal to whom information was leaked. Where possible and worthwhile, complainants were interviewed in order to provide further details to assist the investigation. Call charge records were rarely used in these investigations, although they were not always necessary.

- Tip offs accounted for 20% of the purpose of alleged leaks of information, none of which were substantiated.

- When complaints were categorised by purpose of the alleged leak of information, the greatest proportions of substantiated complaints were from the categories named 'accidental' (75% of complaints about accidental leaks of information were substantiated) or leaked to others for curiosity or during gossip (60% of these complaints were substantiated).

- The benefit for 41 per cent of alleged leaks of information was not known. A further 38 per cent had no obvious benefit associated with the alleged leak of information and approximately half of these were substantiated. Therefore, only 21 per cent of alleged leaks of information had an obvious benefit for the police officer involved, the majority of which were for personal satisfaction.

- About half (48%) of the complaints indicated that the alleged leaked information was sourced from COPS or office knowledge. Details of the source of the alleged leaked information were not provided for 39 per cent of complaints. When the source of the alleged leaked information was known, the complaint was more likely to be substantiated.

- Approximately half (54%) of all complaints did not indicate whether information was obtained specifically to be leaked. Thirteen per cent of complaints indicated that information was obtained specifically and approximately half of these were substantiated.

- The majority of complaints (63%) regarding leaks of information did not specify the method by which information was allegedly leaked. When the method of leaking information was mentioned in the complaint, information was more commonly leaked face-to-face (11%) or by telephone (9%).

- About two thirds (69%) of complaints did not mention other types of misconduct which occurred in conjunction with the alleged leak of information. The most common other types of misconduct were improper associations, unauthorised access to COPS and unprofessional conduct.

- The most common (54%) consequence of alleged leaks of information was that an individual's privacy was compromised. Approximately 30 per cent of these instances were substantiated and the involved police officer was commonly counselled in relation to this. The consequences of 17 per cent of alleged leaks of information were not known. The consequences of very few complaints involved criminals evading the law (1%) or investigations being compromised (3%). Nineteen per cent of complaints had no obvious consequences from allegedly leaking information, few of these were substantiated.

- When police officers who allegedly leaked information were interviewed, they most commonly denied leaking information (16%) or they claimed that exchanging the information was a necessary part of their jobs (13%). In 22 per cent of cases, the investigation report does not mention the attitude of the police officer involved in the alleged leak of information.

- A very small proportion of investigators reports (8%) included details concerning the involved police officer being aware of the NSW Police Force's policy regarding confidential information.

4. Implications for Management and Prevention of Leaks of Information

A number of different strategies are commonly used to manage and prevent misconduct in policing agencies. These strategies include (but are not limited to) training in ethics and ethical decision making, the use of deterrence strategies such as penalties and the existence of policies and other corporate documents such as a Code of Conduct (Poerting and Vahlenkamp 1998; Punch 2000; Pogarsky and Piquero 2004; Moran 2005).

The NSW Police Force uses the strategies mentioned above to provide messages and rules to police officers regarding confidential information. This study has identified patterns in the characteristics of leaks of information which highlight some issues of concern in the training, deterrence strategies, policies and procedures in use by the NSW Police Force to manage and prevent this type of misconduct. These issues and suggestions for their improvement are discussed below. This is then followed by a response from the NSW Police Force.

4.1 Training and Policy

In NSW, police officers are provided with training at various stages in their careers. Initial training is provided at the NSW Police College and further training is provided on the job, on the NSW Police Force's intranet as well as formal ongoing training. During their training, police officers are informed about confidential information and that it is a requirement they do not disclose information without proper authorisation. The need for confidentiality is also stressed in a number of different NSW Police Force policies, codes and guidelines (e.g. the Code of Conduct and Ethics, the Media Policy and the Code of Best Practice for Information Management). The policies, codes and guidelines are available to police officers online via the NSW Police Force's intranet, the main source for police officers to find information and guidance on policies, procedures and issues that affect them.

Despite the training received by police officers and the availability of policies and other documents on the NSW Police Force's intranet, it was surprising that several results of this study indicated that there is confusion, misunderstanding and/or a lack of awareness among some NSW police officers regarding confidential information and the methods that should be used to deal with and disseminate it. For example, when complaints were categorised according to their purpose, approximately one third (33 of the 104) of all alleged leaks of information probably occurred due to confusion, misunderstandings or lack of awareness regarding policies and procedures; eight were accidental, 15 occurred as part of the police officer's job and ten occurred due to curiosity or gossip. Fifteen of these complaints were substantiated, which represents 58 per cent of all substantiated complaints.

Also, when the investigators reports were analysed and the attitude of police officers who allegedly leaked information was categorised, one third (22 of the 66) of their attitudes indicated that there are problems with confusion, misunderstandings and/or lack of awareness regarding policies and procedures; three claimed they did not realise what they did was wrong, two claimed it was an accident, 14 claimed it was necessary to divulge information as part of their jobs and 3 claimed they believed they did the right thing. Twelve of these complaints were substantiated, which represents 55 per cent of the substantiated complaints where a police officer was identified. An additional third (23 out of 66) of the investigator's reports did not include any information regarding the attitudes of the police officers named in allegations of leaks of information. Further, investigator's reports rarely indicated whether the police officer alleged to have leaked information was aware of the training or policies of the NSW Police Force that relate to confidential information and, most surprisingly, of the five investigator's reports that did indicate this information, three police officers stated they were not aware of the training or the policies.

Another example of misunderstanding and confusion regarding policies and procedures stems from the complaints that were not substantiated. Up to 31 of these complaints (40% of complaints that were not substantiated) most likely occurred because of misunderstandings between the police officer involved and the complainant, or misunderstandings by the complainant regarding events that occurred which led them to believe information had been leaked.

The examples provided above show that a number of complaints about leaks of information resulted from misunderstandings, confusion or lack of awareness regarding policies and procedures used by the NSW Police Force. Minimising misunderstandings and confusion, and increasing awareness of policies and procedures can prevent some leaks of information from occurring, and can also help to reduce the number of complaints made regarding this type of misconduct. One method of addressing this issue is to ensure that policies, procedures and guidelines for dealing with and managing confidential information are clear and easily accessible via a number of avenues, including the NSW Police Force's intranet.

As mentioned earlier, a number of NSW Police Force documents describe the policies, procedures and guidelines that are concerned with confidential information. There is, however, no single NSW Police Force document dedicated only to the management of confidential information. Searching for guidance when dealing with confidential information can, therefore, be difficult because information relevant to confidential information is spread throughout the many different documents. Searching for guidance could be simplified by combining all sections of codes, guidelines and policies relating to confidential information in a single document to create a one-step resource for dealing with confidential information. Such a document could provide an overview of methods to deal with and manage confidential information and refer to sections of codes, guidelines and policies as necessary. This could also be achieved on the intranet by comprehensive linkage of all web pages that refer to documents concerned with confidential information. Such amalgamation and linkage would greatly assist in minimising confusion and misunderstanding.

Confusion and misunderstanding could also be minimised by clearly stating the functions, purposes and objectives of each document. Providing these details can help police officers who are searching for guidance on a particular issue to determine which document is most relevant to their needs. In order to minimise confusion and misunderstandings between complainants and police officers when information is provided to other agencies as a part of the police officer's job, it may also be helpful to emphasise to police officers that, whenever possible, it is important to inform members of the public when their personal details are given to other agencies.

To further minimise misunderstandings and confusion, leaks of information must be clearly defined. It is important to ensure that police officers understand what constitutes a leak of confidential information and that all leaks of confidential information are considered a breach of the NSW Police Force's Policies and Code of Conduct and Ethics. Stereotypically, leaks of information are thought of as instances where information is provided to criminals or the media for some kind of benefit, such as favours or money. Leaks of information are also stereotypically thought to have grave consequences such as compromising investigations, allowing criminals to evade detection or serious physical harm to persons.

This study showed that about 25 per cent of all complaints were concerned with leaks of information to criminals and about 10 per cent were concerned with leaks of information to the media. Therefore, 65 per cent of all complaints concerning leaks of information were not of the stereotypical kind. In fact, a quarter of all complaints in this study were concerned with leaks of information to members of the public. The most common consequence from data collected in this study was that an individual's privacy was compromised.[1] Twenty per cent of alleged leaks of information had no obvious consequences and 38 per cent had no obvious benefit to the police officer who allegedly leaked the information. Very few allegations of leaks of information had benefits such as gaining financially or getting satisfaction from a grudge. Some leaks of information were accidental. There is, therefore, a need to clearly define confidential information and a need to emphasise that providing any confidential information to persons who do not have the authority to know such information is considered a leak of information, despite whom the information is given to and whether or not there are benefits or consequences.

4.2. Investigations

The investigators reports included in this study contained little information regarding the attitudes of the police officers named in allegations of leaks of information or whether they were aware of the policies and procedures of the NSW Police Force that relate to confidential information. In some cases, the officer alleged to have leaked information was not interviewed as part of the investigation. Interviewing the officer involved and finding out his or her attitude and knowledge of the NSW Police Force's policies and guidelines can help to determine the general level of understanding of these documents among police officers, and more specifically, whether the police officer being investigated requires further training.

[1] This result might reflect the fact that the data came from complaints. For situations where financial benefits are involved, it is unlikely that there are victims to make the complaint.

4.3. Deterrence strategies

Although some leaks of information were accidental or occurred due to misunderstandings between police officers and complainants, there were instances where information was deliberately leaked. For example, 13 per cent of complaints included details to suggest that information was obtained specifically (about half of these were substantiated), indicating that there was a deliberate intention to search for and release confidential information. In other words, 28 per cent of all substantiated complaints were cases where information was deliberately leaked. About half of the complaints analysed in this study alleged the information was sourced from COPS or office knowledge. Some of these cases involved police officers calling a police station and asking another police officer to make checks for them on COPS.

It is difficult to stop police officers from planning and deliberately leaking information, but some police officers may be deterred from leaking information if the consequences of doing so are clear and well-understood (Pogarsky and Piquero 2004). It is important that police officers are aware that if they leak information, management action will be taken. Police officers also need to be aware that they can be prosecuted and, in certain cases, dismissed from the NSW Police Force. This is also relevant for leaks of information to the media. In this study, 12 per cent of allegations regarding leaks of information indicated that confidential information was released to the media and 25 per cent of these were substantiated. Although the numbers for these types of leaks of information were small, such leaks of information are very serious and can have a much larger impact than those to other persons because information leaked to the media can be dispersed to a large proportion of the population. The NSW Police Force's Media Policy mentions that 'breaches may result in disciplinary action and/or criminal or civil sanctions'. Similarly, the final sentence of item 8 of the NSW Police Force's Code of Conduct and Ethics indicates that 'failure to comply with the Code of Conduct and Ethics may result in management action'. Elaborating on the penalties that apply if information is leaked may help deter police officers from engaging in this form of misconduct. Tightening the language used in policies from 'may result in management action' to 'will result in management action' may also help achieve this.

4.4. Recording information for intelligence

About 34 per cent of complaints regarding leaks of information were not substantiated because of lack of sufficient evidence. Some investigations of complaints regarding leaks of information are difficult and challenging and it may not be possible to provide evidence that a leak of information occurred. For example, as shown in this study, the majority (79%) of complaints regarding leaks of information mentioned that only one police officer was involved and most complaints (63%) included the name of the police officer who allegedly leaked the information.

Twenty-five per cent of all complaints analysed in this study were substantiated. This percentage is much smaller than the percentage of complaints for which names of police officers were provided (63%). Hence, finding sufficient evidence to sustain complaints is obviously difficult, even when the name of a police officer is provided in the allegation. Also, a relatively large number of complaints made alleged that information was leaked to criminals or criminal groups or was given to another party as a tip off. None of these complaints were substantiated, despite their investigations. In many instances, the complaints were not substantiated because of a lack of evidence. For example, 16 of the 24 alleged leaks of information to criminals were not substantiated because of a lack of evidence.

Storing such information in a database for potential use for intelligence purposes could help to prevent similar leaks of information or other problems with the police officers allegedly involved in the leak of information. Storing information regarding other types of misconduct that were reported within the same complaint as a leak of confidential information could also be useful for intelligence purposes.

4.5. Substantiation rates

The proportion of complaints substantiated varied greatly depending on the type of complainant. When complaints were made by police officers, they were much more likely to be substantiated than complaints made by other persons. The reasons for this are unknown. One explanation is that police officer complainants provided a greater number of details regarding a leak of information than other types of complainants. The data in this study, however, did not support this possibility. There are many other possibilities to explain the reasons that complaints made by police officers are most likely to be substantiated than complaints made by other persons. For example, complaints made by police officers may provide better quality of information, may be given more credibility or they may be investigated more carefully to avoid dissatisfaction among members of the NSW Police Force. It is also possible that complaints made by police officers are more likely to be substantiated than those made by other persons because police officers understand which types of disclosures of information are appropriate and which types are inappropriate, hence they are more likely to know what constitutes an unauthorised disclosure of information. The data collected in this study could not be used to analyse these other possibilities and further research would be required to address them.

5. Conclusions

The purpose of this study was to use data sourced from complaints to describe patterns in the characteristics of alleged instances of unauthorised disclosures of confidential information by NSW police officers. Patterns were identified which have important implications for the management and prevention of leaks of information. A number of the results from this study indicate that there is confusion, misunderstanding and lack of awareness regarding confidential information and its use and management among some police officers of the NSW Police Force. The results also revealed that some police officers deliberately seek information to release it. Other results highlighted the difficulties involved in finding evidence to determine whether or not a leak of information occurred, particularly with regard to allegations of leaks of information to known criminals or to allegations of tip offs from police officers. The above issues can generally be addressed by modifications to the training, deterrence strategies, policies and procedures currently used by the NSW Police Force.

6. Response from the NSW Police Force

As indicated in its public report on Operation Abelia (PIC 2005, pp. 337-344), the PIC considers that clear messages and rules must be effectively communicated to NSW police officers as to acceptable and unacceptable behaviour as part of the NSW Police Force's efforts to prevent misconduct.

The above study regarding the unauthorised disclosure of confidential information revealed that there are several issues with the clarity and communication of NSW Police Force documents, particularly in regards to the ways in which they are presented on the NSW Police Force's intranet, which is the primary repository for policies and procedures.

Following the completion of this study, the PIC conducted a thorough search of the NSW Police Force's intranet to examine in detail the ways in which policies, guidelines and other documents concerned with confidential information are presented and communicated by the NSW Police Force.

Several specific issues were identified which could cause confusion or misunderstandings of policies and procedures. Also, while there were no direct problems viewing documents regarding the use and management of confidential information on the intranet, difficulties arose in finding and accessing the most relevant documents. Many of the issues found relate directly to those described in the research study, however, a number of additional issues were also identified. These are described below.

Item 8 of the Code of Conduct and Ethics indicates that officers are required to comply with the NSW Police Force's policies governing the use and disclosure of confidential information. The clear implication is that there is a defined and established suite of policies with which police officers must comply. The PIC's search of the NSW Police Force's intranet, however, found that the policies concerning the management and communication of confidential information with which officers are expected to comply were not clearly identified on the intranet.

A number of documents available on the NSW Police Force's intranet have similar titles or are concerned with similar topics. The PIC's search of the NSW Police Force's intranet found that the distinction between some of these policy documents which relate to the use and disclosure of confidential information was not apparent.

The PIC's search of the intranet found that the term 'confidential information' which is used in the Code of Conduct and Ethics, among other documents, is not defined either within the Code or elsewhere on the intranet. The PIC's search also found that other terms, such as 'sensitive information', are used in some policy documents and it was unclear whether these terms have the same meaning as confidential information.

The PIC's search of the NSW Police Force's intranet found that in key places on the intranet, some policy documents were not referred to by their correct titles.

Publication dates were frequently printed within policy and training documents on the intranet. The PIC's search found that often there was no indication as to whether or not these documents still represent the position of the NSW Police Force on the issues to which they relate.

The NSW Police Force was approached by the PIC regarding the findings of the research study and of the examination of the intranet. The NSW Ombudsman's Office was also consulted in view of its role in oversighting complaints about NSW police officers. In July 2008, discussions were held among the three agencies regarding these findings, their implications for prevention and management of confidential information, and the actions that could be taken to strengthen the capacity of the NSW Police Force to manage and communicate confidential information.

Following this consultation process, the NSW Police Force indicated that it will make amendments to its policies and procedures and the way in which they are arranged and presented on the NSW Police Force intranet so that:

- Policies concerning the management and communication of confidential information with which officers are expected to comply are clearly identified on the NSW Police Force intranet;

- All policies regarding confidential information are easily accessible on the intranet;
- Through the intranet and training, all NSW Police Force staff have access to, awareness of and an understanding of the policies regarding confidential information;
- There is a clear distinction between similar policy documents available on the intranet which relate to the management and communication of confidential information;
- The term confidential information is clearly defined within the Code of Conduct and Ethics and other key policies relating to this issue;
- The use of terminology relating to the management and communication of confidential information is standardised;
- Policy documents concerning confidential information are referred to by their correct titles on the intranet; and
- Only updated versions of policy and training documents pertaining to the use and communication of confidential information are available on the intranet and the date of all documents is clearly displayed.

At present, Item 8 of the Code of Conduct and Ethics along with other policy documents indicate that non-compliance may result in management action. No other information is provided regarding the penalties that apply for non-compliance and the word 'may' does not necessarily act as a deterrent. The NSW Police Force also indicated that it would consider making changes to ensure that the language used to describe the consequences of failing to comply with Item 8 of the Code of Conduct and Ethics is clear and acts as a deterrent.

It is acknowledged that the NSW Police Force is currently examining some internal policy development options in relation to clause 46 of the *Police Regulation 2000*, which relates to the communication of confidential information. The intended outcome of this process, which was initiated independently of the Commission's research, will be some internal communication to staff clarifying roles and responsibilities in terms of the communication of confidential information.

References

Alpert, G. P. and Smith, M.R., 1999. Police use-of –force data: Where we are and where we should be going. Police Quarterly. 2(1): 57-78.

Criminal Justice Commission, 1997. Reducing police-civilian conflict: An analysis of assault complaints against Queensland Police, Brisbane.

Criminal Justice Commission, 2000. Protecting confidential information, Brisbane.

Ede, A., Homel, R. and Prenzler, T., 2002. Reducing complaints against police and preventing misconduct: A diagnostic study using hot spot analysis. Australian and New Zealand Journal of Criminology. 35(1): 27-42.

Goldsmith, A.J., 1991. External review and self-regulation: Police accountability and the dialectic of complaints procedures. *In*: Complaints against the police: The trend to external review. Ed. A. Goldsmith. Oxford University Press, Melbourne.

Goldsmith, A.J., 1996. What's wrong with complaints investigations? Dealing with difference differently in complaints against police. Criminal Justice Ethics. 15(1): 36-55.

Independent Commission Against Corruption, 1994. Report on investigation into matters relating to police and confidential information, Sydney.

Maguire, M. and Corbett, C., 1991. A study of the police complaints system, Stationery Office, London.

Moran, J., 2005. 'Blue walls,' 'grey areas' and 'cleanups': Issues in the control of police corruption in England and Wales. Crime, Law and Social Change. 43: 57–79.

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

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

Poerting, P. and Vahlenkamp, W., 1998. Internal strategies against corruption: Guidelines for preventing and combating corruption in police authorities. Crime, Law and Social Change, 29: 225–249.

Pogarsky, G. and Piquero, A. R., 2004. Studying the reach of deterrence: Can deterrence theory help explain police misconduct? Journal of Criminal Justice, 32: 371– 386.

Police Integrity Commission, 2005. Operation Abelia, Research and Investigations into Illegal Drug Use by some NSW Police Officers, Volume 3, Sydney.

Police Integrity Commission, 2005. Operation Cobalt, Sydney.

Prenzler, T., 2004. Stakeholder perspectives on police complaints and discipline: Towards a civilian control model. Australian and New Zealand Journal of Criminology. 37(1): 85-113.

Punch, M., 2000 Police corruption and its prevention. European Journal on Criminal Policy and Research, 8: 301-324.

NSW Police Integrity Commission

Address: Level 3, 111 Elizabeth Street, Sydney NSW 2000
Postal Address: GPO Box 3880, Sydney NSW 2001
Telephone: (612) 9321 6700 - **Freecall:** 1800 657 079
Fax: (612) 9321 6799 - **Website:** www.pic.nsw.gov.au

ISBN 1 74003 150 4

© Police integrity Commission 2008