Davids C and Boyce G (2016) "Integrity, accountability, and public trust: Issues raised by the unauthorised use of confidential police information", in Lister S and Rowe M (eds) Accountability of Policing, Routledge Frontiers of Criminal Justice, Abingdon and New York: Routledge, pp. 86–110. (ISBN 978-0-415-71533-1)

In announcing the establishment of *An Inquiry into the Culture, Practices and Ethics of the Press* in July 2011 the UK Prime Minister David Cameron stated:

> … the whole country has been shocked by the revelations of the phone hacking scandal … an episode that is, frankly, disgraceful: accusations of widespread law breaking by parts of our press: alleged corruption by some police officers; and … the failure of our political system over many, many years to tackle a problem that has been getting worse… let me turn to the issue of ethics in the police, and in particular their relationship with the press. Of course it is important that there is a good relationship between the media and the police. Police often use newspapers and other media to hunt down wanted criminals and to appeal for information. However, allegations have been made that some corrupt police officers may have taken payments from newspapers. And there are wider concerns that the relationship between the police and the press can also be too close. (HC Hansard, 13 July 2011, vol 531, cols 311,313)

In conducting the Inquiry, Lord Justice Leveson was, in part, tasked with the responsibility of exploring the relationship between the media and police, reflecting widespread concerns in the UK that this relationship was "inappropriately close and if not actually corrupt, very close to it" (Jay, quoted in Leveson 2012b: 743). Particular attention was drawn to this issue when it became known that police had failed to investigate properly allegations of illegal and improper phone hacking in 2006, 2009 and 2010. There were associated concerns about the unauthorised transmission of confidential information by police in the context of what Leveson found to be an "arguably over-cosy relationship between the police and the press" (Leveson 2012b: 744). The Inquiry "examined many facets of the way in which press and police interact … looking at the overlapping issues of 'tip offs', 'taking media on operations', 'off-the-record' briefings, leaks, whistleblowing, gifts and hospitality, entertainment etc" (Leveson 2012b: 980). Leveson found that "the best present analysis would suggest that although corruption is not widespread in the Police Service, where it does exist it has a corrosive effect on public confidence in the service as a whole" (p.943).

Concerns about misuse of police information are both long-standing and well-founded. In one sense, the matters before the Leveson Inquiry highlighted the increased potential for inappropriate access to and use of information in an environment where significant amounts of information are stored in digital forms. On the other hand, the increased use of information and communication technologies (ICTs) within policing provides the potential for greater information security and tracking of use. In these circumstances, a sound understanding of the nature and dimensions of the problem of unauthorised use of police information is important to developing suitable systems for the collection, storage and use of information, detection of breaches, and developing systems of accountability to deal with misuse.

Drawing on the academic literature and a number of data sources (complaints against police, prosecutions, and a range of public reports including the Leveson Inquiry itself), this chapter examines what happens when police information gets into the wrong hands. Distinguishing inappropriate *private/personal* use of information from inappropriate *disclosure*, we consider

types, sources, and uses of information. Through an accountability lens, we seek to expound harms that can arise for individual officers, the community, and the system of public administration. Our analysis suggests that viewing the problem of misuse of police information as part of the broader problem of conflict of interest facilitates a clearer perspective on the relationship between these concerns and issues of public trust, police integrity, and accountability.

Following an outline of the nature of the problem and its relationship to the broader context of police accountability, we draw on empirical data and official reports from Australia and the UK in order to elaborate key dimensions of the problem providing an outline of a variety of types and sources of information. We subsequently analyse the range of circumstances involved in the unofficial uses to which that information can be put – in the context of both private or so-called "domestic" use of information and disclosure (or leaks) to outside parties. The range of scenarios canvassed is elucidated with original case data and a range of reports from Australia and the UK. We consider how this problem may be addressed as a part of the broader problem of conflict of interest and argue for a social accountability lens that attends to both accountability mechanisms and the need to develop accountability as virtue.

Method and data sources

The analysis in the chapter draws on real case examples drawn from several key sources. First an original in-depth study that examined 377 internal investigations case files dealing with conflict of interest over a ten year period in the Australian state of Victoria (Davids 2005; Davids 2008; Cases from this data set are referred to throughout the chapter by their case number in the original study). The data set included all complaints against police for the ten-year period where conflict of interest was the primary element of complaint, as identified by the Victorian Ombudsman's office, which had oversight responsibility for complaints against police. The files were initiated by complaints from diverse sources including aggrieved members of the public, solicitors acting on behalf of members of the public, public sector agencies, private businesses, and by Victoria Police members who lodged against other police officers (Davids 2005: 12–16). Of the total sample examined, 58 matters (15 per cent) involved misuse of confidential police information.[1] We also utilise Victorian court cases involving prosecutions for matters related to misuse of police information.

The second key source is reports from public sector oversight and similar agencies in Australia and the UK, including:

- A British Home Office study that drew on interviews with staff in the professional standards units (PSUs) of eight UK police forces and the National Crime Squad (Miller 2003).[2]
- Reports from police oversight and similar agencies including, in Australia, the Victorian Office of Police Integrity[3] and the New South Wales Police Integrity Commission, and in the UK, Her Majesty's Inspectorate of the Constabulary.
- Reports from the Leveson Inquiry in the UK (esp. Leveson 2012a, 2012b).

When police information gets into the wrong hands …

A perennial problem

The problem of inappropriate access and/or use of police information for private purposes is common to police forces across the world. It has long been recognised that "[i]nformation and intelligence is the lifeblood of policing", representing "the most valuable commodity the Police Service needs to protect" (HM Inspectorate of Constabulary 1999: 39; Office of Police Integrity

2010a; Commissioner for Law Enforcement Data Security 2009; KPMG 2009). Police officers *necessarily* have access to a range of official information sources in the course of their usual duties, including formal records such as paper and digital files and documents, and various forms of verbal and similar 'intelligence'. The increased focus in contemporary policing on intelligence-led methods (Miller 2003: 13) and on the use of information technology (Chan *et al.* 2001) enhances both the amount of information available to police officers and the means to gain access to such data.

A 2003 British Home Office study of police corruption in England and Wales (Miller 2003) found that the compromise of police information was "the single most common type of corrupt activity" in UK policing (p.10, iii). It was suggested that "the picture of corruption [in England and Wales] is *dominated* by the leaking of information to those outside the organisation" (Miller 2003: 8, emphasis added). Misuse of information represents a major risk in contemporary policing, given that "Information, or law enforcement data, held by police can … be extremely valuable to individuals or groups outside law enforcement agencies" (Office of Police Integrity 2010a: 8). Confidential police information may be "what criminals most want to obtain, and is the currency corrupt officers have used when betraying their colleagues and their profession" (HM Inspectorate of Constabulary 1999: 39).

When police information gets into the wrong hands investigations may be compromised, criminals may evade justice, and the policing function may be undermined in a number of ways:

> The consequences … of information security and integrity failures can lead to catastrophic operational failures – complex investigations can be compromised, criminals can evade apprehension and conviction and the lives of law enforcement officers and others can be put at risk. Information security failures also lead to reputation damage. Other law enforcement agencies are less likely to share their sensitive information with an insecure and unreliable partner. Individuals and organisations are understandably reluctant to fully and frankly disclose information to a law enforcement agency that has a reputation for leaking. A law enforcement culture that is disrespectful of the security and integrity of law enforcement data is one that will fail to attract and retain the right law enforcement officers. (Commissioner for Law Enforcement Data Security 2009: 7; see also People 2008)

In a 2010 review of "recurring themes" in the management of high profile police investigations, the Victorian Office of Police Integrity noted how the "possibly unforeseen and unintended consequences" of information disclosure can strike at the very heart of the policing function:

> In addition to compromising the privacy of individuals, the success of an operation or the integrity of an investigation or prosecution, other consequences of unauthorised disclosures may be even more serious. There are two high profile cases since 2004 where publication of leaked information immediately preceded the murder of key police witnesses in police corruption cases. There are other instances where leaked information has also:
>
> - put at risk the safety of operational police
> - created opportunities for suspects to collude, flee or destroy evidence
> - compelled a premature response by police requiring a covert operation to become overt
> - re-traumatised victims
> - caused witnesses to withdraw cooperation.'
>
> (Office of Police Integrity 2012: 16; see also Office of Police Integrity 2010b)

It stated that "[a]lthough many of our investigations indicate a reckless disregard for the consequences of 'leaking', only a few indicate a deliberate self-interest or malicious motivation behind the leak" (Office of Police Integrity 2012: 15; see also People 2008). Nevertheless, it was suggested that "[t]he prevalence of 'leaking' from within Victoria Police … indicates that Victoria Police has a cultural problem" that manifests in "a disturbing pattern of longstanding behaviour whereby police routinely leak confidential and sensitive information" (Office of Police Integrity 2010b: 16, 9).

Davids (2005, 2008) analysed the problem of inappropriate access and use of police information as part of a wider study of conflict of interest, noting that the problem of information misuse extends beyond mere *curiosity* or *interestedness*, with many cases involving active attempts to advance personal interests. Around many parts of the world, public awareness of the playing-out of conflicts of interest in public roles has contributed to a general decline in trust in public officials (Boyce and Davids 2009). Unauthorised access and disclosure of police information presents an archetypal conflict of interest because it unambiguously involves the placement of private interests ahead of the public interest. It also generally breaches police information access protocols and *ipso facto* may itself be classified as police misconduct or corruption as well as being a possible precursor to more serious breaches of duty (Davids 2008).

Unauthorised disclosure of information from a police database is a criminal offence in some jurisdictions.[4] In addition to statutory regimes, the behaviour may also be caught through a broad common law offence of 'misconduct in public office' or statutory codifications of the same offence.[5] The majority of misconduct in public office offences prosecuted at common law appear to involve public officials (but not necessarily police officers) who make improper use of information (Crime and Misconduct Commission 2008: 29). However, for police, such matters are more commonly dealt with through internal discipline systems and recourse to criminal prosecution and sanctions is unusual (Director—Police Integrity 2005b: 23).[6]

Social accountability and public trust in policing

Cultural problems that are manifested in an apparent normative acceptance of the misuse of police information represent a particular challenge for developing appropriate systems of accountability. In many respects, accountability is an elusive concept – "one of those evocative political words that can be used to patch up a rambling argument, to evoke an image of trustworthiness, fidelity, and justice, or to hold critics at bay" (Bovens 2005: 182). Bovens notes that it therefore has rhetorical and iconic dimensions that evoke notions of 'good governance'. 'Public' accountability relates both to the status of both account-giving and account-giver – relating to the public sector, where the account-giving is done in some public way, to (or on behalf of) the public, and relating to public managers, spending public money, exercising public authority, and/or managing under public law.

It may generally be agreed that public accountability includes both administrative forms manifest in the structures and organisational arrangements, and a moral or ethical sense that revolves around the need for public officials and public institutions to consistently demonstrate integrity and trustworthiness. Accountability has an inherent social dimension to the extent that an actor (individual or organisation) is obligated to explain and to justify their conduct to some forum, and to take responsibility for that conduct and its effects on others (Day and Klein 1987; Sinclair 1995; Bovens 1998). In this chapter we utilise the social accountability perspective enunciated by Boyce and Davids (2009, 2010). This is a broad-scope approach that incorporates multiple dimensions of

answerability (to formal systems of accountability) and responsibility (in the sense of virtue – see Bovens 2010, 1998). Recognising that public officials who possess and exercise legal power and authority are accountable to the wider public for the exercise of that power, the social aspect adds a focus on the bottom–up dimension of responsibility that complements traditional top–down hierarchical perspectives (Roberts 1991).

A social accountability perspective can help to transcend the limitations of formal accountability mechanisms that "may bypass central questions of moral responsibility that lie at the heart of corruption" (Boyce and Davids 2009: 632). It addresses both the need for appropriate accountability mechanisms, including regulation and enforcement, and the imperative to address ethical, organisational, and cultural dimensions through a focus on accountability as virtue (Bovens 2010). Thus, social accountability seeks:

> … to nurture proactive accountability through the development of responsibility as a personal and subjective sense of rightness and good conscience … [as well as] accountab[ility] for the exercise of … power. Accountability operates through organisational structures and hierarchies, but public officers must also be accountable to the broader community … (Boyce and Davids 2010: 283–284)

The pervasive, persistent and recurring nature of problems surrounding unauthorised access to or use of police information suggests that "progress, over the long term, has been unacceptably slow" (Commissioner for Law Enforcement Data Security 2012: 4). The more recent revelations from the Leveson Inquiry suggest that both operational police and police management may have insufficient practical understanding of the nature and dimensions of the problem of inappropriate access to and use of information, and of the accountability issues involved. These matters are examined in the remainder of the chapter.

Inappropriate access and use of information: The nature of the problem

Miller (2003) reported that abuse of the UK Police National Computer (PNC) database was said to be the subject of approximately five per cent of UK police disciplinary cases (p. 13, fn 7). The Leveson Inquiry provided more recent evidence on this issue, with the Independent Police Complaints Commission reporting to the Inquiry that between 2006/7 and 2010/11 there were 5,179 recorded allegations relating to the improper disclosure of information, constituting around two per cent of all allegations recorded for the period (Furniss, quoted in Leveson 2012a: 810).

In Davids' Australian study, fifteen per cent of all conflict of interest cases involved the misuse of confidential police information, with two-thirds of these cases involving disclosure of information to outside parties (see Davids 2008: 153). Contemporary concerns in Australia regarding unauthorised disclosure of police information are reflected in reports from various independent oversight agencies, which have identified the issue as a particular problem that often presents as a crucial dimension or common denominator in many flow-on issues for policing (e.g. Director—Police Integrity 2005c: 23; Crime and Misconduct Commission 2011). In addition, a number of high profile official investigations examining the circulation of highly protected Police Information Reports or parts thereof to media, criminals and others underscores the need to protect confidential police information (Director—Police Integrity 2005d).

Information and communication technologies

ICTs and official computer databases are increasingly important to policing. In Australia, which has separate police jurisdictions in each state, each police force holds its own computerised database; however, as in the UK, there is a National Police Reference System, which can link information for

Australia's state-based police agencies (known as "CrimTrac" – http://www.crimtrac.gov.au). Databases provide police officers with online access to information relating to crime reports and associated dealings between police and victims, offenders and members of the public. For example, the Victoria Police 'LEAP' (Law Enforcement Assistance Program) computer database is:

> … used to record crime incidents and personal particulars and captures a range of information including details of lost and stolen property and vehicles of interest to law enforcement. LEAP provides an online interface to internal and external systems to facilitate name, vehicle and place searches. It is also used in relation to fingerprint classifications, case management and intelligence collation. Access to LEAP peaks at around 350,000 transactions daily and the system is lined to over 5,000 terminals 24 hours per day. The system is extensively used in support of operational policing and as a resource to provide management data.
>
> Information stored on LEAP is, in large part, sensitive and personal … (Director – Police Integrity, 2005b: 9–10)

The ease with which access can be gained often means that it is a relatively simple matter for a police officer or member of police staff to obtain information in which he or she has no *official* interest. Increasing use of ICTs has made the perpetration of ethical breaches easier because formerly bureaucratic processes have been replaced by technology accessible to all those working inside police institutions. Although ICTs also provide the possibility of tracking and monitoring police access to such information, recent history suggests that attempts at 'technological fixes' have been less than successful. Although access codes and audit trails provide a good source of evidence of database use, such evidence is not always conclusive or definitive and is generally only useful *ex post* – as a source of evidence after misconduct has occurred. Reliance on access codes has notable weaknesses; for example, police officers invariably know, or can guess, the access codes of colleagues (Independent Commission Against Corruption 1992: 13, 108–109), or steal them from other police officers (*R v Bunning* [2007] VSCA 205). Further, allegations of inappropriate access to police databases commonly lead to a range of stock responses from officers, such as:

- They are unable to recall why they performed the transaction and their duty book, which might have assisted them to remember, cannot be located;
- There is a common practice to leave computer terminals open and it must have been someone else who used their ID; and
- They could have been using the computer and someone else requested them to perform a transaction on their behalf but they have no recollection as to who that person might have been (Kennedy Royal Commission, quoted by Director—Police Integrity 2005b: 23).

Similarly, a Victorian Ombudsman's Report made the point that, when interviewed:

> … members have commonly justified their access by reference to some police duty - for example, to avoid forming a possible undesirable personal association; to ascertain from car registration details seen in the vicinity of a person's home if the member or his family were under possible surveillance or to ascertain whether there were outstanding warrants against a family member. (The Ombudsman 2001: 20)

Evidence to the Leveson Inquiry from various UK Constabularies did not paint a clear picture of computer database misuse, however some important evidence emerged relating to Britain's PNC database. The PNC (established in 1974) links a number of separate databases and holds a range of records including the details of individuals who are convicted, cautioned, arrested, wanted or missing; the registered keeper of vehicles; individuals with a driving licence entitlement or who are

disqualified; certain types of stolen and recovered property including animals, firearms, trailers, plant machinery and engines; it supports enquiries against the national phone register and contains the details of individuals on the national Firearms Certificate Holders Register. The PNC is used by all UK police forces and other authorised agencies, including those with a brief to examine serious organised crime. Evidence to the Inquiry indicated that it has "in excess of 250,000 users and handles in excess of 169 million transactions per annum, giving a daily average of just under 463,000 transactions" all of which were subjected to user activity and logging protocols (National Policing Improvement Agency Head of PNC Services, Karl Wissgott, quoted in Leveson 2012a: 812).

It is perhaps surprising, given the huge transaction rate of the system, that it was claimed that the PNC was only "misused occasionally" for unlawful disclosure, with the associated belief expressed that the current security measures are "effective and proportionate" and that there was no "widespread systemic problem, nor that any particular and specific additional security measure would be effective" (Wissgott, quoted in Leveson 2012a: 813). By contrast, the Commissioner of the Metropolitan Police Service confirmed that over 200 officers and support staff had been disciplined for unlawful PNC access in the previous 10 years, with 106 of these matters relating to the last 3 years; it suggested additional safeguards were required (Hogan-Howe, cited in Leveson 2012a: 813). These figures and the implicit trend represented therein provide an indication of the persistence of this problem – which is likely to be even more significant given the likelihood of additional undetected and unknown breaches.

There is some evidence to suggest that there is a tolerance for *accessing* database information, which is often regarded as a relatively minor offence. This seems particularly the case if access is motivated by professional curiosity rather than malicious intent or nefarious motives and if the information is not passed on, or disclosed, to third parties (Davids 2005).[7] The idea that police members are *entitled* to access information may be culturally ingrained within police forces (see Director—Police Integrity 2005b: 15).
It is clear that the increasing use of technologically-mediated systems has brought a new series of challenges for systems of accountability in terms of their effectiveness and reach. In circumstances where information is ever more important to policing, it is vital to recognise that "[i]nformation security and integrity … are the preconditions for effective information systems that empower police to do their jobs effectively and safely" (Commissioner for Law Enforcement Data Security 2009: 7). The technological tightening of audit trails may assist in identifying system users and provide proof of access, but debate about the legitimacy of individual actions often centres on the *justification* offered for accessing information. This emphasises the importance of ensuring that the design and implementation of information systems is intertwined with systems of accountability, such that all users of ICTs are cognisant of their responsibilities and accountabilities for the use of official information.

Other sources
Whilst police databases provide a ready and convenient source of information, police officers may also make private use of information gleaned in the ordinary course of their duties – for example, during an investigation – or may actively use a police position to *obtain* information for private purposes. In the latter instance, information may be sought and obtained solely for private purposes that would not otherwise be obtained by the police officer either in an official or non-official capacity. Davids (2008: Ch 6) identified two sources of police information that were significant in this regard: (1) information gleaned in the ordinary course of police duties and not necessarily entered into computerised databases; and (2) the *active* use of a police position and

police channels to obtain information which would not otherwise be available to the police officer (either in an official or non-official capacity) (see also Miller 2003: iii).

Dimensions of the problem: domestic use

Miller (2003: 13) characterised the typical "domestic" use of information as involving inappropriate use of police databases for "personal interest purposes" such as the conduct of checks on friends and neighbours or on motor vehicles that a police officer is considering purchasing. This type of abuse was said to be "a common feature of misconduct cases". Davids (2008) expanded Miller's categorisation to distinguish several other domestic uses of information: private commercial dealings; private business and secondary employment; to assist friends or family members in private commercial dealings; personal advantage in private, non-commercial matters; private family matters; intimate personal relationships; and professional curiosity.

Analysis of cases by Davids found that many problems arise in the context of private business, commercial and employment dealings and arrangements, where information itself is often an important 'currency'. Police information may be obtained from databases previously outlined, or the position of police officer may be used to obtain information (in relation to a private matter) that would not be available to an ordinary citizen.

The use of police information in such contexts may also be combined with injudicious behaviour towards those engaged in business with the officer. For example, a case where a police officer obtained personal details (home address; licence details) of a debt collector with a major finance company, who had contacted the officer in relation to monies owed on a vehicle (Case 69). In another case, a police officer used his position to obtain prior ownership and sale details of a motor vehicle he had purchased in a private sale, then used this information in an attempt to have the sale (to him) nullified and have his money returned (Case 121). Yet another matter involved a dispute over the parts used in repairs to a motor vehicle, where an officer pretended to be conducting an official investigation in order to obtain information that would assist him in this dispute (Case 64).

Police may also attempt to obtain a private benefit from the use of information in the context of their own private business or secondary employment arrangements. In this context, the use of police information may be associated with an apparent intention to derive a financial benefit that would not otherwise be available to the individual. There is significant potential for such interests to interfere with a police officer's impartial enforcement of the law. Case examples include:

- Allegations that a police officer used unreported crime information (not entered onto the police database, contrary to regulations) relating to an alleged robbery in order to assist in soliciting or securing private security business (Case 310);
- Intended use of information obtained in the course of police duties to assist in setting up a private business in police recruitment, education and training services (Case 234);
- A police officer, whilst on his way to work (on duty), conducted an ostensibly 'random' licence check of a driver; he subsequently obtained database details about the driver and contacted the person in an effort to recruit him into a work from-home networking business opportunity (Case 236); and
- Secondary employment in the surveillance or private investigations industry and the use of official motor vehicle registration information in this context (Case 345).[8]

The use of police information in the manner described above may also extend to attempts to assist family members or associates of police in the context of their own private business and commercial dealings, such as debt collection matters or business/commercial disputes (Case 256) or tenancy disputes (Case 176).
Police officers may also seek to gain a personal advantage in private, non-commercial matters, including what would normally be regarded as relating to 'family' and relationship matters. For example, the use of a police database to track an ex-spouse in relation to problems concerning maintenance payments or other family law disputes (Cases 120, 152, 375), including child custody disputes (Case 360). There is also evidence that police officers may seek to use police information in the context of attempts to further intimate personal relationships, such as obtaining personal particulars of a person in whom the individual officer may be 'interested' (Cases 113, 111, 19), or personal information about a former domestic partner (Case 223). Information use in some circumstances may be easily (mis)interpreted as constituting harassment or stalking (Case 268).
The 'domestic' uses of police information extend to police officers accessing personal details of members of the public and other matters on the basis of an apparent or claimed "professional curiosity". Evidence suggests that police accountability systems tend to deal with such matters on an *ad hoc* or reactive basis. For instance, following a 2003 public scandal over several police officers' access to the police files of a candidate standing in a state government election, the then Chief Commissioner of Victoria Police announced that much tougher rules and protocols over access to police information would be instituted. Under this approach, "professional curiosity" would not be an acceptable reason for accessing any file, even where there was no malicious intent.[9] While this could be regarded as representing an appropriate response in relation to the formal rules for information use, such rule-changes alone are insufficient to challenge the apparent *cultural* acceptance of domestic use of police information.

In 2005 in Western Australia, 580 police officers were censured and sanctioned for sending emails carrying confidential images of two young men who died in the Great Sandy Desert. Multiple graphic photographs of the men's bodies were circulated, with some ending up on a United States-based website featuring macabre events. Such was the public outrage that police management convened a "restorative justice" event that involved relatives of the dead men being invited to a forum in which they could tell fifty of the offending police officers of the pain and suffering they had experienced upon learning of the unauthorised circulation of the images.[10] Again, such a restorative justice event may be regarded as an appropriate response in the individual circumstances, perhaps producing some individual acceptance of personal responsibility, but the *ad hoc* nature of such an approach is likely to be insufficient to produce the kind of cultural change that is central to the acceptance of the broader responsibilities that attend to a police position and accompanying accountability for actions.

Dimensions of the problem: disclosure
The release of confidential police information to outside parties has been an official concern for many years. As far back as 1993, the Victorian Deputy Ombudsman (Police Complaints) expressed concern over both the frequency of this type of complaint and the high substantiation rate (The Ombudsman 1993: 11).[11] The disclosures identified by the Deputy Ombudsman included "purposeful, mischievous 'leaks'" of several kinds of information:

> …the names of people charged, criminal histories, police intelligence, police photographs and vehicle registration details. The types of information most commonly released have been criminal histories and registration details. The release has usually been to friends and relatives of the police involved and, more generally, to representatives of the media. (The Ombudsman 1993: 11)

As noted by the Victorian Commissioner for Law Enforcement Data Security, leaking of police information is particularly problematic on a number of fronts:

> As has been demonstrated in an international context, the actions of a single individual who releases sensitive information without authorisation can have a disproportionately large effect on organisational security and public trust and confidence in the institutions tasked with protecting community safety and security. (Commissioner for Law Enforcement Data Security 2012: 4)

Miller found that the "leaking of information plays a central role" in the "more common form" of "individual corruption" in England and Wales, whereby "members of police staff engaged in corrupt activities in isolation from colleagues" (2003: 10, iii). He outlined several types of leaks of police information to outside parties: "'low-level' leaks" to friends or associates, such as carrying out police data checks for friends running businesses, which was described as "common"; leaks of information, including "sensitive operational police information" in relation to "high profile cases", to journalists in the media – an activity that "tended to involve payment of police staff by journalists" (clearly identifying this problem long before the Leveson Inquiry); and the deliberate leaking of police information to criminals, whether directly or through an intermediary – either as a favour or for payment (Miller 2003: 13). Davids' (2008) empirical study found several significant categories of leaks to outside parties: low-level leaks; leaks in the context of a business or commercial matter; leaks in the context of criminal investigations, legal, or associated matters; and leaks to the media.[12]

Low-level leaks

Many low-level leaks may be conceptualised as an extension of the 'domestic' use of information, where the personal or professional interests or curiosity of the police officer is replaced or supplemented by the curiosity or interest of another party to whom information is disclosed. Thus, a police officer may pass on police information in order to assist family members or associates of police in the context of their own private business and commercial dealings, such as tenancy disputes (Case 365), personal relationships (Case 237), and other family-related matters (Case 242).

Davids' analysis showed that the conflict of interest involved in low-level leaks is often evident on the facts, yet not acknowledged either by the police officers concerned or police management – both often see the problem as relatively innocuous. As with the apparent acceptance of domestic use of information (above), a police culture that accepts or marginalises the importance of 'low-level' breaches does not recognise how even seemingly minor breaches in such matters may impinge on police integrity and damage public trust. One prosecuted case in Victoria involved the disclosure by a serving police officer to a former police officer (friend) of a number of police manuals regarding the operation of speed detection devices – the context was the friend was intending to contest impending charges of exceeding the speed limit.[13] Although the defendant was acquitted because most of the material provided was also available on the internet, questions about partiality and 'helping a mate' are problematic from a public accountability perspective. Accountability systems, and individual officers, must attend to both the action itself and "political optics" (Davids and Boyce 2008).

Leaks in the context of a business or commercial matter, or secondary employment

At what might be regarded as the 'high end' of low-level leaks are leaks in the context of a business or commercial matter – 'high' because disclosure is motivated by a quite specific type of

business or commercial interest, and there may be particular damage to both the reputation of the Force and trust in the integrity of policing.

Problematic contexts include outside or secondary employment in the surveillance, private investigations, and process serving industries, where intelligence about police operations or motor vehicle and other similar data is particularly valuable (Case 345; Cade 380). A recognised problem exists in relation to "ex-police officers working in the private investigation industry who requested information" from former colleagues who are still serving officers (Miller 2003: 13). The opportunities for networks of police colleagues and former colleagues are significant, as illustrated by an organised illicit trade in police information that came to light in New South Wales In the early 1990s. Here a corrupt trade in government information involved a "vast information network … freely and regularly exchanged for many years" (Independent Commission Against Corruption 1992: 14, 5). The trade included the provision of licence records and criminal histories to outside parties – often private inquiry agents, many of whom were former police officers, with the ultimate recipients of information, including insurance companies and financial institutions. These external parties were found to be a significant part of the problem insofar as they 'embraced' the trade and provided a ready market that contributed to its development.

Cases such as this illustrate the importance of police accountability systems dealing not just with the actions and activities of officers, but also with their personal relationships and involvements. Individual officers and police organisations must recognise the need to separate clearly private from personal interests and associations. Although problems with some kinds of personal relationships, such as associations with criminals or suspects, are well recognised and generally dealt with systematically within police accountability systems (through regulation, registration, or prohibition of interests), the more general problems that can flow from private relationships and involvements must also be attended to (Davids 2006). Recognition of the 'shades of grey' in professional integrity and operational decision-making must be accompanied by enhanced understanding of the form of 'active accountability' that requires development of a sense of personal and collective responsibility in complex ethical situations.

Leaks in the context of criminal investigations, legal, or associated matters

Leaking of police information to criminals and others has been identified as a particular contemporary problem in Australia and the UK (Director—Police Integrity 2005a; Miller 2003; Davids 2008: 228–232). In Victoria, there has been much concern surrounding leaks of sensitive police information to criminals. Some of these leaks have compromised major drug-trafficking investigations, prosecutions and, in one instance, were believed to have resulted in the murders of a police informer and his wife (Director—Police Integrity 2005d; Taskforce Keel – see Victoria Police 2013).

Leaks of police information of this nature are much more serious than low-level leaks both because of the nature of the information and the context within which it may be used, which includes police investigation, criminal matters, or in civil or criminal proceedings. This kind of conflict of interest may compromise the administration of justice in the matters concerned, hinder police operations, assist criminals to evade detection and/or prevent them being brought before the law (Cases 192, 241, 289). The impartiality of police overall may be called into question. Significant cases brought before the Victorian courts have included matters involving the disclosure of police database information to a drug dealing friend and his associates regarding an ongoing investigation into the associates,[14] and the disclosure by a detective of confidential police

information from various sources regarding police investigations, surveillance, telephone intercepts to a registered police informer and drug dealer.[15]

Other cases examined in Davids' study involved the supply of police evidence briefs, witness statements, criminal histories of individuals, and other sensitive information. Most cases involved concerns about releases of information to alleged offenders but it can be equally problematic for the administration of justice to provide information to an alleged victim in a criminal matter (Case 212). The context of such leaks included pending or possible criminal charges (Cases 76, 15), civil proceedings (Cases 45, 115), employment law issues (Case 160), and family law and other family or relationship matters (Cases 255, 86, 18, 149, 247). In addition to concerns over conflict of interest, such matters could be regarded as attempts to pervert the course of justice and could impact on the viability of legal proceedings (Case 15).

Such cases illustrate the potential for damage to be caused to individuals, which is present whether leaked information (e.g. about a criminal history) is accurate or not (e.g. about allegations or other unproven matters). This reiterates the importance of police officers being aware of their duty not to release confidential information, *and* the general injunction to not allow personal interests to interfere in official actions and decisions. Leaks of information may *seem* harmless from the perspective of the police officer involved, but the flow-on implications for public trust may be substantial.

Even more serious are deliberate leaks to criminals, which may be done as a favour to illicit associates of a police officer or in return for payment (Miller 2003: 13). Leaks to criminals may also be unintended, and may effectively result from what may be thought of as a low-level leak, as found in Miller's study:

> Leaked information can find its way to criminals even where this is not deliberately intended. In some cases, it is passed to associates, such as relatives, friends, social acquaintances or even ex-police colleagues, who, in turn, pass this information on to criminals. These types of arrangements apparently allow some criminals to network their way indirectly into police circles to obtain police information … some criminals [appear] to have a number of links of this kind with different members of police staff. (Miller 2003: 17)

Recent revelations in Victoria indicate a large volume of police records (including LEAP database records and sensitive information relating to police informers) have been provided to high-profile 'outlaw motorcycle gangs', resulting in criminal charges against one officer and investigations into other potentially corrupt police (Taskforce Keel – see Victoria Police 2013: 63). Allegations include the use of performance-enhancing drugs, leaked intelligence regarding crucial drug operations, and inappropriate social relations (police and organised crime figure friendships are particularly problematic) between serving police officers and senior motorcycle club members convicted of drug dealing.[16]

Leaks to the media

The Leveson Inquiry in the UK reinforced the notion of policing by consent and drew attention to the important role of the media in shaping the relationship between police and citizens. It pointed out that public confidence in the police is axiomatic in the policing-by-consent model and noted the crucial role the media can play as a conduit for intelligence in relation to preventing and solving crime. Thus, effective and professional relationships between police and the media are important for successful policing. They can also prevent media stories from inadvertently

scuppering investigations and in worse case scenarios jeopardising the safety of victims or highly sensitive case planning.

In its submissions to the Leveson Inquiry, the Commissioner of the Metropolitan Police Service (MPS) identified five areas in which "keeping the media properly informed about policing and criminal matters was critical to the functioning" of the police (Leveson 2012b: 7465):

1. Police can communicate key messages associated with preventing and detecting crime;
2. A healthy relationship can increase public understanding of the work of policing;
3. Police can seek the assistance of the public, via the media;
4. Public confidence in the police may be enhanced, generating greater understanding of police policies and initiatives; and
5. The relationship provides a means whereby the public can scrutinise police actions and policies, and the police can "test the persuasiveness of their strategies, policies and tactics" (Hogan-Howe, cited in Leveson 2012b 746–747).

The key concern outlined by Miller (2003) for the release of police information to the media was that it often involves the making of payments to police officers for information provided to journalists. Concern was also expressed that the disclosure of sensitive operational police information could directly impact on police sources. It was also noted that there could be an association between leaks to the media and to criminals: "Certainly, where information is leaked to journalists it is likely to end up in the public domain, which will inevitably include criminals" (Miller 2003: 14).

In high-profile cases the release of confidential or sensitive police information to the media may directly impact on police sources by jeopardising the security of witnesses, informants and, on occasion, the operation itself (Miller 2003: 13; and see Director—Police Integrity 2005d). A 2013 prosecution in the Victorian Courts involved a senior detective in an anti-terrorism operation who leaked advance information about the raid to a journalist.[17] There was no suggestion that the officer gained as a result of the leak; he and the journalist appeared to have had a long-standing relationship and shared some mutual professional interests. In another Victorian matter that was prosecuted through the courts, the issue was not a release of information to the media, but the publication of very sensitive police material in a book written by a serving detective. The material relating to a high-profile investigation was regarded by police management as possibly leading to the identification of police informers.[18]

Balanced against the general injunction against releasing information to the media is the notion that the release of police information to parties outside the organisation, including to the media, may form an important public accountability function, sometimes known as 'whistleblowing'. A 1990s case in Victoria involved a prominent whistleblower who made unauthorised public comments about internal police operations, primarily relating to a major internal investigation. These whistleblower's comments were made to various media outlets, including mainstream and radical print media and radio (Case 318). An investigation of the underlying case by the State Ombudsman and Victoria Police internal investigations (1995–1997) resulted in disciplinary charges against approximately 550 Victoria Police members (see The Ombudsman 2003: 72). The whistleblower himself faced disciplinary proceedings for allegedly failing to comply with a lawful instruction from the Chief Commissioner to cease making public comments; it was argued that public comment could compromise a specific police operation.

Taking a different perspective, Sandra Laville, Crime Correspondent for the *Guardian* newspaper, identified to the Leveson Inquiry (2012b: 747) how journalism plays an important role in maintaining the media as the "people's 'eyes and ears'" in relation to the coercive powers afforded to the police. On this basis, a proper public interest and democratic function of the media is to challenge, interrogate and question police actions. The Inquiry noted the possibility of tension in the relationship between media and police, pointing to the differing needs of each party in relation to high-profile investigations (Leveson 2012b: 748–750). It is broadly recognised that:

> Both police and the media have an important role in serving the public interest … Media attention can assist police to solve crimes and convey important messages about emergency evacuations in natural disasters, road safety or alcohol-related violence. The media is also used to hold police accountable to the public they serve. (Office of Police Integrity 2012: 25)

As the Leveson Inquiry demonstrated, however, police–media relations are fraught with difficulty and it is not only the public image of integrity and impartiality in policing that is at stake:

> In addition to breaching the privacy of individuals, public airing of details from an investigation before it is finalised compromises the integrity of the investigation. When details of offences are publicly aired there is a real risk other evidence gathering processes will be tainted. For example, leaked details can trigger a witness to provide an account that is influenced by what he or she has read or heard in the media, rather than providing details from the person's own knowledge. Furthermore, if only one version of an incident under investigation is publicly aired, public opinion about the case can be determined without access to a full set of accurate data. This can give rise to public expectations that police will act in a particular way, for example charge a person. This places pressure on police to meet those expectations. (Office of Police Integrity 2012: 17)

Buttressing integrity through accountability

Conflict of interest and police integrity

The public impact of ethical breaches relating to disclosure and/or use of police information is high. The failure of honesty and impartiality on the part of individual public officials can have a particularly damaging effect on public trust in the integrity and impartiality of police. When integrity is not evident, public trust and confidence in the whole police organisation is affected. In part, public trust relates to the extent to which individuals expect others to be constrained by the duties and requirements attached to their roles, and to act to prevent abuses of official positions. It relies on a belief in the integrity of both individual police officers and police organisations as a whole. In addition to directly compromising investigations, unauthorised disclosure may negatively impact many practical aspects of policing. For instance, it may lead to reluctance on the part of those who supply information to police to do so in the future, which may undermine the continued supply of information essential to the policing function (see Billingsley *et al.* 2001).

In terms of conflict of interest, the leaking or use of official information for non-official purposes involves private interests (including the interests of family, friends and associates of a police officer) prevailing over public ethics and public duty. Notions of friendship and mateship, which may motivate leaks, are equally misguided in situations where a police officer is asked by a friend, relative, acquaintance, former colleague or private inquiry agent to make unofficial inquiries on their behalf. Even though low-level leaks may be regarded as minor, police officers can be caught in a conflict between loyalty to family or friends and their obligation to keep confidential those matters coming to their attention as a police member. It may also be that "… officers do not appreciate the seriousness of unauthorised disclosure at any time" (HM Inspectorate of

Constabulary 1999: 42). Effective management lies in the responses that police make to these requests and in recognising that this area presents a problem that police officers may reasonably expect to have to confront.

Accountability

Earlier in the chapter, it was suggested that public accountability includes both administrative dimensions (structural, organisational, regulatory) and a moral or ethical sense that relates to the *demonstration* of integrity and trustworthiness. Bovens (2005, 2010) highlights several key functions of public accountability:

1. democratic control within institutional arrangements, which may be regarded as including hierarchical accountability within organisations and agencies, ultimately proceeding up to ministerial and governmental levels;
2. enhancement of the integrity of public governance by preventing and detecting corruption, nepotism, abuse of power, and other forms of unauthorised and inappropriate behaviour, particularly in the context of the application of delegated powers;
3. maintaining and enhancing the legitimacy of public governance – a particular challenge in light of a general decline in public confidence in public institutions and an absence of automatic deference to public authority;
4. ritual and purifying functions that may provide some form of public catharsis in response to tragedies, fiascos, scandals, and failures;
5. fostering individual and organisational learning in ways that discourage or prevent future misconduct and enhance future performance – often through the development and reinforcement of appropriate norms and organisational culture that induce reflexivity and openness.

Dealing with the multiple challenges of accountability that are reflected in these functions implicates "... a whole series of flows, circuits, connections, disconnections, selections, favourings, accounts, holding to account and attempts at analysis" that means accountability in action involves a certain degree of "messiness" ((Neyland and Woolgar 2002: 272). As Bovens (2005) comments, "[p]ublic accountability may be the complement of public management—it certainly is the predicament of public managers" (Bovens 2005: 202).

The traditional concept of accountability in the public sector involves answerability to the community for, and exercise of, legal power and authority by a public official. The broader concept of *social* accountability invoked in this chapter takes a bottom–up social, rather than a top–down organisational, perspective in order to address ethical, organizational, and cultural dimensions of organisational management. Thus, it also encapsulates both an "ex post answering for past decisions and actions and the need to have mechanisms in place that seek to deal with neglects of duty before they happen … [including] some level of attention to political optics in terms of 'how things look' to reasonable members of the public …" (Boyce and Davids 2009: 604). The inclusion of this latter element recognises the importance of public confidence in public institutions. There is an implicit recognition here that social accountability involves more than "internalizing the values, processes and practices of accountability" that may produce rule-bound approaches that obviate the need to address how "performance … establishes the moral order that can be seen to provide the reference point for the mess and flows of connections" (Neyland and Woolgar 2002: 272).

Formal mechanisms of accountability embodied in organisational structures, rules, procedures, and the like are vital to the first four functions of accountability outlined above and are instrumental to good governance. Just as important, and vital to the development of accountable organisational cultures that underpin the operation of accountability mechanisms, is the nurturing of accountability as individual and organisational virtue – an active sense of goodness and rightness that reflects a commitment to integrity and development of public trust.

Accountability as a mechanism and accountability as virtue are complementary and mutually reinforcing, but must be separately recognised and addressed (Bovens 2010). The social accountability framework for public sector conflict of interest developed by Boyce and Davids (2009, 2010) tackles the three core dimensions of the problem via three key elements of social accountability, with a 'reasonable person' standard (see Figure 1).

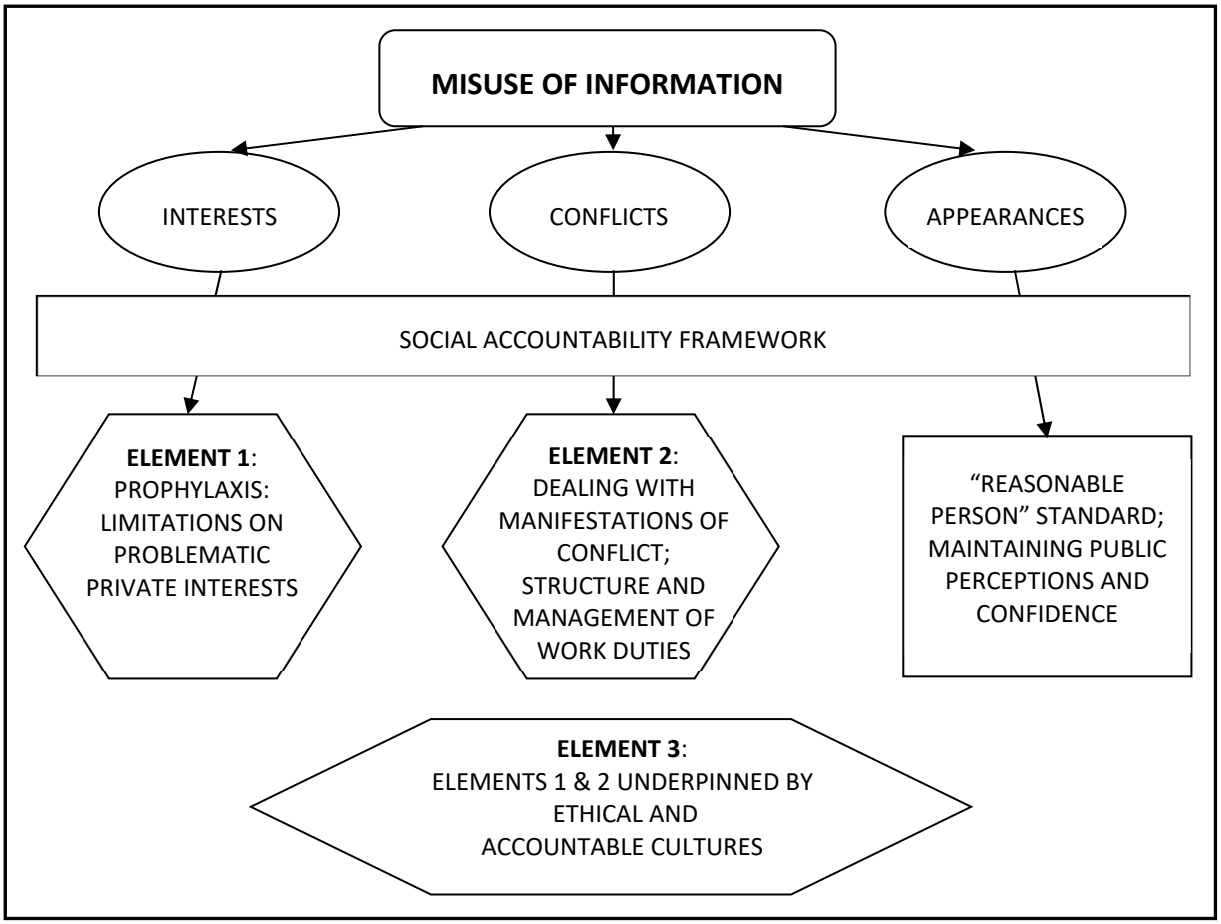

Figure 1: Social accountability framework for police integrity in the context of private interests
(adapted from Boyce and Davids 2009, 2010)

It is possible for an accountability system to deal with unauthorised use of confidential police information as an aspect of the broader problem of conflict of interest. Thus, problematic *interests* are attended to by limiting or prohibiting certain private interests that are inherently problematic. Such interests may be defined for this purpose as identifiable types of private interest that are deemed to be especially problematic, and therefore unacceptable, due to inherent incompatibility with police roles. The analysis in this chapter suggests that this is likely to include interests such as associations with criminals, commercial or off-the-record relations with journalists, and identifiably problematic forms of outside or secondary employment or business arrangements (including in the private inquiry industry).

Nevertheless, it is recognised that not all potentially conflicting interests can be effectively or reasonably regulated, such as those associated with familial and friendship relationships. These interests are recognised as giving rise to possible conflicts in certain circumstances only, and may be dealt with through the structuring of roles and functions so that officers are not involved in matters that may give rise to a conflict of interest. This requires both awareness of the potential problems and a preparedness to manage them in a situation-specific manner. These two elements – dealing with problematic interests and potential and actual conflicts – are buttressed and underpinned by ethical and accountable organisational cultures. Finally, appearances, or public perceptions are an essential consideration in dealing with conflict of interest issues. The key aspect of conflict of interest that undermines public trust and confidence in police relates to perceptions that a public position has been used for private advantage, challenging the ostensible commitment to serve the public rather than private interest. This is therefore destabilising for the policing function itself.

Understanding, managing, and responding to conflicts of interest generated by unauthorised and inappropriate use of confidential information requires consideration of'the intersection of subjective and objective elements. The subjective element relates to whether an individual has *actually* sought to gain a private advantage for themselves or others from the inappropriate use of a public position. The objective element revolves around application of a 'reasonable person' test that considers how things, in a particular circumstance, would *appear* to a reasonable member of the public. Because subjective concerns cannot be determined without 'knowing' the mind of the individual, effective management of conflicts of interest focuses on the objective element, which provides the standard or test against which judgements about conflict of interest may be made. This involves considering how things would look to a reasonable observer. Judgments about the appropriateness of particular classes of interests, and about the structuring of work duties to deal with conflicts, may also be made with reference to this standard.

Overall, a social accountability framework seeks to nurture proactive accountability through the development of responsibility as both a shared and personal and subjective sense of rightness and good conscience (see also chapter four), while accountability judgements can be made by applying an objective standard (Bovens 1998; Boyce and Davids 2009). As in any domain, public officials who hold power and authority must be accountable for their exercise of power. While accountability as a *mechanism* operates through organisational structures and hierarchies, broader social accountability and accountability to the community is a concept of accountability as *virtue* (Bovens 2010) that must consider both facts and appearances. Both forms of accountability are central to effective policing, because "[p]olicing is accountability, and without it the police have no legitimacy and hence cannot function effectively in a democratic society" (Punch 2010: 315).

Conclusion

> Changing the police culture of 'leaking' has proven to be difficult, it requires a two pronged attack – an education program to drive home an understanding of the risks and consequences of an unauthorised disclosure of information, together with a highly visible sanctions program which will demonstrate that such disclosures will not be tolerated. (Office of Police Integrity 2012: 17)

The issue of "leaks" of police information demonstrates how the power and position of police officers may be used to obtain information that is not required for official purposes, but which may be used to further the private interests of the police officer and associates. The conflict with

official police duties is clear and unambiguous. When such matters come to light, they have the potential to severely damage the reputation of a police force, and to diminish the willingness and propensity of members of the public to trust police officers who rely on them to support the policing function. Although a range of harms can result, in worst case scenarios, they can jeopardise investigations and lead to the injury or death of witnesses and informers. Failure to respect the trust that is placed in police to protect confidential information is also likely to have serious consequences for operational policing and for the reputation of a police force and the public trust that is placed in it.

Effectively dealing with the issues canvassed in this chapter requires some reflection on the nature and purposes of the public sector and of policing within the public realm. A clear "commitment to integrity and ethics in the pursuit of the public interest is a bedrock of a socially accountable approach" (Boyce and Davids 2009: 633), but effective accountability requires both the assurance provided by rigorous mechanisms and a commitment to embrace an active sense of responsibility and adherence to public values by individuals, managers, and their organisations.

References

Billingsley R, T Nimitz, and P Bean, Eds. (2001). *Informers: Policing, Policy*, Practice. Cullompton, Willan.

Bovens M (1998). The Quest for Responsibility: Accountability and Citizenship in Complex Organisations. Cambridge, Cambridge University Press.

Bovens M (2005). Public accountability. Oxford Handbook of Public Management. E Ferlie, L E Lynn, and C Pollitt. Oxford and New York, Oxford University Press: 182–208.

Bovens M (2010). "Two concepts of accountability: Accountability as a virtue and as a mechanism." West European Politics 33(5): 946–967.

Boyce G and C Davids (2009). "Conflict of interest in policing and the public sector: Ethics, integrity, and social accountability." Public Management Review 11(5): 601–640.

Boyce G and C Davids (2010). A social accountability framework for public sector conflict of interest: Private interests, public duties, and ethical cultures. Social Accounting and Public Management: Accountability for the Public Good. A Ball and S P Osborne. New York and Abingdon, Routledge: 275–286.

Chan J, D Brereton, M Legosz, and S Doran (2001). E-policing: The Impact of Information Technology on Police Practices. Brisbane, Queensland Criminal Justice Commission.

Commissioner for Law Enforcement Data Security (2009). Annual Report 2008–2009. Melbourne, Commission for Law Enforcement Data Security.

Commissioner for Law Enforcement Data Security (2012). Annual Report 2012–2013. Melbourne, Commission for Law Enforcement Data Security.

Crime and Misconduct Commission (2008). Public Duty, Private Interests: Issues in pre-separation conduct and post-separation employment for the Queensland public sector. Brisbane, Crime and Misconduct Commission (Queensland).

Crime and Misconduct Commission (2011). Operation Tesco: Report of an investigation into allegations of police misconduct on the Gold Coast. Brisbane, Crime and Misconduct Commission—Queensland.

Davids C (2005). Police Misconduct, Regulation, and Accountability: Conflict of Interest Complaints Against Victoria Police Officers 1988–1998. Faculty of Law. Sydney, University of New South Wales.

Davids C (2006). “Conflict of interest and the private lives of police officers: Friendships, civic and political activities.” Journal of Policing, Intelligence and Counter Terrorism 1: 14–35.

Davids C (2008). Conflict of Interest in Policing: Problems, Practices, and Principles. Sydney, Institute of Criminology Press.

Davids C and G Boyce (2008). “The perennial problem of police gratuities: Public concerns, political optics, and an accountability ethos.” Journal of Policing, Intelligence and Counter Terrorism 3(2): 44–69.

Day P and R Klein (1987). Accountabilities: Five Public Services. London and New York, Tavistock.

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

Director—Police Integrity (2005b). Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP). Melbourne, Office of Police Integrity.

Director—Police Integrity (2005c). Office of Police Integrity Annual Report. 30 June 2005. Edition 01. Melbourne, Office of Police Integity.

Director—Police Integrity (2005d). Report on the Leak of a Sensitive Victoria Police Information Report. Melbourne, Office of Police Integity.

HM Inspectorate of Constabulary (1999). Police Integrity, England, Wales and Northern Ireland: Securing and maintaining public confidence. London, Home Office Communication Directorate/HMIC.

Independent Commission Against Corruption (1992). Report on Unauthorised Release of Government Information: Volume I. Sydney, Independent Commission Against Corruption.

KPMG (2009). Review of Information Governance within Victoria Police: Final Report, KPMG (for the Commissioner for Law Enforcement Data Security).

Leveson B (2012a). An Inquiry Into the Culture, Practices and Ethics of the Press. Report (Volume I). London, The Stationery Office.

Leveson B (2012b). An Inquiry Into the Culture, Practices and Ethics of the Press. Report (Volume II). London, The Stationery Office.

Miller J (2003). Police Corruption in England and Wales: An assessment of current evidence. London, Home Office.

Neyland D and S Woolgar (2002). “Accountability in action?: The case of a database purchasing decision.” British Journal of Sociology 53(2): 259–274.

Office of Police Integrity (2010a). Information Security and the Victoria Police State Surveillance Unit. Melbourne, OPI Victoria.

Office of Police Integrity (2010b). Sensitive and confidential information in a police environment: Discussion Paper no.2. Melbourne, OPI Victoria.

Office of Police Integrity (2012). Victoria Police: recurring themes in the management of high profile investigations. Melbourne, OPI Victoria.

People J (2008). Unauthorised Disclosure of Confidential Information by NSW Police Officers. Research and Issues Papers. Sydney, NSW Police Integrity Commission. 2.

Punch M (2010). “Police corruption: Deviance, accountability and reform in policing.” Policing 4(4): 315–321.

Roberts J (1991). “The possibilities of accountability.” Accounting, Organizations and Society 16(4): 355–368.

Sinclair A (1995). “The chameleon of accountability: Forms and discourses.” Accounting, Organizations and Society 20(2/3): 219–237.

The Ombudsman (1993). Annual Reports: Report of the Deputy Ombudsman (Police Complaints) for years ending 30 June 1992 and 30 June 1993. Melbourne, Office of the Ombudsman, Victoria.

The Ombudsman (2001). 2000/2001 Annual Report: Twenty-eighth Report of The Ombudsman. Melbourne, Office of the Ombudsman, Victoria.

The Ombudsman (2003). Annual Report. Melbourne, Office of the Ombudsman, Victoria.

Victoria Police (2013). Annual Report 2012–2013. Melbourne, Victoria Police.

Notes

[1] See Davids (2005: 105) for an explanation of the methodology for counting allegations or instances of conflict of interest. Space limitations mean that only brief case information can be provided in this chapter (see Davids 2005 for detailed case description and analyses; and a sumamarised analysis in Davids 2008: Ch 6).

[2] These PSUs "proactively cultivate and analyse information or 'intelligence' on unethical police activity from a range of sources (e.g. police colleagues, informants, the public, other agencies, audits, and surveillance) and mount formal investigations into suspects identified" (Miller 2003: i).

[3] The Victorian Office of Police Integrity was absorbed into a new Independent Broad-based Anti-corruption Commission established in 2012.

[4] For example, *Police Regulation Act 1979* (Victoria) s127; *Crimes (Controlled Operations) Act 2004* (Victoria), s36; *Crimes (Assumed Identities) Act 2004* (Victoria), s30).

[5] For example, *Criminal Law Consolidation Act 1935* (South Australia), ss251, 238; *Commonwealth Criminal Code* (Australia), s142.2).

[6] There have been several recent Victorian cases of police officers being prosecuted for offences involving disclosure of confidential information – included in the discussion in Sections 4 and 5.

[7] Cases 268 & 372.

[8] In this case, the police officers also used police vehicles, radios, and mobile telephones in the private surveillance work (see Davids 2008).

[9] Silvester J and R Baker (2003). "Police will face sack for improper use of files." *The Age*, October 24: 3.

[10] ABC (2005). "Relatives confront police about emailed photos". *ABC Online* 9 December (http://www.abc.net.au/news/2005-12-09/relatives-confront-police-about-emailed-photos/758420).

[11] During 1991–1993, 78 complaints relating to disclosure of information were investigated, and 25 of these (32 per cent) were found to be substantiated. Davids' study covered 1988–1998; 39 cases files included an allegation of disclosure of police information to outside parties; 38.5 per cent of these matters were found to be substantiated.

[12] For the purposes of the present analysis, Davids' category of "trading in police information for financial or commercial benefit" has been combined with "leaks in the context of criminal investigations, legal, or associated matters"; "inadvertent leaks" have been omitted.

[13] *DPP v Zierk* [2008] VSC 184.

[14] *DPP v Marks* [2005] VSCA 277.

[15] *R v Bunning* [2007] VSCA.

[16] McKenzie N and Baker R (2013) "Bikies infiltrate police" and "Friends in all the wrong places". *The Age* (Melbourne), 27 March, pp. 1–3, and 18–19.

[17] *DPP V Artz* [2013] VCC 56.

[18] *D'Alo v Nolan* [2006] VSC 362.