

“Police corruption and information security management”

ABSTRACT

The main focus of legislative measures and controls imposed on private and public organisations is to provide open and transparent environment where confidential information and customer privacy are protected. Law enforcement agencies such as police are expected to enforce the law where it is not complied with but they themselves find it challenging to properly manage vast quantities of confidential information.

First, the rationale of collecting police information together with the common sources of information useful to police are described. An example of policies and guidelines to guide the management of police information is given, followed by the identification of information security breaches as specific examples of police corruption, sometimes leading to tragic consequences. Different types of police corruption involving mishandling of police information are identified together with factors that increase the likelihood of corruption and breaches of confidentiality. Finally, the article outlines possible mitigation approaches to reduce the risk of information leaks and corrupt conduct among police officers

INTRODUCTION.

Much is being said in the treatment of ethics about appropriate governance, transparency and accountability for private organisations. After a string of highly-visible business scandals such as Enron, WorldCom and, more recently, billion-dollar financial frauds committed by Bernard Madoff and Allen Stanford it is highly surprising that there is not much public confidence in the business ethics within the private enterprise. Legislative measures, introduced immediately after Enron and Worldcom failures, include the legislation such as the Sarbanes-Oxley Act 2002 in the United States and similar legislation in Canada, Australia and UK introduced to deal with such issues.

Civil servants in most of countries would be very quick to point out that public entities were under public scrutiny for a long time and, consequently, ethical standards maintained in the civil service are higher compared to the private sector. This view could be debatable given that ethical scandals arise within civil service as well. In any case, both the private and the public sectors are regulated by the same legislation that sets out information security management standards and practices and stipulates obligations that need to be met when dealing with collection, processing and use of data, eg. collected from private individuals or citizens. There are usually severe penalties imposed for non-compliance, enforced by the law enforcement agencies. So, by this very virtue, we should expect that law enforcement agencies, as *primus inter pares*¹, exhibit leadership and demonstrate the best practice when it comes to maintaining high ethical standards in the information management and keeping the data they collect safe and secure.

Unfortunately, the picture that emerges is rather different: law enforcement agencies such as police do not demonstrate such high ethical standards in managing information as we would have

¹ First among equals

expected, despite a threat of criminal prosecution or dismissal. How does this form of police corruption manifest itself, what are the factors contributing to it and what are the remedies?

POLICE INFORMATION

By the very nature of their job police are in a very privileged position. As the designated guardians of public law and order, police have an immense capacity and authority to collect and gather information to support their activities. Most of us have it ingrained in our minds since our childhood that a policeperson represents the authority, law and order and, as such, should be respected and obeyed, perhaps even feared a little. This “social programming” remains with us for the rest of our lives and affects our interaction with police, particularly when providing information. I have experienced myself situations where I would be told first that it is against the company policy to provide mobile numbers of staff to callers and then, contrary to that very policy, I would be given the number when I clarified that I work for the police. A small amount of social engineering, like telling the receptionist “Don’t worry, he/she is not in trouble” with a little chuckle, did not go astray.

The above anecdotal description aside, police jurisdictions worldwide collect and maintain huge amounts of information. Whilst a general perception may be that the information collected would be about hardened criminals and more serious crime in general, police collects information on a broader scale, for many reasons and from many sources.

Using UK as an example, the Association of Chief Police Officers (ACPO) in the guidelines on management of police information (ACPO, 2006) identified the rationale for collecting police information as ranging from protection of law and property and preservation of order to any duty or responsibility arising from common or statute law. The latter would be applicable to any situation covered by the legislation such a traffic rules and regulations. The same guidelines also indicated that “all police activities will generate police information”. Examples of activities provided include not only activities such as arrests, patrols and stop checks but also traffic incidents, public inquiries, closed circuit camera operation and automated number plate recognition activities. In a similar vein, the UK Police National Computer records contain personal records for anyone currently disqualified from driving, missing or who has otherwise come to notice. The latter practice provides a wide range of personal information as it is customary to capture information about witnesses, neighbours and other persons who may be interviewed about a crime incident or similar.

With the introduction of computerised records, police build databases with large volume of records. The scope of data contained in such databases is quite wide, with police officers having access to not only names, dates of birth, gender and ethnicity but also to phone numbers, driving licence numbers and car registration numbers (Kennedy, 2004). Modern information systems also provide police with the ability of reverse look-up phone numbers (Reverse White Pages) and access other information not available to general public. Additionally, police information systems would also contain police-specific information such as confidential intelligence or surveillance reports.

The question of what is confidential information not available to a general public is often difficult to answer. It is easy to grasp that an intelligence or surveillance report would be confidential and should not be disclosed. On the other hand, what constitutes confidential personal information? As examples, person’s surname, address or a phone number by themselves do not have confidential

characteristics – any of the above data items would be available in a telephone directory. Peltier proposes one definition of confidential information: information that, when disclosed, would violate the privacy of individuals, diminish any competitive advantage over competition or damage the entity (Peltier, 2004). On this basis, information such as the person's name, date of birth, address and phone number combined together would constitute confidential information that should not be disclosed to third parties without authorisation.

With such wide range of information available to police officers guidelines and other measures are required to ensure that the access to information is not abused. Legislative measures such as the Western Australia's Criminal Code Section 440A and Public Sector Management Act 1994 are two examples of legislation setting criminal prosecution or dismissal as some of the possible penalties for unauthorised computer access and breach of confidentiality (Kennedy, 2004). Other police jurisdictions publish guidelines clearly advocating use of practices to ensure that the information is used for "...police purposes and in compliance with the law" and that there are procedures and measures to minimise the risk of "unauthorised or accidental access to, amendment or loss of police information" (ACPO, 2006). At a national level, common security policies outline controls to be applied, from further policies and procedures to technical and personnel security, mitigating a wide range of risks from terrorist and criminal groups to natural disasters (ACPO/ACPOS, 2006). More detailed data protection guidelines provide specific examples of unauthorised or unlawful use of data, eg. selling of burglary victims' addresses to double-glazing firms or using police records information in a personal dispute (ACPO DPPG, 2006).

MISUSE OF POLICE INFORMATION

With so many administrative instructions and guidelines as well as legislation intended to protect lawful data use, why is the misuse of information so widespread within police? This is not a rhetorical question: a report on the police corruption in England and Wales, published by the Home Office in 2003, clearly identified information compromise and breaches of confidentiality by police as the most common occurrence of corruption (Miller, 2003). The same report puts forward a sort of taxonomy for information security breaches, classifying these into 'domestic' use of information where police officers unlawfully access police data to source information for personal use such as vehicle information or checks on friends and new acquaintances, 'low-level' leaks on behalf of friends running businesses, media leaks and deliberate leaks to criminals.

Unfortunately, these trends are not unique to a specific police jurisdiction and such examples of corruption through unauthorised and unlawful information dissemination are common to all police jurisdictions. A report on the corruption and serious misconduct in the Victorian Police, published in 2007, provides a detailed example of misuse of police information with a Detective Senior Constable engaged in conducting 361 unlawful car checks over a year, collaborating with an insurance investigator. The same report talks of a case of a police sergeant providing the same insurance investigator with the details of a stolen car and colluding with him to submit a fraudulent application for the insurance reward (OPI, 2007).

Breaches in maintaining confidentiality of information and ethical handling of information form a common trend in police corruption. A study by two South African police researchers, Sayed and Bruce, published in 1998 identifies seven major forms of police corruption and twenty two types of

corrupt police activities ranging from a misconduct of favouritism towards family and friends to criminal activities such as robbery. The study considers information passing and tipping-off as a form of paid protection, a form of bribery and related activities (Sayed and Bruce, 1998).

Corrupt police behaviour applied to information management frequently shows a trend of progressing from transgressing in administrative matters to performing criminal activities or activities bordering on criminal and having very serious repercussions. Transparency International report on confronting corruption (Pope 2000) recalls studies by the police inspectorate showing that some police units in UK falsified crime statistics to show improved clearance rates to embellish their performance. Such behaviour is consistent with the description of deceptive practices and falsifying documents or evidence to enhance one's own performance provided by Sayed and Bruce in their study (Sayed and Bruce, 1998). A more celebrated case in the same category is the case of the Queensland's Police Commissioner, Sir Terrence Lewis, who took a bribe to provide a completely falsified report on poker machines to the Queensland Government (Pope, 2000).

The unfortunate side of breaches in the security of police information is that it may ultimately lead to a loss of life. One such case is documented in the final report of the Kennedy Royal Commission into WA Police corrupt activities (Kennedy, 2004). The Commission documented a case of Andrew Petrelis, a small drug dealer turned police informer and ultimately a forthcoming witness in a major drug case. Petrelis was placed under the Witness Protection Program and relocated to Queensland under a new identity. According to system log and alert information, a number of WA police officers accessed police computer records associated with Petrelis's new identity. Out of these, two officers long suspected of criminal association could not provide a valid reason for doing so, with one officer claiming that he accessed the record accidentally, whilst practicing the use of the system and choosing Petrelis's alias of "Andrew Parker" as he was a fan of Elvis Presley². Telephone intercepts from the surveillance of the officer record his contacts with a criminal identity shortly after, unfortunately not mentioning explicitly the nature of his findings from the police database. Not long after Andrew Petrelis was found dead, apparently from a drug overdose. One of the issues that the Kennedy Royal Commission raised was the lack of any resulting criminal prosecution against the suspected officers despite their well documented association with a known criminal and previous internal investigations.

Andrew Petrelis died in 1995 and other police jurisdictions should have learnt from this unfortunate experience. Unfortunately, this was not the case. Even as late as 2004, a police informer, Terry Hodson, and his wife were shot in their own home after a confidential police dossier on Hodson was leaked to criminal elements in late 2003. In 2009 a former police officer stood trial accused of their murder. Referring to this incident, The Melbourne Age reported in December 2008 that confidential surveillance reports were leaked to several Victorian police surveillance targets, causing some of them to flee overseas and compromising several lengthy state and federal police investigations (McKenzie and Baker, 2008). The history of corruption in the Victorian police even involves a break into the Drug Squad offices in 1996 with the theft of confidential files and records and suspected involvement of police.

² Elvis Presley manager was Col. Tom Parker

With such widespread corruption involving police information, what are the contributing factors that cause so many police officers to commit misconduct or to carry out illegal activities?

Psychological predisposition is definitively one factor. Police, by the virtue of the job and interaction with the society, attracts certain types of personalities who want to join not to “protect and serve” but to gain. Such individuals see police as the means to get money and influence. The importance of getting people with right ethical approach and predisposition figures very strongly in recommendations from inquiries into police corruption such as the Fitzgerald Inquiry, Wood Commission and Kennedy Commission (Kennedy, 2004). Studies show that 20% of 1500 integrity tests administered to New York police officers result in a test failure and dismissal of the officer (Smith, 2004). There is also a very strong link between deviation from fulfilling job requirements and expectations and a potential for future corruption (Boes and Chandler, 1997).

There is much of a debate, particularly in the developing countries, that a primary driver for police corruption is economic, where underpaid police officers look for ways to supplement their income and support their families. Although its is a fact that police officers in many countries are underpaid and overworked, a working paper from the Norwegian Institute of International Affairs suggests caution in adopting readily this view, proposing instead that it is sometimes unreasonable income expectation than being underpaid that is the driver (Andvig and Fjeldstad, 2008). This would make it a greed-driven rather than economic-driven corruption. The cash component of the officer’s salary is often just one form of a benefit: in many cases police officers also receive full board and lodging, free education and healthcare for their families and, with middle to senior officers, fully maintained cars.

Another factor contributing towards the spread of police corruption is the occupational opportunity. As indicated earlier, by the very nature of their job police officers have access to a lot of confidential or sensitive information which is of value to third parties or criminal elements. Another aspect arising from the occupational opportunity is working in close contact with criminal elements and the ability to observe rewards that criminal or illegal activities can bring (Miller, 2003).

More specific to police information and associated corruption is the lack of adequate standards and controls in controlling access to police information, wide availability of information without the need to know and lack of mechanisms to prevent unauthorised use of other officers’ system accounts. In such environment there are many opportunities to access information without any fear of possible consequences.

Last but not least, lack of adequate promulgation of ethical culture through leadership, management supervision and awareness raising is an overarching factor. Lack of ethical culture in the Queensland Police under Sir Terence Lewis is one example where the rot from the top spread throughout the organisation. Other, less extreme examples involve lack of action, ineffective internal investigations and inappropriate disciplinary measures as documented by a number of Royal Commissions into police corruption (Kennedy, 2004).

MEASURES TO COMBAT CORRUPTION IN THE USE OF POLICE INFORMATION

It is no coincidence therefore that information security forms one of the key elements of anti-corruption strategy applied to clean out the police (Miller, 2003). In addition to appropriate information security policies and procedures, appropriate processes such as applications for system access and non-disclosure or confidentiality statements should be applied. Policies and procedures should be backed by commensurate technical controls.

Interpol, the International Criminal Police Organisation (ICPO), published a list of IT security and crime prevention checklist (ICPO, 2009) listing 17 categories of information security issues that need to be considered. The checklist starts with the management and staff responsibilities, looks at information classification, software, hardware and documentation issues and finishes with incident handling and contingency planning. More notable suggestions are the separation of production and development system environments, use of “two-person” rule for granting access and system privileges, backup and archive handling, use of two-factor authentication and multiple log types.

Reports from investigations into police corruption proposed additional measures such as preventative auditing, where a system trap is sprung when the user accesses a particular record, profiling of system use, where system transaction logs are used to identify excessive and uncharacteristic use, use of role-based security to support need-to-know information access, automatic system lockout, terminating computer session after a set period of inactivity (eg. 5 minutes) and recording of the reason for information access (Kennedy, 2004). Some Australian police jurisdictions took these recommendations even further, eg. logging individual keystrokes so that the user transaction can be replayed later if need be.

Information security management standards make a point that information security management is not a single process but a continuous cycle. Transparency International highlights this point, stressing the need for continuous monitoring and auditing to ensure that appropriate standards are maintained on an ongoing basis. The same recommendation also proposes the use of integrity testing as the means of identification of corrupt officers, a suggestion echoed by the Interpol checklist information and other publications.

CONCLUSION

Police jurisdictions have a lot of power vested in them to ensure that they can access information necessary to maintain public law and order, protect property and prevent crime. With this power comes the public trust that the police will use such information for the lawful, policing purposes and that police will do their utmost to protect the confidentiality of information entrusted into the police’s care.

In the words of John Acton, “Power tends to corrupt, and absolute power corrupts absolutely”. Without adequate checks and balances, the power vested in police becomes absolute and the potential for corruption increases significantly, with adverse impact on the police organization and on thousands of honest police officers protecting and serving their communities. It should be a concern that, despite many inquiries and commissions, the issue of police corruption in the use of information is still so prevalent. Perhaps the closely knit police community and closed police culture are also to blame.

REFERENCES

Association of Chief Police Officers (APCO), 2006. *Guidance on the management of police information*, National Centre for Policing Excellence

Kennedy, G A, 2004. *Royal Commission into whether there has been corrupt or criminal conduct by any Western Australian Police Officer: Final Report*, ROYAL COMMISSION INTO WHETHER THERE HAS BEEN CORRUPT OR CRIMINAL CONDUCT BY ANY WESTERN AUSTRALIAN POLICE OFFICER

Peltier, T R, 2004. *Information Security Policies and Procedures: A Practitioner's Reference*, 2nd Edition, CRC Press

Association of Chief Police Officers of England, Wales & Northern Ireland & Association of Chief Police Officers in Scotland (ACPO/ACPOS), 2006. *Information Systems Community Security Policy*, PITO

ACPO Data Protection Portfolio Group (ACPO DPPG), 2006. *Data Protection Manual of Guidance Part 1: Standards*, Version 1.0, ACPO DPPG

Miller, J, 2003. *Police corruption in England and Wales: an assessment of current evidence*, Home Office

Office of Police Integrity (OPI), 2007. *Past Patterns – Future Directions: Victoria Police and the problem of corruption and serious misconduct*, Victorian Government Printer

Smith, C, 2004, *Pivot Report Calls for Police Integrity Tests*. Vancouver Free Press, Available at www.straight.com [Accessed on 8/02/2009]

Sayed, T and Bruce, D, 1998. *Inside and Outside the Boundaries of Police Corruption*, African Security Review, vol.7 no. 2

Pope, J, 2000. *Confronting Corruption: the elements of a national integrity system*, Transparency International

McKenzie, N and Baker, R, 2008. Secret police files leaked to alleged crime bosses, *The Age*, 2 December 2008

Boes, J and Chandler, C, 1997. Police Integrity: use of personality measures to identify corruption-prone officers. *PERSEREC*, September 1997

Andvig, J.C and Fjeldstad, O, 2008. *Crime, Poverty and Police Corruption in Non-Rich Countries*, Norwegian Institute of International Affairs (NUPI)

International Criminal Police Organisation (ICPO), 2009. *Information security and crime prevention*, Available at: <http://www.interpol.int/Public/TechnologyCrime/CrimePrev/default.asp> [Accessed on 9/02/2009]