Police corruption and computer misuse: an analysis of the contributing factors

Nathan G Briant

Professional Doctorate in Policing, Security and Community Safety.

2013

London Metropolitan University

Acknowledgements

In presenting this thesis the author would like to thank all interviewees who took part in the research with particular thanks to Mr Bernard Lawson, QPM from the Association of Chief Police Officers (ACPO) and Mr Steve Evans from the National Police Federation.

Police corruption and computer misuse: an analysis of the contributing factors.

Contents

Index of Tables and figures

Glossary of Terms

ACPO	***The Association of Chief Police Officers*** *The umbrella organisation representing senior police officers within England and Wales of Assistant Chief Countable and upwards.*
CERT	***Computer Emergency Response Team*** *Government agency monitoring threat from computer misuse across the UK. (Most Western countries operate a similar system)*
CID	***Criminal Investigation Department*** *The detective branch of a police force*
CPS	***The Crown Prosecution Service*** *Prosecuting authority for criminal offences within England and Wales*
HMIC	***Her Majesty's Inspector of Constabulary***
IPCC	***Independent Police Complaints Commission***
Met	***Metropolitan Police*** *(Colloquial term)*
OCG	***Organised Crime Group*** *A group undertaking cross boarder organised crime activity*
PNC	***Police National Computer*** *The main computer system used by forces for the storage of information on vehicles and people.*
PSD	***Professional Standards Department*** *The department within a force responsible for complaints, discipline and counter corruption.*
SERCS	***South East Regional Crime Squad*** *One of the Regional Crime Squads set up in the 1980s to deal with serious cross boarder crime*
SOCA	***Serious Organised Crime Agency*** *Cross Boarder agency dealing with serious crime nationally and internationally.*

Police corruption and computer misuse: an analysis of the contributing factors.

Abstract

Recent high profile media coverage of a number of police corruption cases has understandably caused an increase in public concern at the possibility of widespread malpractice within forces. These concerns have been further heightened by the instigation of a number of public and judicial reviews of police relationships with the media, as well as the resignation of the Metropolitan Police Commissioner and other senior figures.

The causes and motivations of police corruption have been the subject of a small number of academic studies, generally focussing on types and typologies of the act itself and offenders. In this contribution the author has examined a number of factors which impact on the likelihood of police officers undertaking deviant practice in the small but focussed area of computer misuse.

In conducting the research four sample groups were identified; two from the organisational side of policing; National leads in the corruption arena and local heads of Counter Corruption Units, and two from the employee side; The Police Federation and officers who themselves had misused police computer systems. The author conducted a total of thirty one interviews split between these four groups, examining factors such as 'knowledge of wrongdoing', 'perception and fear of being caught', 'awareness of sanctions', 'ease' and 'stigma'.

Whilst demonstrating the misuse of police data to assist criminal gangs or disrupt police investigations is rare, the results of the research show a widespread misuse of police computer systems for personal reasons, against a backdrop of a lack of awareness of the restrictions on legitimate use, and conflicting views on the perception of the likelihood of detection.

In conclusion the thesis sets out two original arguments; first in relation to academic theory by amending two existing typologies, that of Roebuck and Barker (1973)(as amended by Punch 1985), and Sherman (1974), to allow for advances in technology and new forms of deviant behaviour. Secondly in the area of practical application to policing, the thesis outlines a starting point 'test' to determine whether computer use constitutes a 'Genuine Policing Purpose'. This test is central in determining whether computer use is legitimate or not. Additionally the author outlines his other 'impacting factors' which, with work by enforcement teams, is likely to reduce incidences of computer misuse in the future.

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 1
Introduction

Background and Rationale

"Policing and corruption go hand in hand. That the two are inextricably linked is a grave matter because the police organisation is the prime agency of the state for law enforcement and social control" (*Reiner 2000 in Punch 2009, p1*). This quotation, provided by perhaps one of the most ardent contemporary social researchers into policing appears to suggest that police corruption is unavoidable and that it forms part of the very fabric of policing organisations. Whilst controversial, there is some supporting evidence for this suggestion, with deviant behaviour being reported from the inception of the 'new police' (*Reiner 2010*), through to the very modern day.[1]

As well as highlighting the 'inextricable link' between policing and corruption, Reiner also begins to outline why this presents such a grave concern, although he stops short of fully explaining the potential implications. These can arguably be traced back to the origins of contract theory itself and ideas first articulated in the 1600s by Thomas Hobbes in his famous 'Leviathan'. Here Hobbes argued that prior to any law and order a state of nature existed which saw individuals as "*solitary, poor, nasty, brutish and*

[1] Between 1831 and 1833 a Police Constable Popay having been asked to infiltrate the National Political Union, is alleged to have gone too far in this work and actually started encouraging the establishment of an arms depot. He was dismissed from the force for 'highly reprehensible' conduct (Morton, J. 1993). More recently the News International scandal of 2011 saw allegations against the Metropolitan Police Commissioner, and his subsequent resignation, along with at least one of his assistants.

short" (Hobbes in Gaskin, 1996 p84). As individuals sought security and social connection they came together to concede some of their own rights in exchange for protection from others. Hobbes called this agreement the 'social contract' in which an individual traded some of their own freedoms with 'the state' in order to receive the state's protection from others. Hence the state was central to the maintenance of law and order in preventing injury to individuals in exchange for those same individuals not injuring others. Moving further forward some 200 years the ideas of Hobbes (although reviewed and added to by a number of social theorists), meet the ideas of Max Weber in his lecture 'politics as a vocation'[2] Here Weber outlines his views that in pursuance of law and order the state holds a monopoly on the legitimate use of force. The instruments for such use, Weber asserts, are the police and the military. Within liberal democracies, and outside emergency provisions, the sole instrument is arguably the police. The two ideas of Hobbes and Weber when taken together, demonstrate the importance of confidence in policing in order to maintain the social contract and therefore law and order.

The nature of this confidence is however questioned by Jerome Skolnick, in his 1966 work, *'Justice Without Trial'*. In this book Skolnick reviews the formation of the 'new police' in 1829 and asks the purpose of the police. *"Are the police to be principally an agency of social control with their chief value the efficient enforcement of prohibitive norms of substantive criminal law? Or are the police to be an institution falling under the hegemony of the legal system with a basic commitment to the rule of law, even if this obligation may result in a reduction of social order?"* (Skolnick, 1966, p1). Skolnick

[2] Subsequently published, various editions, and available on line http://anthropos-lab.net/wp/wp-content/uploads/2011/12/Weber-Politics-as-a-Vocation.pdf (accessed 2/1/13)

explains that whilst Sir Robert Peel based his arguments for the formation of the new police on a need for public order, he gained support from parliament on the basis of accountability and an assertion that he was "*confident they would be able to dispense with the necessity of a military force in London for the preservation of the tranquility of the Metropolis*" (Peel in Skolnick 1966, p2). Thus the question posed by Skolnick is whether public confidence in the police is best served by low crime rates and public order or a dogged adherence to the rule of law, even if this means higher crime and greater disorder. This tension between crime control and due process appears to focus on malpractice with a view to a greater good such as noble cause corruption[3]. Any type of police malpractice however, by the fact that it demonstrates a willingness to break the rules, has the potential to impact on the very nature of the social contract, as such an agreement can only be viable if individuals have confidence in the state's ability and willingness to uphold its end of the bargain.

Public interest in police mal-practice appears to wax and wane in harmony with high profile cases and media exposés, and whilst there does not appear to be a shortage of examples of alleged police deviance in the media, associated academic work is limited to a small number of social researchers and generally focused upon large scale corruption involving groups of employees. (*Morton 1983, Punch 2009, Reiner 2010*). Likewise existing research appears generic in its approach to deviant behaviour, considering a number of activities under the same cover-all term; 'corruption'.

Corruption however is a term used liberally, to describe an inordinate number of different types of deviant activity (*Barker and Roebuck 1973*). These activities range

[3] Post

from the receiving of free drinks and meals in local cafes, to extortion of money from criminal enterprises in exchange for the protection of their illegal activities and the undermining of criminal investigations. Whilst the former of these may seem relatively trivial and the latter very serious, between these two extremes sits a series of activities which either serve to provide a corrupt officer with some personal gain or reward[4] at the expense of their duty, or pervert the due process of law in some misguided belief that crime control ranks higher than the law itself. (Skolnick, 1966). Whilst the objectives of police corruption (personal gain or noble cause) may have remained reasonably consistent throughout the last 200 years, the corrupt acts themselves appear to have moved with the times. Whereas previously corrupt officers may have sought to 'lose' evidence to disrupt criminal investigations, todays corrupt officer has a wealth of information from police computer databases which, if disclosed to criminals, can derail police investigations just as effectively if not more so. Additionally the rise of the computer age has presented officers with a tempting source of information on society, with virtually all police records being loaded onto electronic databases, searchable from every desk. This temptation presents a danger to policing in that the public generally are concerned at the vast amount of information collected about them. The only mitigating factor the police can put forward to justify such databases is the conceptual 'agreement' that they are only used for 'Genuine Policing Purposes', such as the protection of life and the prevention and detection of crime. Where any corrupt practice breaches that 'agreement' the legitimacy of police information storage is called into question.

[4] Including personal gratification.

This idea has the potential to replicate Hobbes contract theory on a smaller scale, in that if the police (the state) do not uphold their end of the bargain, then the contract is invalid. As the effectiveness of policing nationally relies increasingly upon robust computer records and databases, the loss in confidence of these has a real potential to impact on the confidence in policing as a whole. Examples of modern day corruption therefore include not only traditional activities such as taking bribes, concealing evidence, and stealing from insecure premises, but also the modern day practices of unauthorised computer searches either to pass information to third parties or to satisfy one's own personal desire for knowledge not needed in the course of one's work[5]. What is clear is that as policing has developed, and society (but in particular technology) has progressed there are an increasing number of modern day methods of stepping outside the organisation's norms and undertaking what may be viewed as a corrupt practice.

In this work the author seeks to close a gap in the existing academic research in examining the particular area of computer misuse within the police service and in particular the factors contributing to the individual decision to undertake this corrupt activity. As discussed this may of course be in support of further aims, such as the frustration of police operations and protection of illegal activities or indeed be merely to satisfy a personal desire for knowledge with no further motivation.

The research examines not the motivation for computer misuse, but asks what are the contributing factors impacting on the decision to undertake such activity. In particular it examines how easy such practice is, the level of awareness as to limits of authorised

[5] Whilst this practice carries a reduced risk of impacting on public confidence as by its nature it is not disclosed to third parties it remains both a criminal offence (see post) and a breach of the standards of professional behaviour.

use, the likelihood of detection, the perception of likely sanction and any stigma attached to the activity. Specifically the research excludes individuals who may have joined a police organisation with the pre-conceived aim of corruption.[6]

As a serving police officer leading a three force department focused at counter corruption and the national lead on the ACPO 'Anti-Corruption Advisory Group' (ACAG) for computer misuse use, the author has experienced first-hand the increasing number of incidences of this type of deviance. He has therefore sought in this work not only to contribute to academic theory, but also provide practical tools for professional application in the reduction of unauthorised practice.

Structure and direction

By way of introduction the author seeks to set out the history of police corruption within the UK. He traces a number of high profile cases from the inception of the new police through to modern day, and examines the impact these may have had on the public perception of policing. The research then moves on to consider high profile campaigns that have set about tackling police corruption and how the organisation has tried to develop a culture which not only shuns, but actively attempts to uncover mal-practice.

In the second and third chapters, the literature review, the author separates the two issues of police corruption and computer misuse, examining existing research into both issues. In the area of police corruption the research reviews three distinct contributions to definitions, typologies, and causes; these come from academic works,

[6] This is commonly referred to as infiltration, where criminal gangs attempt to have one of their members recruited into the police in order to provide information on, or disrupt police activity. (ACPO,2012)

internal reviews and finally journalistic material. Having considered a number of differing definitions and highlighting the fact that there exists no single agreed upon definition either within academia or law enforcement circles, the author outlines a modified version of Maurice Punch's 1985 definition of police corruption for the purpose of this research; *"receipt or promise of advantage, reward or gratification (personal group or organisational) for doing something that an official is under a duty to do anyway, that he is under a duty not to do, or for exercising a legitimate discretion for improper reasons, and for employing illegal means to achieve approved goals" (Adapted from Punch 1985. p14).* Of the typologies reviewed the research pays particular attention to the 1973 work of Barker and Roebuck detailing eight categories of police corruption; 'corruption of authority, kickbacks, theft, shakedowns, protection of illegal activities, undermining criminal investigations, criminal activities and internal pay-offs' (Barker & Roebuck, 1973). The author also makes specific mention of the amendments to this typology by Punch in 1985 with a view to modernising it to incorporate newly emerging corrupt practices involving drug gangs of the 1980s. The principle of adaptation of Barker and Roebucks work is further explored later in the research when the author suggests further amendments to incorporate the ever changing nature of corruption. In considering the causes of police corruption the author examines ideas of initial corrupt practice stemming from Stoddard's 1968 view on the social norm of corruption as well as theories of recidivism from Sherman's 1985 'moral career of a police officer', through to Kleinig's 1996 'slippery slope argument'. The work also examines in detail the ideas of Sherman's 1974 work on constant and variable features and how their presence or absence supports or opposes corruption. Sherman's features hold particular relevance to the research

conclusions as they make up a contribution to the author's 'perfect storm'[7] or environment for computer misuse corruption.

In the second part of the literary review the author focuses on computer misuse generically, examining contributions from academia and national legislation. Again the author opens up three distinct paths for review; those of definition, typologies and causes. In defining computer misuse, the research explores the ideas of David Wall and Martin Wasik and their definitions of cybercrime, before arriving at the view that for the purpose of this work the 'black letter law' of the Computer Misuse Act 1990 amply defines the issue. In considering types of computer misuse the author pays particular attention to the 2007 work of David Wall and his three generations of crime. In particular the idea of motivation is raised which bears significant relevance to the research conclusions in the final chapter where practical solutions to prevent misuse are outlined. In considering the causes of computer misuse the research examines the ideas of Stefan Fafinski in his comparisons between the rise of internet usage over the last 20 years and the rise in reports of computer misuse incidents, before advancing the more persuasive social commentary of David Wall as it relates to the rise of the 'information generation' and their expectation of the right to computer usage and demand for instantaneous knowledge.

In chapter four the author outlines the research methods used in this investigation, examining the most effective of both the hard and soft paradigms of quantitative and qualitative methods. The research parameters are defined as well as four research groups; national leads in counter corruption, senior officers working within counter

[7] Chapter 7, post.

corruption units, Police Federation representatives, and officers who themselves had been disciplined or prosecuted for computer misuse offences. The author then moves to explain the nature of the interviews conducted and how, during these interviews, it became necessary to amend questions for the last three groups following the emergence of a 'seriousness hierarchy' from the national lead interviews. The author also highlights the difficulty in contacting and interviewing disciplined officers, and the importance of the support of the Police Federation in this regard.

In introducing chapter five the author provides a commentary on each of the research groups as well as the current political landscape as it relates to each of them. He moves on to explain the research findings by group, identifying seven impacting factors contributing to computer misuse; awareness of prohibition, perceived fear of detection, perception of sanction, perceived likelihood of detection, ease, stigma and perception of seriousness. Additionally the research demonstrates the widespread nature of police computer misuse as well as a mismatch between the perceptions of the four research groups as to the likelihood of detection.

In the sixth chapter the author discusses the findings, considering each of the seven impacting factors in turn against the views of interview subjects, and highlighting consistencies and discrepancies in their perceptions and beliefs. He then moves on to consider the interview subjects' views against the backdrop of the literature examined in the second and third chapters, again highlighting where these support each other or conflict. In summary the author revisits each of the impacting factors placing them in an order of hierarchy according to their impact on the decision to undertake computer

misuse. Finally he examines the limitations and possible alternative explanations for results achieved.

The thesis conclusion in chapter seven outlines the argument for the 'perfect storm' which creates an environment for computer misuse within the police service. This 'storm' consists of the social relationship individuals have with computers in modern society outlined by David Wall, the constant and variable features of police work lending themselves to corruption as demonstrated by Lawrence Sherman and finally the contributing factors outlined in this research. The research moves on to conclude that the 1973 typology of Roebuck and Barker, amended in 1985 by Maurice Punch, should be further amended to make provision for a new category of 'browsing', to incorporate the unauthorised searching and reviewing of police computer systems. Finally the author draws on the findings from interview subjects that they generally suffered a lack of awareness as to what was and was not permitted use of police systems, as well as the ideas of motivation advanced by David Wall, to devise a test to determine whether computer use is legitimate or not. The purpose of this test being to greater inform officers of the limitations of use, as well as providing a framework for counter corruption units to base investigations. In closing the author outlines limitations to this research as well as possible areas for future study.

'Hand in Hand' – A Retrospective of Policing and Corruption

Following the founding of the new police in 1829, the first two Commissioners, Rowan and Mayne, faced a number of low level disciplinary breaches and criminal offences by their men. These ranged from drunkenness on duty to petty theft, and reports suggest that within the first ten years of the force, some 6000 men had resigned and a

further 5200 had been dismissed (*Morton, 1983*).[8] Whilst these infringements did nothing to assist the public acceptance of the new police, an allegation of rape against a police Inspector led to his and his Superintendent's dismissal, despite the former's acquittal at court. This appears to have prompted early praise for the force in Grant's 'Sketches in London', *"The integrity and trustworthiness of the New Police considered as a body, are above all praise. It is surprising in how few instances charges of corruption have been preferred, far less proved, against any of their number... ... There seems to be a rivalry as to who shall be the most honest..."* (*Grant, J 1838 p392; Morton 1983*). Far worse was of course yet to come and the following years saw a number of allegations of police misconduct ranging from the planting of evidence, perjury, larceny, and receiving stolen goods. These however appear isolated to individual officers undertaking unilateral action to their own ends. 1877 however saw what has become noted as the first of the great police corruption scandals involving a number of senior officers working together with a criminal group.

The background to what became known as the 'Turf Trials' relates to two fraudsters, William Kurr and Harry Benson who operated a series of racing scams and swindles. The initial spark to this scandal appears to be the then Sergeant Meiklejohn who had been taking bribes from Kurr to provide him with information on police enquires into betting frauds, but other officers were soon recruited as a result of either promises of substantial sums of money, or for the waiving of their own or family member's gambling debts. Following an extravagant fraud attempt against the Countess of Goncourt in Paris, both Kurr and Benson were arrested, tried and imprisoned. Hoping

[8] In the first two years, of the original 4000 officers, it is reported that some 1989 were dismissed, mainly for drunkenness. (Morton 1983, p22)

for early release both provided details of the police officers who had assisted them in their illegal activities. This information led to the arrest and subsequent imprisonment of four of Scotland Yard's detectives.[9] Upon sentencing, Judge Baron Pollock affirmed a point which holds true today in the guidance issued by the Crown Prosecution Service[10] *"The spirit and rule of law in England have been and I trust always will be, to make a wide distinction between offences committed under either sudden impulse or under pressure of want or poverty and offences committed by persons placed in a position of trust"*.(Pollock: Morton, 1983. p46)

As a result of the case a review was carried out of the detective branch with a view to taking a tighter control of this department. Whilst this led to the professionalisation of detective work, it also rendered the Criminal Investigation Department (CID), a near autonomous empire within the Metropolitan Police (*Allason 1983; Punch 2009, p127*).

Further corruption revelations occurred in the 1920s when a Sergeant Goddard working within the CID was the subject of an anonymous note to the then Commissioner. It suggested that the officer was taking bribes from several West End nightclub owners. Following an investigation significant sums of money were recovered from Goddard's personal bank accounts and he was ultimately convicted of taking bribes and imprisoned for 18 months. Whilst this case does not display the level of organised corruption associated with the Turf Trials, it did demonstrate a far wider problem than had been previously recognised, that of the total endemic nature of police bribery. (*Morton 1983, Punch 2009*).

[9] Whilst this information is obtained from Morton's 1983 Bent Coppers (p45) and Punch's 'police Corruption' p127, a more detailed account is provided in George Dilnot's 'The trial of the Detectives' (Dilnot, 1928).
[10] The Code for Crown Prosecutors contains a 'public interest test' which features among other aggravating factors the fact that the alleged offender was in a position of trust.

Despite further allegations of corruption and resignations the mid-20th century saw what can be described as the golden era in police / public perception. For many the image of television's 'Dixon of Dock Green' was the unassailable representation of the British police. (*Morton 1983, P90*). The interest in police corruption seemed to wane until November 1955 when the Daily Mail published an article, 'Tipped off?'[11] In this article the paper alleged that gaming houses and brothels were being given police information as to raids in exchange for regular payments. The Metropolitan Police and government officials acted quickly to deny the allegations, despite the Mails' claim to have possession of an internal document raising these concerns with the Commissioner. The police response once again, was that the newspaper's reporting of the document was *'utterly misleading and most mischievous'*. (*Morton 1983, p94*). Despite the denials, the following months saw a number of disciplinary investigations take place and criminal trials relating to the perverting of internal investigations.

Whilst minor revelations continued to occur, perhaps the next large scale corruption issue occurred in 1969 when the Times newspaper published allegations of corruption against the Metropolitan Police. This time protestations were more difficult to make, as the newspaper was seen as a reliable source and had also been able to produce photographs and tape recordings to back up their article (*Punch 2009*). This story led to a number of difficult enquires for the Met, and a breakdown of their hitherto positive image.

In 1972 Robert Mark, an officer who had previously worked exclusively outside London, but had been appointed to the Metropolitan Police as an Assistant

[11] The Daily Mail 17th November 1955.

Commissioner some years earlier, was promoted to Commissioner. He is most noted for the strident action he took to tackle police corruption. He formed a new department within the force to investigate other officers, and he openly expressed to detective officers that they represented *'what had long been the most routinely corrupt organisation in London, and that nothing would prevent him from putting an end to it' (Punch 2009, pp133-134)*. Mark's primary strategy being to rid the organisation of the 'cancer of corruption', he accepted a number of officer's resignations[12]. He did however prompt the charging and subsequent trial of 14 officers.

Whilst Mark undoubtedly made a number of inroads into the tackling of police corruption, a year after his retirement in 1978 a bank robbery and the shooting of a security guard led to further allegations of police corruption. A number of 'super grass' exposés suggested that criminals themselves were becoming intolerant of police corruption as they were increasingly working for the police, giving them the lion's share of the proceeds. (*Punch 2009, p135*). As a result of these new allegations perhaps the largest and most well-known anti-corruption programme was started. 'Operation Countryman' was led by Dorset's Assistant Chief Constable Leonard Burt and was originally based in Godalming in Surrey; as any premises within the Metropolitan Police area were not deemed sufficiently secure. (*Reiner 2010 & McLagan 2003*). Over a four year period Countryman investigated over 200 officers, including a number of senior officers. (*Punch 2009*). From the outset however the operation was dogged with accusations of being frustrated by Met officers. By the time the enquiry had closed, the team had taken 2000 statements, pursued 200

[12] It is suggested that almost 500 officers left the force rather than face investigation (*Hobbs, 1988: Punch 2009, p134*)

separate corruption allegations, and submitted 41 reports to the Director of Public Prosecutions. Only 4 prosecutions were sanctioned and of these only two officers were convicted of any offences *(Reiner, 2010. p82).* These low conviction figures led to allegations from the Countryman team of obstruction by Met officers to protect their colleagues[13]. These in turn were countered by comments from the then Commissioner, Sir David McNee, that the Metropolitan Police would have had more success if they had handled the inquiry internally rather than giving it to another force[14].

Following Operation Countryman the police service in general appears to have experienced a lull in corruption allegations. This was soon broken when in early 1993 the BBC's Panorama aired a television programme exposing DC John Donald, an experienced detective working within the élite South East Regional Crime Squad (SERCS) as being involved in taking money in order to frustrate criminal trials. Donald was covertly recorded by the BBC bargaining with one of his informants for money in order to 'lose' surveillance logs in a large drugs trial, an action which would undoubtedly cause the collapse of the trial. Following the programme Donald and a number of his colleagues were arrested. The damage however had been done with virtually every national newspaper following up the story the next day. *(McLagan, 2003, p27).* The significant embarrassment caused again prompted the Metropolitan Police to act, this time in developing a covert anti-corruption squad, more importantly however it placed police corruption back on the public agenda. In 1997 the then

[13] Allegations included the leaking of information by Met Officers to criminals about their enquires as well as surveillance operations being compromised by marked patrol cars 'inconveniently appearing to alert those under observation' (Reiner 2000. P136).
[14] Whilst the number of convictions obtained compared to the number of investigations is low, it has been convincingly argued that the enquiry cast doubt on the suggestion that endemic corruption had been eliminated from Scotland Yard (Hobbs, 1988 : Reiner 2000, p82). The success of Operation countryman therefore was probably to maintain the issue of corruption on the political radar.

Commissioner, Sir Paul Condon gave evidence to the Home Affairs Select Committee, stating, *"I do have a minority of officers who are corrupt, dishonest and unethical. We believe sadly, that they commit crimes, they neutralise evidence in important cases and they betray police operations and techniques to criminals". (Condon, P in McLagan, 2003. p1).* The Commissioner's statement did not put a figure on this 'minority of officers', but during questioning, on being asked how many 'bad apples'[15] there were in London, he replied that there were up to 250.[16] *(McLagan, 2003 pp3-5)*

With the maintenance of the Metropolitan Police's Anti-Corruption Unit, and more and more provincial forces adopting a similar model, police corruption as an open problem was from that point here to stay. The next ten to fifteen years were littered with a number of trials and reports in national newspapers, but with what appeared to be a far more measured approach, treating it on a par with other serious crime reporting. The days of huge public exposés identifying endemic corruption at senior levels appeared to be gone, until the summer of 2011 when allegations were made regarding inappropriate links between the police and the media themselves. These allegations were based around previous criminal enquiries into phone hacking.[17]

The 2011 allegations led to a number of senior Metropolitan Police officers giving evidence at the Home Affairs Select Committee. Criticism was made of inappropriate relationships based on excessive hospitality that had developed, and that these had allegedly clouded some investigations. In July that year the Metropolitan Police

[15] The bad apple analogy is used extensively by Punch in his 2003 and 2009 work where he goes on to suggest that the problem is not bad apples, but bad barrels and even bad orchards. (punch 2009 ,p9)
[16] The quoting of such a finite figure is believed to have caused significant problems to Sir Paul and his Successor Sir John Stevens, and was used by corrupt cops to hit back at their accusers in subsequent trials *(McLagan 2003 , p5)*
[17] 2010 saw a number of allegations made against journalists for the illegal interception of voice mail messages left on the mobile phones of a number of high profile persons. Following the investigation only one person was convicted, although popular belief was that many more were involved.

Commissioner, Sir Paul Stephenson, publicly acknowledged the acceptance of approximately £12,000 of hospitality at a Hertfordshire health club[18] and this was quickly followed by his resignation from post.[19] Some days later Assistant Commissioner John Yates also resigned from the force following personal criticism of his handling of the original 2010 investigation. Once again it appeared that the spectre of police corruption had dented public confidence, and this time, with the loss of such senior figures within the police it was the government who acted. The Home Secretary, Theresa May launched a package of reviews designed to uncover further inappropriate behaviour, put measures in place to prevent recurrences, and to reassure the public. These included a review by Her Majesty's Inspectorate of Constabulary (HMIC) into Police Integrity, an IPCC Inspection into Police Corruption, and a Judicial enquiry led by Lord Justice Leveson into the conduct of the British media. In addition, the Metropolitan Police launched two investigations themselves, one into the original 'phone hacking' allegations and the second into media relationships.

Doses of Antibiotics

"It's not a scandal to have a corruption problem. It's a scandal not to recognise the problem... We had to break the cycle of corruption; it's like doses of antibiotics to deal

[18] (Guardian News and Media Ltd, 2011) http://www.guardian.co.uk/uk/2011/jul/17/sir-paul-stephenson-resignation-statement (Accsessed 29-1-13)
[19] It should be noted that a subsequent Independent Police Complaints Commission (IPCC) investigation cleared Sir Paul of any criminal wrongdoing.

with bacteria. Unless you take the full dose, the bacteria get stronger." (Clark, R in McLagan, 2003. P7)

Whilst it may appear that police corruption has only been countered by individual and sporadic high profile events driven by embarrassing exposés and media revelations, this is unlikely to be a fair representation of the facts today. Since the early 1990s significant work has been undertaken in the area of values, ethics and integrity. In addition more recent work, in the first instance by the Metropolitan Police Service (but subsequently by other forces) has tackled corruption and corrupt officers directly.

1990 saw the national introduction of the Statement of Common Purpose and Values, providing a set of values that all forces should adhere to. In the mid-1990s, albeit following high profile revelations, the Metropolitan Police formed a permanent Anti-Corruption Unit working under its Directorate of Professional Standards. Sir Paul Condon, the then Commissioner is quoted *"We recognise that a small number of officers either through bad behaviour or corruption can have a disproportionate impact on our reputation. We want them to be in constant fear of exposure". (Condon, P, in McLagan 2003 p79).*

In 1999 Her Majesty's Inspectorate of Constabulary (HMIC) conducted a review of police integrity. Paragraph 19 of the executive summary reads *"Robust, proactive investigation into suspected corruption and the proactive maintaining of integrity by auditing, random or non-targeted integrity testing, as well as quality of service checking, is being developed in several forces and is very much encouraged" (HMIC 1999. p19).*

Between 2000 and 2009 more anti-corruption units were formed in forces outside London [20] and in 2006 the Anti-Corruption structure was further enhanced by the setting up of the Serious and Organised Crime Agency (SOCA) with a specific arm focused at police corruption. This unit produces a three yearly police corruption threat assessment circulated to all forces.

When, in 2011 the reports by HMIC and the IPCC were completed, they revealed a number of findings. The former, whilst going to some lengths to engage with every force in England and Wales produced a report which made no reference to individual areas; but provided an overview of the situation UK wide. Much mention was made of 'Gifts and Hospitality' procedures[21] and once again reinforced the necessity for strong anti-corruption units within forces. The IPCC report focused directly on corruption but consisted of a number of case studies that had been previously referred to them. It made a small number of recommendations as to further safeguards forces should consider in order to protect themselves, particularly in the area of information leakage.

Having provided an overview of a number of historic and contemporary police corruption cases and their impact on public confidence, along with a summary of the police and government responses to these, the author now moves in the following chapter, to examine existing research in the field of police corruption and how this relates to the specific area of study, the corrupt mishandling of police information.

[20] Whilst data on exact go live dates is difficult to obtain as different perspectives exist as to the make-up and work of such units, it is clear that very little mention was made of such units in the 1999 HMIC review, whilst in 2009, they were widespread.
[21] This is perhaps not surprising as events leading to the inspection include an increase in public concern at the receiving of significant gifts and hospitality by some senior police officers.

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 2
Literary Review (Part 1)
Police Corruption

Overview

In this and the following chapter the author considers two main areas for literary review; firstly and principally, the issue of police corruption, and secondly, with particular reference to this thesis, the rise of computer misuse generally in society. In so doing the author hopes to greater inform discussion in the later parts of this work by overlaying the two concepts.

Police Corruption

The arena of police corruption is such that contributions to the literature on the topic come from a number of sources and backgrounds. They are likewise varied in their subject matter, ranging from exposés, to studies of the causes, to research into methods of prevention, to internal police reviews on estimating the scale of the problem. In order to maintain workable boundaries for the purpose of this thesis the author has separated works into three distinct areas; academic research, journalistic material, and internal reviews undertaken by or on behalf of the police. Likewise, the nature of the material reviewed here, particularly in the academic field, is limited to work from the latter part of the 20th century onwards. It includes definitions, typologies, and the causes of corruption, in order to draw meaningful comparisons to the research findings. The first section as it relates to police corruption therefore

consists of a chronological examination of previous works on each theme from the three source types.

Defining Police Corruption

There exist a significant number of definitions of corruption, used by academics in previous studies, these range from rather narrow definitions like those used by McMullan his 1961 'A Theory of Corruption' (McMullan, 1961)[22], through to those far wider in nature such as that put forward by Kleinig in his 1996 study 'The Ethics of Policing' (Kleinig, 1996). It has also been argued that given the various different activities which could fall into the corruption arena a precise definition is difficult to come by and of limited use, as corrupt practice is recognisable when encountered regardless of particular labels. (Newburn, 1999).

McMullan's view in 1961 was that *"a public official is corrupt if he accepts money or money's worth for doing something that he is under a duty to do anyway, that he is under a duty not to do, or to exercise a legitimate discretion for improper reasons." (McMullan, 1961. P183)*. This definition may at first sight appear to be very limited as it excludes any activity the motivation for which is not money or 'money's worth'. To understand why there may be this omission it is necessary to look at the original focus of McMullan's research, that of public officials generally rather than policing in particular. Whilst he provides some specific examples involving the taking of bribes by

[22] McMullan was examining corruption in the public services of British Colonies, and not the police specifically. The definition provided however gives a good starting point as a definition of corruption.

prison officers, his definition can perhaps be forgiven for failing to include activities peculiar to policing.[23]

Some two years later James Wilson conducted a study specifically into policing, directed at what he termed 'The problem of the crusade'. In this he outlines the difficulties placed upon police officers who are expected to uphold the law, but at the same time not to uphold the law[24] (Wilson, 1963). In addition he makes a distinction between police corruption and criminal acts *per se*. He advances the idea that although corrupt acts may be criminal (such as the accepting of bribes where prohibited by criminal law), and criminal acts may be corrupt (such as the perverting the course of justice for private gain), the two are not inextricably linked, moreover there exists a significant divide. For Wilson therefore unless the activity itself relied upon the abuse of authority or position of trust, it did not amount to corruption. Significantly he argues that even offences such as burglary by officers on duty amount to criminal acts alone, and not corruption.

A supporting view is provided by Stoddard in his 1968 study, 'The informal code of police deviancy', in which he draws a similar distinction between criminal acts and police corruption. Whilst Stoddard acknowledges the weakness in his own study of the use of a single 'informant' in his research, the strength of the paper is not necessarily in the descriptions of illicit police activities provided, but the distinction advanced between straightforward criminal acts and what is termed 'Blue Coat

[23] Activities such as 'noble cause corruption' rarely involve the gain of money or money's worth by any individual but are generally seen as corrupt practice.
[24] By this Wilson explains that officers are expected to uphold the law in the prevention of crime but also to understand the social pressures and maintain compassion for the poor and disenfranchised who often break laws in order to survive.

crime'[25] (Stoddard, 1968). Here Stoddard has widened the scope of police mal-practice[26] to three distinct categories of behaviour; firstly corrupt acts which may not necessarily breach the criminal law, but may include activities such as accepting small gratuities or gifts. The second category consists of Wilson's criminal acts but only to the point where the use or exploitation of the official position of the police officer is not involved. In this way criminal acts committed by officers outside their role in policing are treated no differently than criminal acts committed by any other member of the public. The final category consists of those criminal acts which rely upon the participant's role as a police officer in order to be committed. These include such offences as accepting bribes or committing perjury and it is these activities Stoddard labels 'Blue Coat Crime'.

The 1977 work by Carl Klockars again focuses on the distinctions between the types of police mal-practice. Whilst accepting Stoddard's boundary between generic criminal acts and 'Blue Coat Crime' he goes on to reinforce his view that in matters of corruption the all important aspect is that which is corrupted, and for Klockars this is *'the special trust invested in the occupation'* (*Klockars, 1977*). For Klockars therefore there is only one essential part to any definition on police corruption, that of *'the exploitation or misuse of authority'*. (*Klockars, 1977*). His 1977 work goes on to provide a more in-depth definition by separating down the consequences of corruption into two categories. Firstly he argues that the acceptance of bribes (McMullan's' *'money or money's worth'*) perverts *'the fair distribution of the ends of policing'*, whilst the commission of criminal acts perverts *'both the ends and the means*

[25] Here Stoddard modifies the Edwin Sutherland's term 'White collar crime' (Sutherland, 1968) to denote crime that is committed or facilitated through the exploitation of an official position.
[26] The author uses the term 'mal-practice' here to avoid encroaching on the term 'corruption' with its different definitions.

we entrust the police to achieve them'. (*Klockars, 1977, p334*). For Klockars therefore any definition of police corruption must include an exploitation of authority and impact on either the end or means of policing.

Maurice Punch, in his 1985 book *'Conduct unbecoming: The social construction of police deviance and control'* appears to move back to a more traditional and straightforward definition of police corruption which, whilst not challenging the views of Wilson, Stoddard or Klockars, is far more aligned to the traditional view of McMullan. He therefore appears to suggest that categorisation of different types of mal-practice, consideration of the ends and means of policing and other labels used in describing various acts are not needed simply to identify police corruption. Instead he provides a definition not dissimilar to that of McMullan, but expanded in order to overcome the noble cause aspect and exclude the requirement for personal gain. For Punch therefore corruption occurs *"when an official receives or is promised significant advantage or reward (personal group or organisational) for doing something that he is under a duty to do anyway, that he is under a duty not to do, or for exercising a legitimate discretion for improper reasons, and for employing illegal means to achieve approved goals" (Punch, 1985, p14)*

If Punch is seen to provide a traditional all-encompassing definition of police corruption a more holistic approach is taken by John Kleinig in his 1996 *'The ethics of policing'*. In this Kleinig asserts that *"Police officers act corruptly when, in exercising or failing to exercise their authority, they act with the primary intention of furthering private or departmental / divisional advantage."* (*Kleinig, 1966, p166*) In so doing he argues that previous definitions do not allow for the inclusion of mal-practice which is

neither criminal nor contrary to any regulation but is nonetheless motivated otherwise than in accordance with the organisational good. He provides an example to illustrate this assertion of over-zealous policing for personal advancement by an individual officer. (Kleinig, 1996). For Kleinig therefore police corruption is an ethical and motivational issue rather than a matter of regulation or criminal transgression.

Whilst the availability of academic material may seem limited, even more so is the work carried out internally by governments and police forces in gauging the scale of, and tackling corruption. In the United States, the early 1970s saw perhaps their most high profile enquiry into corruption with the opening of 'The commission to investigate alleged police corruption' under Judge Whitman Knapp[27], but it was not until later that decade that the UK experienced a similarly high profile investigation, in 'Operation Countryman'. Whilst both were high profile and captured daily headlines, the former was a judicially led public enquiry whilst the latter was a covert internal investigation only releasing its findings at its conclusion. In addition to these two large scale and high profile enquiries, the UK has also seen the setting up and reporting back of the 'Committee of Standards in Public Life'[28], three inspections by Her Majesty's Inspectorate of Constabulary (HMIC); 1999 – *'Police Integrity – securing and maintaining Public Confidence'*; 2006 *'Raising the Standard'*; and 2011 *'Without Fear or Favour'* and an enquiry in 2011 by the Independent Police Complaints Commission (IPCC).

With such a number of enquiries and reviews it may be expected that at least one would include as a starting point a bespoke definition of police corruption.

[27] This subsequently became known as the Knapp Commission and is almost universally referred to as such.
[28] This Committee is often referred to by the name of its first chairman, Lord Nolan.

Regrettably however this appears to be universally lacking.[29] This is not to suggest that the various reviews and committees do not assist in any way, but it is necessary to review the type of behaviour they have examined in order to ascertain what each report deems to be 'corruption'.

Both the Knapp Commission and 'Operation Countryman' have focused on corruption at an organised level. The former was instigated following revelations by a serving officer frustrated by endemic corruption within the force whilst the latter was formed following internal allegations of corruption within the Metropolitan Police after the collapse of a number of serious trials. The Knapp Commission received evidence from a number of officers in relation to low level corruption such as the accepting of free meals at restaurants, as well as more organised crime such as the protection of illegal vice and gambling operations. 'Operation Countryman' in contrast, focused purely at organised corruption within the detective ranks. It would appear therefore that the two enquiries held differing views of what would fall within their scope. Whilst it is useful from a review perspective to draw such boundaries, these cannot be taken to determine a categorical definition of police corruption, merely that which was deemed sufficiently important at that time to investigate.

In 1995 Lord Nolan published the first of his committee's reports into the standards of public life. Whilst not focused on policing but on the whole of the public sector, he avoided definitions of what was outside of an acceptable norm by reinforcing what have now become known as his seven principles; Selflessness, Integrity, Objectivity, Accountability, Openness, Honesty and Leadership. Importantly for this study Nolan

[29] The IPCC review in 2011 does provide a dictionary definition of corruption as "dishonest or fraudulent conduct by those in power" and point readers towards two other agencies; 'The Association of Chief Police Officers' (ACPO) and 'The Serious and Organised Crime Agency' (SOCA) for other definitions

made specific comment as to the expansion of application of these principles *"These principles apply to all aspects of public life. The committee has set them out here for the benefit of all who serve the public in any way" (Nolan LJ, 1995 p14)*. It can be seen therefore that for Nolan, any deviance from the acceptable standards in public life were unacceptable.

In the first of the three HMIC inspections touching on Police Corruption, the 1999 report 'Police Integrity, Securing and Maintaining Public Confidence', states *"Cases of corruption are thankfully rare. This is illustrated by the data in appendix C which shows that, as at 31 December 1998, 153[30] officers were suspended for alleged corruption and similar matters." (HMIC, 1999 p7).* Whilst maintaining its position of being *"not about corruption in a narrow sense, but how public confidence is secured and maintained" (HMIC, 1999 p7),* it does go on to outline one type of corruption in particular, that of *'noble cause'*[31] of which it is fierce in its rejection. *(HMIC, 1999 p21).* The report also makes mention of differing levels of corruption and draws a distinction between higher level and lower level corruption, before firmly rejecting the acceptability of either *"... some people expressed the view to the Inspection Team that the Service should be concentrating on combating hard-edged corruption, and not be concerned about minor perks. The Director General of The National Criminal Intelligence Service, however, expressed his belief that, 'Corruption results from a failure to maintain integrity.' Her Majesty's Inspector firmly shares this view and*

[30] Whilst this figure may appear low against the large number of police officers in the UK at that time (100,000 +), it represents only a snapshot on the 31st December 1998 and so does not provide a real assessment of levels of corruption.

[31] Noble Cause corruption is a colloquial term used to describe corruption with the objective of 'seeing justice done' for the benefit of victims or society, rather than with a view to any personal gain. The idea is explored by Punch in his 2009 work where he provides accounts of officers seeing themselves as acting "from a form of altruism", and some emphasising the "sacrifices they had made and energy they had expended without thought of personal gain" (Punch 2009. p 107).

considers it will be far more difficult for corruption to flourish if gifts, gratuities and perks are seen as totally unacceptable within the Police Service." (HMIC 1999, p48).

Whilst still not providing a firm definition it is notable that from the appendices of the report, a number of activities are linked together under a heading including corruption; *'Dishonesty, Perjury, Deception, Theft, Fraud, Corruption, Forgery and Bribery'*. This category alone however shows only 110 officers suspended and so in order to arrive at the stated 153 a further 43 are required. These are found in categories headed *'Integrity of Investigation'* (5), *'Improper practice'* (1) *'Perverting the course of justice'* (26), *'Undisclosed Business Interests'* (5), and the *'Unlawful disclosure of information'*(6). Whilst stopping short of providing a definition it does provide an insight into HMIC's view of the boundaries of corruption. (*HMIC 1999, App C, p94*)

The second HMIC thematic Review in 2006, *'Raising the Standard'*, was more specifically focused at force's Professional Standards Departments (PSDs)[32], and for the first time places an emphasis on the importance of Anti-Corruption Units. Interestingly however the report highlights areas of corruption that it sees as the greatest areas of threat as *"information leakage, in particular using intelligence or information for personal gain or passing it on to associates; infiltration of the organisation, which is an increasing threat in the ever-widening 'police family'; and substance misuse, with its associated risks of coercion and targeting for blackmail." (HMIC, 2006 p7)* This is in contrast to the previous study where only six officers were suspended nationally for the improper disclosure of information. (*HMIC 1999, App C,*

[32] Professional Standards Departments are internal units working within forces. Among other functions, their role generally consists of dealing with public complaints, internal misconduct and of course police corruption. They are in actuality a British version of the American "Internal Affairs" departments made famous by the US film industry.

p94). Whilst again stopping short of providing a definition of corruption it is possible to see from the report the changing activities falling under the corruption banner, reflecting the changing face of technology and information storage. With the exponential rise in the use of police databases and the ever increasing storage capabilities, a rise in the risk of their misuse and subsequent information leakage was to be expected. This coupled with ever increasing audit capabilities of Professional Standards Departments doubtless led to HMIC's strong assertion that the rise of information leakage was a significant problem. With the benefit of current knowledge, the 1999 report may be seen as prophetic in its highlighting of computer misuse and information leakage. Today this area constitutes a significant majority of police corruption enquiries and is highlighted in the recently published Leveson report into police / media relationships *(Leveson LJ. 2012)*[33] and the Met Police's operations Elvedon and Weeting[34].

The year 2011 was characterised by allegations of police corruption and wrongdoing. Many of these were prompted by investigations into improper associations between senior police officers and national newspapers, along with allegations of phone hacking. As a result of these allegations the Home Secretary directed HMIC to conduct a further review of Police Integrity, and the IPCC to carry out a review of corruption. The HMIC review itself did not assist in the definition of corruption, but the IPCC enquiry did offer a dictionary definition as well as outlining those definitions adopted by the Association of Chief Police Officers (ACPO) and the Serious and Organised Crime Agency (SOCA). From this document it can be noted that ACPO define

[33] Part two of the Leveson report relates specifically to media / police relationships.
[34] The Metropolitan Police investigations into phone hacking and the relationship between police and media officials to facilitate the original offences and frustrate subsequent investigations.

corruption as *"the abuse of one's role or position held in the service for personal gain or gain for others"(ACPO in IPCC, 2011, p14).* This definition appears to exclude the concept of noble cause corruption in all but the most liberal interpretations of *'gain for others'*[35]. The SOCA definition does appear to fill this gap with a definition which seems to fall somewhere between those of Punch and Kleinig; *"any activity carried out by an individual for gain, favour, advancement or reward that is inconsistent with the proper practice of their office, employment or responsibility" (SOCA in IPCC, 2011, p 14)*

In the second part of their review published in May 2012 the IPCC highlight their concern at the lack of an established working definition of corruption and document their aim to work with the police, Crown Prosecution Service (CPS) , and SOCA to finally provide such a definition. (At the time of writing however, this work has not been completed).

Having reviewed a number of academic definitions and perspectives provided by internal review documents, a further view is provided by journalistic articles and books. These differ from the former categories most notably in their target audience and primary purpose[36] and therefore must be viewed with some caution as examples given tend to be of a more sensational nature. It is likewise notable that prior to the 1970s there are few publications in this area and what appears an explosion of interest since then. Journalistic sources are valuable however, as they often consist of

[35] The definition's use of the term 'gain for others' relates primarily to either financial gain to third parties or protection of third parties from law enforcement activities. At its most liberal interpretation it could be seen to encompass gain for victims at the expense of ethical practice,(and therefore potentially include noble Cause corruption)' but this is not made clear in the document.
[36] The author advances that journalistic material is invariably aimed at the mass consumer with an ultimate aim of financial profit.

first-hand accounts given by corrupt officers and what they lack in rigour is in some way compensated by their proximity to the subject itself.

One of the first popular exposés in this category is Barry Cox's 'The fall of Scotland Yard', in which he describes a number of high profile events between 1969 and 1975. Cox is at pains to clarify that his work is not 'another anti-police book' *(Cox, Shirley, & Short, 1977. p9)* but goes on to provide a background to a number of exposés regarding police corruption. Whilst Cox does not provide any firm definition of corruption, the nature of the cases studied leave little room for doubt that for him, it consists of the receipt of money in exchange for failing to carry out police duty.

James Morton in his 1993 'Bent Coppers' follows a similar path to Cox and whilst not providing his own firm definition of police corruption does give examples of behaviour which he commonly refers to as corrupt. These consist of the higher end organised acts such as bribery, blackmail and the extortion of money by both junior and senior officers to protect other illegal activities such as gambling. The ethos of his work very much reflects organised corruption of endemic proportions, and due to the nature of the corruption he outlines, he tends to focus on cases that have been to trial and resulted in criminal convictions. Whilst avoiding his own definition Morton does reproduce one used by the United States National Advisory Commission in 1975; *"Police Corruption consists of acts which involve the misuse of police authority for the police employee's personal gain: activity of the police employee which compromises or has the potential to compromise, his ability to enforce the law or provide other services impartially; the protection of illicit activities from police enforcement, whether or not*

the police employee's involvement is promoting the business of one person whilst discouraging that of another person" (Morton, 1993 p208).

2003 saw the publication of Graeme McLagan's 'Bent Coppers' in which he, like previous authors focuses on the higher end of police corruption, outlining activities more fitting into everyday organised crime such as robbery and extortion. McLagan's view is however slightly different to that taken by other authors, in that his work is more of a 'fly on the wall' documentary into the creation, and subsequent work of the anti-corruption units. In his book he outlines anti-corruption work in relation to the Flying Squad[37], drug squad and the South East Regional Crime Squad (SERCS), all élite units dealing with serious and organised crime. What comes out from McLagan's work is that for him corruption is highly organised, most notable in detective environments, and consists of serious crimes. In the opening chapter he outlines what he calls 'The Problem', and uses quotations from a previous Metropolitan Police Commissioner, Sir Paul Condon, to portray corruption; *"I do have a minority of officers who are corrupt, dishonest and unethical. We believe, sadly that they commit crimes, they neutralise evidence in important cases and they betray police operations and techniques to criminals" (Condon 1997, [38] in McLagan 2003, p 1).*

It is clear from the academic works, internal reviews and journalistic material that there is limited agreement as to a firm definition of police corruption, however with the exception of early definitions such as that of McMullan they all to a greater or lesser degree encompass what *'the man on the Clapham omnibus'* would determine as corrupt, and indeed some, such as that of Kleinig go much further.

[37] A colloquial term used within the Metropolitan Police for the team tackling armed robberies in London.
[38] Speech to the Home Affairs Committee on police wrongdoing 1997

For the purpose of this research the author is of the view that the most useful definition available would fall somewhere between that of Punch in his 1985 work, and that of Kleinig in his 1996 work. The author puts forward that Punch's definition[39] is too restrictive in that the use of the word '*significant* 'in relation to advantage or reward, appears not only subjective, but also appears to exclude the idea of personal or emotional gratification as a motivation. This is important as it appears strong in a number of computer misuse cases where information is sought out of nosiness or to enhance one's own status within a peer group rather than to disrupt police activities. The definition used by Kleinig however appears almost nebulous in its lack of boundaries[40], with any activity not purely for the good of the organisation constituting corruption. For the author therefore the most helpful working definition for the purpose of this research is Punch's definition with the word 'significant' removed and adapted to include personal gratification; *"when an official receives or is promised advantage, reward or gratification (personal group or organisational) for doing something that he is under a duty to do anyway, that he is under a duty not to do, or for exercising a legitimate discretion for improper reasons, and for employing illegal means to achieve approved goals" (Adapted from Punch 1985, p 14).* Having examined various definitions of corruption the next challenge is to break corruption down by type and distinguish between its different forms.

[39] *"when an official receives or is promised significant advantage or reward (personal group or organisational) for doing something that he is under a duty to do anyway, that he is under a duty not to do, or for exercising a legitimate discretion for improper reasons, and for employing illegal means to achieve approved goals" (Punch, 1985, p14).*

[40] *"Police officers act corruptly when, in exercising or failing to exercise their authority, they act with the primary intention of furthering private or departmental / divisional advantage." (Kleinig, 1996)*

Types and Typologies

Perhaps not surprisingly the greater part of information on typologies within police corruption is to be found within academic research, with journalistic material and internal reviews playing a supporting role. The earliest of these of particular relevance is that provided by Stoddard in his 1968 work. Whilst reiterating the inherent weaknesses in his use of a single source for his work, he avoids any typology of those involved in corruption, focussing instead on varieties of activities. He lists ten activities which his research suggests form the general makeup of corruption;

Table 1- Typology of Police Corruption by Stoddard

Mooching	*Receipt of free gifts.*
Chiselling	*Demands for free admission / gifts*
Favouritism	*Use of cards / signs to gain immunity from prosecution.*
Prejudice	*Less favourable treatment of minority groups with less influence.*
Shopping	*Theft from stores or insecure locations normally small items*
Extortion	*Demands made for adverts in police magazines or for tickets to events.*
Bribery	*Payment of cash or gifts for current of future preferential treatment.*
Shakedown	*Similar to shopping but for larger more expensive items.*
Perjury	*Lying on oath by officers to support each other*
Pre-meditated Theft	*Planned burglary or robberies*

(Stoddard, 1968)

The significance of this early typology is that it has been amended on a number of occasions over the last 50 years but even in its most recent form (Punch's 1985 amendments to Barker and Roebuck's 1973 text), reproduced in his 2009 work, '*Police Corruption; Deviance, Accountability and Reform in Policing*'). The original characteristics can still be seen. It can therefore be seen to provide an early background and doubtless influence to subsequent studies.

Moving some 5 years forward to perhaps the most renowned academic typology of police corruption, Barker and Roebuck in their 1973 literary analysis outline eight types of corrupt practices.[41]

Table 2- Typology of Police Corruption by Roebuck and Barker

Corruption of Authority	*The receipt of free drinks / meals without necessarily violating the law.*
Kickbacks	*Gain for referring business to particular firms, such as the use of preferred boarding up companies, garages for vehicle removal etc.*
Opportunistic theft	*Stealing from detained persons, dead bodies, scenes of crime.*
Shakedowns	*Gain for not correctly applying the law, such as failing to arrest, issue a ticket.*
Protection of illegal activities	*Enabling illegal enterprises to continue such a gambling dens by the provision of tactical / intelligence information. This also can apply to legitimate businesses that occasionally break the law.*
The fix	*Undermining criminal investigations or the losing of evidence.*
Direct criminal activities	*The commission of substantive crimes.*
Internal pay-offs	*The paying of supervisors by officers for favourable adjustments to duties. The opportunity to earn overtime, promotion or easy assignments.*

(Barker & Roebuck, 1973 in Newburn, 1999)

Roebuck and Barker advance that their typology represents a hierarchy of deviant practice. The nature of this hierarchy is however unclear and lacks an explanation as to the basis of the measurement[42], be it potential damage to the organisation, damage to society, ease of undertaking or simply the numbers involved in the practice

[41] A ninth type was subsequently added by Punch in 1985

[42] Stoddard also advanced that his typology represented a hierarchy but clearly spelt out that they were in the order that would elicit least fear of legal prosecution. (Stoddard, 1968)

with the top of the list being more widespread. Whatever position is put, the eight categories provided do conflict with some definitions of police corruption; in particular Wilson (1963) and Stoddard (1968) who maintain the commission of criminal acts are not corruption per-se. Also notable from the typology is the omission of the concept of noble cause corruption. (This is however in keeping with McMullen's view generated in a broadly similar era, perhaps demonstrating the lack of awareness or importance of this area at that time). It is also possible to see that whilst as general principles the typology appears to remain relevant, the advances of technology require a sympathetic interpretation of some of the activities. Activities such as the passing of information on to organised crime groups, can be seen as the *'protection of illegal activities'* it is however more difficult to identify a category which involves the sale of such information to third parties (such as private detectives), other than perhaps the 'default' *'Direct criminal activities'*.

In 1985 Maurice Punch published his 'Conduct Unbecoming: The Social Construction of Police Deviance and Control' in which he presents two typologies relating to types of officers, and types of corruption, *(Punch, 1985).* In the first of these typologies Punch outlines, the *'Uniform carrier'*, *'Mister average'*, *'Professionals'*, *'Dirty Harrys'*, *'Noble causers'*, *'Innovators and number crunchers'*, *'Crusaders'*, *'Ideological combatants'*, the *'Lone wolf'*, and *'Cowboys'*. He advances that corrupt officers are generally found within the last seven types with the first three generally remaining free from deviant practice. There does however appear to be significant overlap in the last seven categories, with only 'innovators and number crunchers[43]', Lone

[43] Here Punch refers to those pushing the boundaries of police practice in order to show themselves in a good light.

wolves[44]' and 'Cowboys' appearing to be outside the paradigm of susceptibility to noble cause corruption. It is the category of 'Cowboy' that appears to conjure up the traditional image of the corrupt officer portrayed in exposés. According to Punch they are the officers who *"were typically undisciplined... treated supervisors with near contempt ... rebellious, keen to get out of uniform and become detectives, enjoyed delving into the watering holes of the underworld" (Punch, 1985 reproduced in Punch, 2009. pp23-26)*.

The second typology presented in Punch's 1985 work is that of Roebuck and Barker with an additional ninth category;

Table 3- Addition made to Roebuck and Barker's typology by Punch

Flacking and Padding	*Planting or adding to evidence 'to set someone up' to ensure a conviction.*

(Punch, , 1985. p11)

Punch advances that this addition is necessary to take into account deviant practices in the new world of drugs enforcement. It is also useful in that it provides an easier fit for the concept of noble cause corruption, rather than having to squeeze this into the 'direct criminal activities' category.

In the field of internal reviews, one in particular has contributed above others to a working typology of police corruption. The 1972 Knapp commission received testimony from a number of officers. One such officer provided his view on three types of officer. His testimony was reviewed and reproduced in Barker and Roebuck's

[44] Punch's 'Lone Wolf' is an officer obsessed by a particular enquiry or aspect of police work, to the detriment of other working practices, whilst he may stop short of noble cause corruption, his practices would be deviant.

1973 work, but it remains however a product of an internal enquiry. The first type of officer outlined was denominated the 'grass-eater', an individual who would graze, take small perks as they came along, such as free meals and price reductions on purchases, but they draw a line between these 'low level' acts and significant corruption. The second category, 'meat-eaters' are more proactive in their abuse of power. They actively seek opportunities for corruption and gain. They would be happy to derail an investigation for money, or extort money from businesses for 'protection'. This group represents the hard-core corrupt officer. The third category is that of 'birds', who soar high above the corruption taking place beneath them. They avoid deviant practice, because they are either honest, or because they do not have sufficient opportunity for corruption. Significantly however, 'birds' do not challenge corruption, moreover they are wilfully ignorant of its practice. *(Knapp, 1973 in Barker & Roebuck, 1973. p35).*

The significance of this typology is that it fits the mainstream definition provided by Punch in his 1985 work by allowing for different types of activities to be categorised into different levels of corruption. Like the work of Roebuck and Barker, there appears to be a hierarchy at least between 'grass-eaters' and 'meat-eaters' if only in the perceptions of the former by the drawing of a line they would not cross. This typology also allows for similar deviant activities to be categorised on different sides of the 'grass / meat' line depending on the motivation of the individual. Such an example would be the leakage of police information from the misuse of computer systems. Where such activity is to provide intelligence to an Organised Crime Group (OCG) to disrupt their apprehension or protect their activities, it is likely to be

categorised as *'meat-eating'* conduct. The same activity where information is passed to a friend enquiring about his daughter's new boyfriend, in order to reassure or protect an individual may well fall into the *'grass-eating'* arena. In this way, the typology supports Kleinig's view that corruption is a motivational issue, rather than an issue of pure activity, as the same activity may be categorised differently depending on its purpose or objective. *(Kleinig, 1996 in Newburn 1999).*

The final source of typology reviewed here is that provided by journalistic material, which, whilst being basic, provides a neat division, again between differing motivations for police corruption. James Morton in his 1993 'Bent Coppers' sets out two distinct categories of corrupt officer; 'Bent for self' and 'Bent for Job' (Morton, 1993). The former category covers officers undertaking deviant practice for their own personal gain, which may include accepting free gifts (aligned to Knapp's' Grass-eating) to bribery, or extortion (meat-eating), the defining characteristic, being the motivation of personal gain. This is consistent with the early definition of corruption provided by McMullan, as it comfortably excludes any noble cause activity, and again supports Kleinig's motivational view. The latter category, 'Bent for Job' covers acts or omissions, primarily motivated by noble cause corruption, in the interests of obtaining a conviction at any costs. This second category links neatly with Punch's 'Dirty Harrys' and 'Noble Causers' types.

Whilst the literature provides a number of different typologies for corrupt acts and officers, these must be seen against the backdrop of the overall causes of corruption. Of the different types and typologies examined most notable for this research is that provided to the Knapp commission in 1972. In defining types of officers (Grass eaters

/ Meat eaters and Birds) it is possible to categorise not only the activities undertaken, but also the motivations, and by extension, the factors impacting on the decision to undertake the activity. This lends itself to the specific area of study in this research. It is therefore now useful to move on to examine ideas on how or why officers undertake corrupt acts.

The Causes of Corruption

The academic literature in relation to the causes of corruption is varied but appears to a certain extent to be consistent. The earliest of relevance to this paper is Stoddard's 1968 work[45] where he interviews a lone informant involved in police mal-practice. In this, Stoddard discusses three possible contributing factors. Firstly there is comment on the *"public expectations placed upon officers who have invariably been drawn from the same public group". (Stoddard, 1968. p202).* Here Stoddard appears to suggest that corruption practice is actually a norm and is only seen as deviant in the paradigm of law enforcement. It therefore follows that if correct, there need be no further search for the cause of police corruption, as it is in effect a natural state, but only placed under a public microscope by circumstance. Whilst it is considered in the paper, Stoddard does not advance this idea but moves on to the suggestion that another contributing factor is that of impotence to carry out official duties; *"While he is responsible to protect the members of his society from those who would do them harm, the corresponding powers for carrying out this mandate are not delegated. To perform his designated duties, the conscientious policeman often must violate the very*

[45] The author again acknowledges that this was based on only one interview subject.

laws he is trying to enforce" (Stoddard, 1968. p202). This appears to be an early allusion to noble cause corruption, which does not appear to feature until the early 1980s in other literature.

The final area Stoddard puts forward as contributory is that of the prevailing culture of existing corruption, whereby 'old-timers' urged new recruits into established corrupt practices with consequences for failing to take part; *"If the recruit cooperated the practices were extended and the rookie became involved ... However those who were straight-laced and wanted to stay honest had their problems too, social isolation appears to be a powerful sanction ..." (Stoddard, 1968. p 209).* This would tend to advance the idea of group acceptance, which as Stoddard recognises from previous research is a powerful incentive for deviant behaviour. Interestingly the study makes mention of one factor, which is almost immediately dismissed, that of money. On being asked directly whether illegal activities are necessary to supplement an officer's income, Stoddard's informant responds, *"I don't think this is the case. I don't think there are many policemen that I knew, and I knew all of them, that were social climbers or that tried to keep up with the Jones, by illegal activities anyway" ('Smith' in Stoddard, 1968. p 210).* The author highlights here however his view that financial motivation is likely to be dependent on external factors such as pay and conditions and relative standards of living in specific eras and locations. The perception of one research subject in the 1960's may not bear relevance to the modern day.

Some six years later, Lawrence Sherman's 1974 study looks at two categories of contributing influences in police corruption cases. The first of these he labels 'Constant Features' or those aspects of policing which are always present and that

have a potential to impact on corruption propensity. The second category, 'Variable Features', which although not always present, are characteristic of policing and may exist to greater or lesser extents depending on role or department. (Sherman, 1974). Whilst Sherman's original paper provides the skeleton for the concept of constant and variable factors, Newburn's 1999 review provides an excellent commentary of how other authors have supported this idea and how their ideas on the causes of police corruption can fit neatly into this framework.

Table 4- Sherman's constant and variable features

Sherman's Constant Features	Sherman's Variable Features
Discretion	*Community Structure*
Low Managerial visibility	*Organisational Characteristics*
Low Public visibility	*Legal Opportunities*
Peer group & Managerial Secrecy	*Corruption Controls*
Status Problems	*Social organisation of corruption*
Association with lawbreakers	*Moral cynicism*

(Adapted from Sherman 1974 in Newburn 1999. p17)

Of the constant features Sherman argues that discretion has both legitimate and illegitimate bases. For example it may be used to overlook minor criminal violations for gain or legitimately it may be used to prioritise enforcement. Herman Goldstein in his 1975 paper argues that discretion is essential to effective policing but acknowledges that *"Police officers are expected to operate in a manner that is in clear contrast to the formal provisions governing their duties"* (Goldstein, 1975. p26), and as Newburn elaborates, where the ethos of policing is to enforce all laws, this is clearly impractical and requires prioritisation through discretion.

The idea of low managerial visibility notes that policing is often a remote activity with little hands on supervision. Police officers are often 'spread out' in order to undertake

their functions which provides the opportunity for mal-practice. (Newburn, 1999). In addition it has been argued that whilst espousing the necessity to stay within the rules, some senior officers celebrate success even where the rules appear to have been broken. (*Punch, 1994 in Newburn 1999. p18*).

Low public visibility relates to the amount of police work that is undertaken outside the view of society. In addition as Newburn notes, *"The police have considerable access to 'private spaces, where they cannot be observed at all' (Newburn, 1999. p19).* This relates to work undertaken in police stations, laboratories, interview rooms, and other places where crucial decisions and actions are taken which directly impact on the criminal justice system, but are often outside the view of anyone but the officers concerned.

Here the author has grouped 'peer group' and 'managerial secrecy' together although in Stoddard's original work they formed two separate categories. The two are however intrinsically linked. Of the former many authors have commented on the code of silence that bonds police officers and has been described as a *'blue curtain of secrecy', (Sherman, 1978 in Newburn, 1999)* and *"A protective armour shielding the force as a whole from public knowledge or infarctions" (Reiner, R, 2000. p122).* Stoddard's 1968 work also supports the idea of a code of silence to achieve acceptance within the group. As officers are promoted this secrecy appears to be taken with them and it has been argued that it is this that makes them *"wilfully blind supervisors who fear the consequences of a corruption scandal more than the corruption itself" (Mollen Commission, 1994 in Newburn, 1999. p20).*

Status problems are outlined in Newburn's paper with the suggestion that *"police officers are sometimes said to be poorly paid relative to their powers."* (Newburn, 1999. p17). Whilst this is shown as a constant factor by Sherman, it is contested by Stoddard's findings (Stoddard, 1968) and the author here advances that it would probably better sit as a variable factor, dependent upon the regional cost of living and economic cycles.

The association with criminals is one of the ever present features of policing. This is necessarily encouraged to fulfil the role. As Newburn states, added with other factors such as remote supervision, low visibility and a veil of silence, *"The temptations with which an officer will inevitably come into contact are great."* (Newburn, 1999. p21).

Of the variable factors, the first outlined by Sherman is that of Community Structure. By this he explains that he predominantly means the political environment, however he acknowledges that certain business communities have a vested interest in maximising police presence and reinforcing positive relations with the police.

To Sherman the organisational characteristics of an organisation included the morale of officers. His view is reinforced by the findings of the Australian Wood Commission into police reform of 1997. Their report maintains that there is a strong link between the absence of professional pride and the development of corruption. (The Wood Commission, 1997)

Sherman's 1978 study outlines that whilst corruption in forces has touched on a number of different criminal activities areas such as prostitution, alcohol and gambling have always been the main contributors. It is these 'illegal pleasures' that Sherman

categorises as his 'legal opportunities for corruption' with laws that are often unenforced, do not command universal acceptance and provide a high cash turnover. (Newburn, 1999)

The existence of corruption controls as a variable factor is clear and straightforward. Within these however he includes social controls both within and outside of an organisation. *(Sherman, 1978)*, and in so doing he overlaps with his 'social organisation' factor. Here he argues that as corrupt practices become more regularised they should become easier to detect and susceptible to challenge. He acknowledges however that this is dependent on the means and will to engage in detection activities.

The last of Sherman's variable factors is that of 'moral cynicism'. The idea is supported by Kleinig's 1996 work where he suggests repeated exposure to wrongdoing, particularly in people previously seen as honest serves to weaken the moral constraints that should guide police conduct. He suggests that the criminal justice system itself may also be a source of cynicism resulting in a lack of confidence in official procedures.

Whilst both the constant and variable factors may provide an insight into why officers undertake their first corrupt act, it does not explain fully why some officers progress to become involved in activities deemed more serious than others. Two alternative views have been put forward, firstly by Sherman in his 1985 paper and more recently by Kleinig in 1996. Both Sherman and Kleinig acknowledge corruption as a hierarchy, and this is probably not surprising given the weight of evidence leading to this conclusion *(Barker & Roebuck, 1973; Stoddard, 1968)*. Sherman however advances

that in order to move up the 'ladder' from one level to the next a psychological redefinition of 'self' is required in order to personally justify the corrupt action. Sherman argues that at some point the redefinition required may be so great that an individual would be discouraged from making it, and therefore remain on their current 'rung'. This Sherman refers to as the moral career of a police officer. *(Sherman, 1985).*

Kleinig by contrast in his 1996 work puts forward the 'slippery slope' argument in that once one type of deviant activity is undertaken, the moral grounds for not moving to the next are undermined; as both acts are illegitimate, and lacking any moral objection to move to the more serious one, it should be seen as a natural progression. (Kleinig, 1996). This distinction between Sherman and Kleinig is important as by the former small gratuities and gifts to police officers runs only a limited risk of climbing a ladder to further corruption. By the latter however even the smallest gift or gratuity has not only the potential, but the likelihood to lead to hard-core corruption. (Newburn, 1999).

Perhaps one of the most common analogies to police corruption is that of the 'bad apple' in an otherwise 'healthy barrel'. This has been put forward on many occasions by a number of forces in defence of allegations of widespread corruption when individual officers are identified as corrupt. *(Punch, 1994; Knapp, 1972)* Doubtless the purpose of such an analogy is to distance an organisation from the suggestion of endemic corruption by the public condemnation of one or a small numbers of its members. Maurice Punch, in his 2009 work examines the analogy in more detail and concludes that the lone 'bad apple' is no longer a credible position. Instead Punch advances that propensity to corruption is an organisational issue, and that *"bent cops'*

are not born but are predominantly made by the culture, the work and the institutional context" (Punch, 2009. P48). In a far reaching and assertive statement he goes on to advance *"The police organisation is to 'blame' for much corruption; it has failed to see it, to prevent it, to control it and to stop segments of the organisation entering recidivism" (Punch, 2009. p48).* This position is very much in keeping with Sherman's 'constant and variable factors' and whereas the analogy may start with a 'bad apple', Punch expands this to talk of rotten orchards, and pushes the cause of police corruption firmly back into the policing arena in asking *"whose duty was it to inspect the fruit and who neglected to apply the insecticide?" (Punch, 2009. p9)*

Whilst academic papers provide the majority of material on the causes of corruption, evidence and findings from organisational reviews are valuable if only to reinforce other work. The 1972 Knapp commission heard substantial evidence from the police union that *"police corruption was confined to a few rotten apples in an otherwise healthy barrel" (Knapp Commission in Newburn, 1999. p14).* This position was firmly rejected by Judge Knapp in his statement "*According to this theory, which bordered on official Department doctrine, any policeman found to be corrupt must promptly be denounced as a rotten apple in an otherwise clean barrel. It must never be admitted that his individual corruption may be symptomatic of underlying disease..." (Knapp, 1972 in Newburn 1999. p15).* Knapp's view was in turn reinforced by the Subsequent Police Commissioner charged with reform maintaining that *"The 'rotten apple' theory won't work any longer. Corrupt police officers are not natural-born criminals, nor morally wicked men, constitutionally different from their honest colleagues. The task of corruption control is to examine the barrel, not just the apples – the organisation,*

not just the individuals in it – because corrupt police are made, not born." (Murphy, P, 1972 quoted in Barker and Carter, 1986: 10 in Newburn 1999. P15). This is clearly in keeping with the later findings and assertions of Punch.

Her Majesty's' inspectorate of Constabulary's 1999 review, whilst not going into the same depth of the causes of police corruption provides one insight into its views; "*It is self-evident that every police officer and member of support staff should behave professionally, courteously and impartially to members of the public and colleagues alike. It is a sad fact, however, that during 1997 well over 6,000 complaints of alleged rudeness and incivility were recorded. How police officers behave is very much a matter of personal integrity and in an environment where bullying, arrogance, rudeness, racist or sexist behaviour is tolerated, corruption and other wrongdoing will flourish, and is more likely to remain unreported.*"(HMIC, 1999, p9). Whilst this assertion appears to support Kleinig's view of a hierarchy and slippery slope, there is no supporting evidence in the report to substantiate the claim.

Of the journalistic material available, the vast majority concentrates on the activities of officers and attempts to uncover deviant practices. One however is particularly useful in outlining the causes of corruption; Graeme McLagan's 2003 book 'Bent Coppers'. In this he interviews a former corrupt detective who having been charged with criminal offences became a supergrass. The officer relates how, having started work at his new department in South East London, he was approached by a colleague; *"He was asking me if I had any debts and things like that. I said I had credit cards and I owed money on them. And he very blatantly turned around and said 'Well don't worry about that. A few months here and we'll have all your debts cleared. You won't have*

any debts and you'll have money" (Putman, N in McLagan, 2003, p252). The statement encapsulates the sentiment of Punch's work in that corrupt cops are made by their environment, but the officer goes further; *"There was no way out, I was in it up to my neck"*[46] *(Putman, N in McLagan, 2003, p252)*, thereby supporting Kleinig's view on the slippery slope and the difficulty in turning back.

Having considered the issue of police corruption the author now moves in the next chapter to the second part of the literary review, considering in particular the area of computer misuse.

[46] Putman explains that having become part of the corrupt group the peer group pressure to continue was immense and that he could not back out as this would cause the group to consider him unreliable and turn against him, and this would undoubtedly have led to his own arrest and prosecution with the testimony of a number of officers against his own

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 3
Literary Review (Part 2)
Computer Misuse

Overview

The issue of computer misuse is rather more contemporary than police corruption generically, as the means for such conduct is confined to the last twenty or thirty years. Whilst there exists a similar three way split for sources in this area, it is fair to say that the journalistic or media material is, for the greater part, science fiction based and therefore of very limited use in this work other than to provide the Hollywood perception of the average computer hacker as *"a disenfranchised, misunderstood genius teenage male who uses technology to put wrongs right whilst having a 'coming of age' experience and possibly some fun in the process"* (Wall, 2008. p864). The two other sources in this area are existing academic work, and legislative reports either as acts of parliament or reporting on appeals or stated cases. In the second part of this literary review the author seeks to examine computer misuse in the same way as he has dealt with police corruption, by considering three particular areas; defining computer misuse, types and typologies of computer misuse and finally the causes of such activity.

Defining Computer Misuse

In 1990 the UK Government passed what is regarded as the first piece of bespoke legislation in relation to computer misuse. The Computer Misuse Act 1990 creates a number of offences; Section 1 of the Act creates an offence for any person to cause a computer to perform any function with intent to secure access to any program or data held in any computer without authority.[47] Section 2 of the Act expands the earlier provision by creating a further offence if the access is sought to facilitate the commission of further offences and section 3 of the Act creates a separate offence of impairing the operation of a computer system without authority.

It can be seen therefore that for 'black letter law' the definition of computer misuse is wide and can incorporate just about any unauthorised activity in relation to a computer system. It is fair to say however that such a wide definition has not been without controversy. The Act was first tested in July 1990 in R v Cropp[48], whereby charges were brought against a former employee of a store, when partway through a checkout process, he distracted the assistant with a store room enquiry long enough for him to enter a 70% discount code into the till. The result of this was a final bill of £204 rather than £710. In criminal proceedings his Honour Judge Aglionby held that the Act had not been breached, as in his view, it applied to the use of one computer to influence the function of another. As in this case there was only one computer used, the defendant was therefore not guilty of the offence. Following appeal by the Attorney General, Judge Aglionby's interpretation was overturned by Lord Taylor CJ. who effectively provided an interpretation which amended section 1 of the act to the

[47] Whilst Data Protection Acts were passed in 1984 and 1988 these related to the registering of databases and data users rather than providing specific protection against computer misuse

[48] Unreported but cited in Fafinksi, 2008: Computer Use and Misuse. Pp 58-59

effect that it was *"an offence for any person to cause a computer to perform any function with intent to secure access to any program or data held in any computer (including itself) without authority."* (Fafinski, 2008. p59)

A second challenge to the Act came in 1998 when two police officers, a husband and wife, instructed a third party computer operator to access the Police National Computer to obtain the owner details of two cars parked outside the house of the male officer's ex-wife. Whilst both were convicted in the first instance of the Section 1 offence, on appeal their convictions were quashed as his Honour Judge Anstill held that the officers had not obtained unauthorised access to the system, in that they were authorised to use the system albeit for a different purpose.[49] This finding effectively protected those acting without a legitimate purpose provided they only used systems that they were authorised to use albeit for a different purpose. This position stood until a House of Lords ruling in 2000 when Lord Hobhouse disapproved the findings of Judge Anstill and created a distinction between *specific* data on a computer system and *any* data on a computer system. (Fafinski, 2008).

It can be seen therefore that despite challenges to a very wide and all-encompassing piece of legislation it remains fairly intact, with interpretation and rulings reinforcing the inclusive nature of the provisions. For the UK legislature therefore, computer misuse can be realistically summed up as any unauthorised activity with a computer.

In the academic arena there are a number of researchers who have carried out work specific to computer misuse.[50] Three views of particular note in defining computer

[49] DPP v Bignall 1998.cited in Fafinksi, 2008: Computer Use and Misuse. Pp 59-60
[50] (Sacco & Zureik, 1990), (Kerr, 2003) (Kesar & Rogerson, 1998) (Herath & Wijayanayake, 2009)

misuse for the purpose of this research, are those of Professor David Wall, Dr Stefan Fafinski and Professor Martin Wasik.

In a definition most aligned to that of the legislation, Wasik defines computer misuse as *"unethical or unauthorised behaviour in relation to the use of computers, programs or data"* (Wasik, 1991. p3). This wide definition provided after the Computer Misusue Act but before legal testing in the higher courts, seems to have stood the test of time, and remains a good representation of what appears to be the spirit of the Act. In a later work whilst maintaining this position Wasik also makes specific comment as to the misuse of computers by public servants, a point particularly relevant to this research. In this work he notes the appeals and counter judgements made in relation to the Computer Misuse Act and highlights the potential for the common law offence of *'Misconduct in public office'* as an alternative to the 'black letter law'; *"The offence of misconduct in public office has been used successfully against police officers in a very wide range of factual circumstances. It has been used relatively frequently in relation to police misuse of police computers." (Wasik, 2008. p 135).*

In Fafinski's 2008 work he focuses primarily on the utility of the computer misuse legislation and therefore perhaps unsurprisingly arrives at a fairly wide definition, stating; *"Although computer misuse may be framed in terms of unauthorised or unethical use of technology, this definition remains both technologically and socially relative. That is, what is unauthorised or unethical depends on the nature and capability of the technology itself as well as the collective viewpoint of its users". (Fafinksi, 2008. p274)*

Here it is possible to see the influence of the legislation in the nature of Fafinski's definition but also his own interpretation around the nature of the technology and what is deemed acceptable by other users.

In contrast to Fafinski's research, Wall in his 2007 journal article (revised 2010) avoids the term computer misuse in favour of the term 'Cybercrime'. It can however be seen that he is broadly talking about the same issue as in the latter parts of his work he refers to Computer Misuse and UK legislative provisions to tackle it. *(Wall, 2007: Revised 2011).*

Wall does not start his work by providing a traditional definition of cybercrime or computer misuse but by stating a number of characteristics by which it may be recognised; *"Since cybercrimes are the product of networked computers, they must be defined in terms of the informational, networked, [...] criminal behaviour". (Wall, 2007: Revised 2011. p.185)* By framing his parameters in this way Wall allows others to determine the scope of his definition by either including or excluding activities depending on interpretation. The importance of this becomes clearer as one examines the challenges that he outlines to the policing of cybercrime.

The first problem Wall outlines in policing cybercrime is that of jurisdictional boundaries. Police forces within the UK work to geographic boundaries and are used to dealing with crimes which occur within their area. Whilst the impact of cybercrime may be felt within a particular physical area, they are often committed elsewhere and this may even be within a virtual environment in the case of automated activity. Wall does note however, that many forces have now created specialist units to deal with

this type of crime and have developed protocols as to who should deal with crimes committed in the virtual world. *(Wall, 2007: Revised 2011. p. 192).*

Secondly Wall highlights the legal issue of 'De-minimis'[51] in that a vast number of cybercrimes are of such little impact that they do not attract sufficient public interest to warrant police resources to investigate.[52] Here again it is possible to see the overlap between Wall's 'cybercrime' and previous definitions of 'computer misuse', as unauthorised access to a system with no further use of the information gained is likely to fall within the realm of *'de minimis'*.

As a further issue Wall examines police culture and its conservative nature as a barrier to investigating cybercrime. He highlights findings from other researchers that police shy away from new and advancing technology with a fear of risk and vulnerability, in favour of traditional knowledge and experience *(Reiner 2000, in Wall 2007, Revised 2011).* As a result of this many cybercrimes go unrecorded or investigated due to the view held by many officers that *"cyberspace is like a neighbourhood without a police department" (Sussman, 1995, p.59 in Wall, 2007. p193).*

Whilst the academic literature provides differing perspectives on a definition of computer misuse, the author is of the view that for the greater part, these reflect the legislative framework of the Computer Misuse Act 1990. For the purpose of this work therefore it is this wide ranging definition used as the basis for research.

[51] 'De-minimis non curat lex' – *The law does not deal with trifles.*
[52] In addition to the public interest in the application of police resources, public interest is also further examined in the event that a case is referred to the Crown Prosecution Service for a prosecution decision.

Types and Typologies

As with defining computer crime, the two principle contributions to typologies come from government and academia. The governmental work in this field is however limited to a small number of conferences and protocols, the most significant of which is the 2001 European Convention on Cybercrime[53]. In a review of the implications of this conference, Profession Marco Gercke relates that member states agreed a distinction between four types of computer crime; offences against confidentiality, computer related offences, content related offences and copyright related offences[54] (Gercke, 2011). The first of these categories relates to access to computer systems and security of the information stored within them. It is this category that bears particular relevance to this research as it relates to the content of databases and protection from unauthorised access and disclosure, and whilst the UK government had already passed domestic legislation to support it,[55] the protocol agreed at this conference required all member states to implement such domestic laws.

The second category, that of content related offences relates to the accuracy of information stored on electronic databases, whilst the third relates primarily to illegal pornography. The final category creates provision to protect owners of copyright. The inclusion of copyright within this protocol, which at first view appears particularly specific in an otherwise broad ranging agreement, provides some insight into the importance to governments of this issue over and above others. This is commented upon by Professor Lawrence Lessig of Stanford University in his assertion that "*Policy*

[53] December 2001, Budapest

[54] The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at:http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[55] The Computer Misuse Act 1990

makers have so far shown themselves to be consistently stupid and bribable, how else can one explain the curious hierarchy of their priorities, online copyrights come at the top due to the powerful lobbying of music companies ... near the bottom comes the online privacy of millions of consumers". (Lessig: Pattavania, 2005 p23).

In a separate legislative contribution to computer misuse typology Dr Stefan Fafinski , in his 2008, thesis examines the Scottish Law Commission's response to a consultative document on the applicability of current legislation to computer offences. The response highlighted eight areas of computer misuse;[56]

- Erasure or falsification of data or programs so as to obtain a pecuniary or other advantage;
- Obtaining unauthorised access to a computer;
- Eavesdropping on a computer;
- Taking of information without physical removal;
- Unauthorised borrowing of computer discs or tapes;
- Making unauthorised use of computer time or facilities;
- Malicious or reckless corruption or erasure of data or programs;
- Denial of access to authorised users.

This typology is significant as it highlights a number of issues but generally reflects the overall ethos of the subsequent UK legislation in its wide scope. Of particular relevance to this research are issues of 'obtaining unauthorised access to a computer' and 'taking of information without physical removal'. The distinction between these

[56] Adapted from Scottish Law Commission, 'Computer Crime' (Consultative Memorandum No. 68,1986). In Fafinski 2008.

two acts would tend to suggest that the mere act of unauthorised use, whether or not it is with any information gathering motive, represents computer misuse and so here, for the first time a motivational distinction is visible, dependent upon the purpose of the computer misuse.

Whilst the limit of usefulness of governmental typologies may be only to reinforce the definitions already examined, as well as to perhaps provide some insight into computer crime priorities at that level, a far greater insight is provided by academic theory. In the academic arena the work of David Wall is again significant and provides two typologies of cybercrime. In the first of these, Wall introduces the idea of three generations of cybercrime with different characteristics depending on the utility of the computer.

Table 5- Typology Computer Crimes by David Wall

Generation	Characteristics
1st Generation	Traditional crimes which computers have been used for information gathering or communication to assist with the organisation of the crime. Remove the computer and the crime persists because the offenders will revert to using other information, sources or types of communication.
2nd Generation	Traditional crimes for which entirely new global opportunities have emerged (e.g. globalised fraud and deceptions). Take away the computer and the crimes will continue but not by the same volume or across such a wide span
3rd Generation	'True Cybercrimes' which are solely the product of opportunities created by the internet and which can only be perpetrated within cyberspace such as online intellectual property thefts.

(Adapted from Wall 2007, revised 2010)

From this typology it is clear that Wall draws a distinction between crimes that require a computer in order to be committed (3rd generation), crimes which have become more sophisticated due to computers (2nd generation), and crimes which have become easier to arrange due to computers (1st generation). This distinction is important in relation to computer misuse by police officers as it begins to involve the 'purpose of misuse' rather than just the act itself, and has the potential to categorise at an early stage certain types of activity. The distinction between the three types is also significant as it demonstrates the chronology of how cybercrime has developed. In the '1st generation', in the early 1980s networked computer systems were few and far between, but stand-alone systems could be used in planning crimes. In the '2nd generation', the 1990s, the rise of the World Wide Web, meant that communication became quicker and easier and a cyber-criminal could reach many more potential victims than had previously been within his scope. Finally as the internet spread to become a global network, Wall's 3rd generation came into being with the realisation *"that Information [or material] legally made available in one country was available globally, even in countries where publication of such information [or material] was criminalised". (Gercke, 2011. p34).* Even more importantly than a chronological perspective, Wall's work demonstrates the social movement towards computer misuse. This is particular relevant to this research as it highlights that police computer misuse does not occur in the vacuum of police culture, but it is a social phenomenon that has developed over a number of decades, and has adapted in line with new opportunities.

As a second typology in the same 2007 work Wall outlines his ideas of 'crimes against machines', 'crimes using machines' and 'crimes in the machine'. The former he describes as assaults on the integrity of machines, such as hacking, vandalism, spying and denial of service attacks. 'Crimes using machines' Wall states, relates to computers being used to engage with victims in order to dishonestly acquire goods or cash, whilst his 'crimes in the machine' relate to the computer content crimes such as the distribution of prohibited pornography. *(Wall, 2007 revised Feb. 2011).* This second typology overlaps somewhat his initial typology with 'crimes using machines' neatly covering 1st and 2nd generation cybercrimes, and 'crimes in the machine' relating to his previously explored 3rd generation.

The new area outlined here relates to 'crimes against the machine' such as hacking, vandalism and spying. The motivations for both vandalism and spying are implicitly to either cause damage or to gain information for some other purpose, hacking however carries no such implicit motivation and may be done for no other reason than self-satisfaction of defeating security systems and gaining access to restricted information. Whilst motivation therefore is considered in legislative typologies, it does not appear to feature highly within academic work.

It is apparent that there is some overlap between the typologies examined when considering computer crime generically. It is therefore useful to consider the specific issue of computer misuse by police officers against the backdrop of the typologies reviewed. For the greater part, misuse by police employees can be characterised as either 'unauthorised access to a computer' or the 'taking of information without physical removal' (both from the Scottish Law Commission work), and at the same

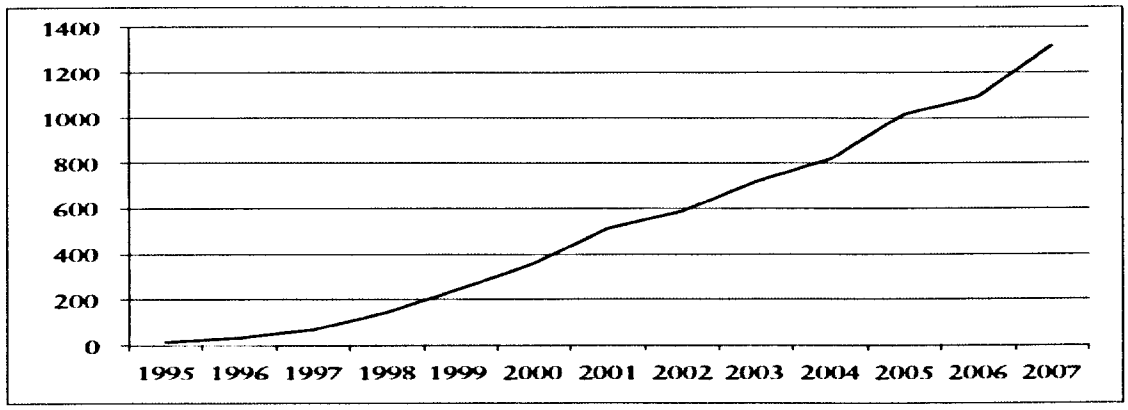
time a 'crime against a machine' (Wall, 2007) where unauthorised access is made to gain information, or a 'crime using a machine' (Wall, 2007) where the object is some other offence such as disruption of a criminal process by the accessing and disclosure or deletion of files. It would appear therefore, that to place a particular act of computer misuse within a typology motivation is all important. Activity with no motivation other than simple access may well fall within the 'unauthorised access' and 'crime against the machine' typology, whereas further use of the information obtained is likely to be categorised as the 'taking of information' and a 'crime using a machine'. This issue of motivation is significant within this research as it recurs in the majority of subject interviews. It is discussed in more detail within chapter 6.

The causes of Computer misuse

The causes of computer misuse have been examined by a number of academic works and generally the rise of computer misuse can be reasonably aligned to two factors; Firstly the rise of the use of the internet, and secondly social evolution and construction of what constitutes acceptable behaviour and activity in computer use. In Fafinski's 2008 work he produces two graphs demonstrating the first of these ideas. These have been reproduced below.

The first graph shows the increase in internet usage from 1995.

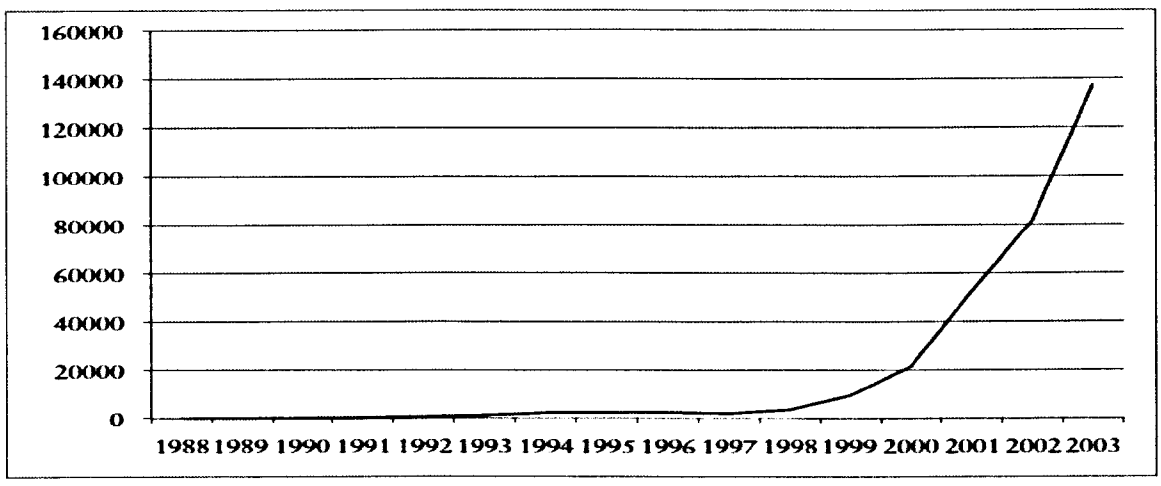
Figure 1.- World Internet usage (millions (1995-2007)



(Reproduced from Fafinski 2008, Pp 52.)

The second shows the number of incidents reported to the UK Computer Emergency Response Team (CERT)[57] between 1988 and 2003.

Figure 2.- Incident Reports received by CERT 1988-2003



(Reproduced from Fafinski 2008, Pp 54.)

These graphs clearly show that prior to 1995 there were few internet users and a negligible number of CERT reports made. As internet usage grew from 1997 onwards

[57] The CERT collects statistical information on security vulnerabilities which may render computers susceptible as targets of misuse. These statistics are compiled from reliable public sources and incidents notified direct to CERT. (Fafinski, 2008)

the number of reports increased significantly. It is therefore reasonable to argue a correlation here if only through ease of access and familiarity with the internet itself.

Ease of access alone however, cannot explain the increase of computer misuse and so it is necessary to look further. Additional insight is provided in part by David Wall in his 2008 work in which he examines a number of factors which appear to have become part of the general social paradigm of internet and computer usage. Whilst these may in many cases be myths, they are deep entrenched and form part of society's perception when dealing with computers. These perceptions, he argues, have built up from reports in the media, the film industry and in some cases ill-conceived government statements[58]

Of significance Wall maintains there are three ideas in particular which have attracted people to cybercrime as opposed to traditional forms of offending;

- Criminals are anonymous and cannot be tracked.
- Criminals go unpunished and get away with crime.
- Users are weak and therefore need protection from themselves.

Whilst Wall is able to unpick and demonstrate the mythology surrounding each one in turn, the important point here is the public perception under which criminals labour when undertaking computer misuse. For Wall therefore a significant factor in the rise of computer misuse is the mythology surrounding it and the general perception of vulnerability of victims and anonymity of perpetrators.

[58] In particular Wall cites a House of Lords report form 2007 adding weight to the mythology that has arisen around the internet. (House of Lords 2007, Pp6 in Wall 2008 Pp868)

Additionally Wall cites the modern culture created by the internet and the general expectation of a right to internet usage like any other utility. *"The internet's global reach, combined with its easy accessibility, made the information generation feel different, - as though they were all hackers. It made them feel free to explore, to roam freely, see and experience new things in what seemed to be a new public commons"* (Wall, 2008. p876). This point is significant because if what Wall maintains is correct, then the information generation, assume a right to use the internet to explore, to play and to experiment, without boundaries and without any understanding of legal limits on what is or is not permitted from the computer in the bedroom.

Further work into the causes of computer misuse has been conducted by Vincent Sacco and Elia Zureik, in their 1990 publication. Whilst this study focused on computer piracy and not computer misuse generically their findings remain of relevance. In particular, they identified that 62% of respondents acknowledged making illegal copies of software, with interviewees also stating *"they believed that a great deal of copying was going on and that the likelihood of detection (getting caught) was very low." (Sacco and Zureik, 1990,: Salahnia 2002, p 122).*

Additional ideas are presented by William Swinyard (*et al*), who advance that before undertaking piracy, subjects weigh up the outcomes or benefits against the potential legal concerns and decide that the risk is worth taking. *(Swinyard, Rinne and Kau , 1990)*[59]. This view is slightly contrary to the findings of Jim Im and Pamela Van Epps in their 1992 analysis of computer piracy in business schools. In this they conclude that a

[59] The research by Sacco and Zureik, and Swinyard, Rinne and Kau related solely to computer software piracy and whilst some insight is provided as to the causes the results are not directly transferable to police computer misuse, as neither a position of trust, nor employment consequences for offenders exist.

solution is to be found in *"educating employees in what is and is not acceptable behaviour" (Im & Van Epps, 1992: Salahnia 2002, p 122)*, thereby indicating that a lack of awareness features in the decision making process to undertake piracy.

A final and more generic piece of work in relation not to causes of criminal conduct, but how those responsible justify their actions is the celebrated work of Gresham Sykes and David Matza in the 1957 'Techniques for Neutralisation'. Whilst this work does not relate specifically to computer misuse[60], it is possible to see some of their ideas reflected in both the responses given to other researchers in previous studies[61] as well as by interview subjects in this work. In their work Sykes and Matza identify five techniques used by those undertaking deviant practice to either self-justify or justify to others their actions. These consist of;

- Denial of responsibility.
- Denial of injury.
- Denial of victim.
- Condemnation of the condemners.
- Appeal to higher loyalties.

(Sykes & Matza, 1957)

Sykes and Matza found that typical responses from subjects could be summed up as; *'It wasn't my fault'*, (Denial of responsibility), *'There was no harm done, they can afford it'* (denial of injury), *'They deserved it, or had it coming to them'* (Denial of victim), *'They probably did worse things in their day'* (Condemnation of the condemners) and *'My friends were depending on me, what else could I do?'* (Appeal to higher loyalties).

[60] The date of the work places it some time before the idea of computer misuse became an issue.
[61] Sacco & Zuriek 1990 , Swinyard Rinne and Kau 1990, Im & Van Epps 1992

The findings of Matza and Sykes are evident in some of the interview responses in this research and of particular note are the notions of;

- Denial of responsibility where subjects often advanced that they were unaware of the limitations of legitimate computer use and so therefore had no idea that they were breaching the regulations.
- Denial of injury whereby subjects maintained that they only looked at information for their own curiosity and it was never passed on and no harm was done.
- Appeal to higher loyalties whereby the objective of the computer misuse was the protection of friends or family.

In summary therefore, there is evidence that the rise of computer misuse is inextricably linked to both the rise of computer use and the social construction of accepted norms as to expectations of computer use. This may seem an obvious fact, but by overlaying a prevailing mythology in relation to risk of being caught and the vulnerability of victims, along with a new generation who see the virtual world as an extension to the physical world, the environment for cybercrime or computer misuse is created.

Having reviewed a number of literary sources the author has reflected on two main areas relevant to the thesis: Firstly, and perhaps most importantly the area of police corruption, by examining the disputed territory of a definition of police corruption itself; different types of corruption and its causes. Secondly, the author has looked at computer misuse and considered what it is, different ways in which it can be undertaken and the causes of such criminality. Having considered these points and

outlined the existing research in these two areas, the review now provides a springboard to a methodology specific to this research and enables later findings to be discussed and considered in the light of existing academic theory.

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 4
Methodology

Overview

Having examined the existing literature in the arena of police corruption, the author now turns to the specific research methodology used in this piece of work. This chapter initially serves to outline the working parameters that were used in the research, and explain why these were chosen rather than others. It also provides a reflection of the specific research limits against the backdrop of the literature previously discussed. Having explained the working arena in which the research took place, the author discusses his personal qualifications for undertaking this project and how these may have assisted or indeed hindered both the data collection and analysis. The chapter moves on to consider the decision making process used to determine the data collection methods used and discusses competing strengths and weaknesses between the soft paradigm of qualitative data and the hard paradigm of the quantitative arena before detailing the exact method of data collection used. Having discussed the methods of data collection employed, by way of conclusion, the author summarises the research phase of this project and outlines the ethical considerations, along with safeguards put in place to overcome these.

Working Parameters

The aim of this research is to provide an analysis of the contributing factors which impact on a police officer undertaking deviant practice. It is hoped that by application of the resultant findings and conclusions, police services and other law enforcement agencies will be in a stronger position to undertake future corruption investigations and more importantly to prevent future corruption.

As has been previously discussed, the boundaries of police corruption are wide and to attempt to examine all aspects would be not only time prohibitive, but runs the risk of being so disparate that meaningful findings and conclusions are difficult to draw. It is also notable that from the existing literature available, such an exercise is probably unnecessary as the idea has been successfully advanced that corruption in this area forms a hierarchy and either a slippery slope or an attractive ladder. (Barker & Roebuck, 1973; Kleinig, 1996; Sherman, 1985).

Having considered a number of factors, the author decided to focus on police officers who had inappropriately accessed or disseminated information from police computer systems, specifically excluding any individual who had entered the organisation with the specific intent of corrupt practice.[62]

This decision was made against the backdrop of the author's perception[63] of such activity in terms of associated stigma or emotion involved in the act itself, level or seriousness of a criminal act, innovation in terms of originality or recent evolution of

[62] This type of corruption, where an individual joins the organisation of their own volition or at the direction of a third party with the specific intent of undermining law enforcement activities is commonly referred to as 'infiltration'. This activity is specifically excluded from this research which focus on the factors impacting on those who joined for legitimate reasons.

[63] The author acknowledges that that the perception used here was his own, based on his experience in the policing environment and previous anti-corruption work.

the act, and availability and ease of data collection. The stigma or emotion involved in an act bears relevance to the ease of identification of data collection subjects. Acts which carry a high stigma[64] value are unlikely to provide a ready source of subjects. Corrupt acts consisting of serious criminal offences pose other difficulties both ethically from the perspective that subjects may feel that their conduct is being glorified or even that they may be tempted to reveal further criminality. On a practical level, those recently convicted of serious criminal offences are likely to be serving periods of imprisonment, difficult to reach, and reluctant to cooperate. It has also been argued that serious criminal acts are outside the scope of police corruption (and therefore the hierarchy) and remain purely criminal, even when committed by serving officers. (Wilson, 1963; Stoddard, 1968). In terms of innovation and originality, the author sought to identify new deviant practices emerging in the current social or technological environment. On the basis of these considerations, the inappropriate access or dissemination of police information appears to be a strong research area.

Following the decision in relation to the type of corrupt act the author considered geographic area. The factors in this arena are more straightforward in that the area needed to be sufficiently large to enable data capture, but not so large that cultural differences or even criminal law differences impacted on the very nature of corruption. The area also needed to be sufficiently wide that any findings could be meaningfully applied and not so specific in nature that the opportunity for application

[64] The word 'stigma' is used throughout this work both here in the selection of research parameters and later in questions to interview subjects. For the purpose of this research the term is used to describe any sense of disgrace or shame either on the part of the subject and his or her own perception or on the part of others who know or work alongside the subject as a result of their actions. A Typical manifestation of such stigma maybe reluctance by others to work with a subject or to provide a subject with information that they would otherwise be entitled to, due to a lack of trust.

is negligible. The author therefore decided that the geographic scope of the research would be England. The choice is further enhanced by the fact that the National Policing policies in relation to Anti-Corruption are consistent throughout this area.

In relation to the timescales of the corrupt act, again factors for consideration are reasonably straightforward. The nature of the act means that by definition it has emerged with the rise of new technology, this however only narrows the period to the last 15 to 20 years. Events some time ago are unlikely to be easy to study and individuals are likely to have long left the policing arena and be difficult to trace. This difficulty needed to be considered against the need for a ready number of subjects, and too short a recent period would hinder this. The author therefore decided that a period of three years was acceptable, but with an emphasis on more recent events where possible.

In summary therefore, whilst the findings and conclusion seek to provide an analysis of factors impacting on corruption which are generally applicable, the working parameters for this project are corruption in the form of inappropriate information access or dissemination in England over the previous three years.

The Author

The author is currently serving as a Detective Superintendent in a Home Office police force and has been a police officer for over 20 years. The majority of his service has been spent working in London, but he has spent two periods with provincial forces. During his service he has worked in a variety of roles which have unusually crossed

between both the detective and uniform fields. Of his formal training, he is a nationally accredited Senior Investigating Officer (SIO), Hostage Negotiator, Family Liaison Co-ordinator and Senior Identification Manager (SIM). His practical experience ranges from working as a junior detective on a South London drugs squad focused firmly at the enforcement aspect of class 'A' drug supply, to a middle management position leading a community safety team in Surrey with a remit of increasing public confidence in policing, to his current position as a senior officer working in a Professional Standards Department (PSD).

In 2007, and following the review of police discipline regulations by Lord Taylor, he was appointed project lead for the practical implementation of the proposals for Hertfordshire Constabulary. This allowed him to influence the way in which the force dealt with complaints and misconduct at a practical level, creating structures and processes still in use today.

Following a period overseas, in 2010 he was appointed Head of Professional Standards for both Hertfordshire and Bedfordshire forces and within months Cambridgeshire Police was added to this portfolio. This posting enabled him to work with, and enhance the processes he had designed as original project lead on 2007.

The author's current command includes operational security, security vetting, misconduct, IT Security, as well as a covert anti-corruption team working undercover to identify malpractice within the three forces. Within his peer group the author currently chairs the Eastern Region's Anti-Corruption Advisory Group, as well as sitting on the 'ACPO National Counter Corruption Group', where he is the national lead for data and computer misuse.

In relation to this specific area of research, the author is uniquely placed to gain access to key individuals within the police anti-corruption arena. He has access to internal documents up to and including those carrying a Government Protective Marking System (GPMS) of Top Secret, and whilst these have not and cannot be disclosed within the work, they have assisted in influencing the direction of study. His position likewise provides access to senior UK officials working within the corruption arena.

Whilst the unique positioning of the author undoubtedly contributes to the ability to conduct the research, he acknowledges his position within the organisation and the potential suggestion that as an insider looking inside[65] the organisation he forms part of the occupational culture he seeks to examine. Likewise, he is conscious of the potential 'intervention effect' of his work whereby the very fact that he is conducting the research could impact on the responses obtained. (Murji, 2011 and Brown, 1996). The author does however, advance that this is significantly mitigated by his role within the Professional Standards Department, which due to the nature of its work, is partitioned both physically and culturally away from the organisation as a whole. Officers working within such a department are vetted to a high level and intrusive enquiries made into their professional, private and financial affairs. It is fair to say that due to the police culture generally, such departments are not easily integrated into the main force, and where there does exist evidence of this it is almost exclusively in the area of complaints against police rather than anti-corruption.

[65] The concept of four observational positions has been advanced by Jennifer Brown in the 1996 publication 'Police Research: Some Critical Issues'. In this she outlines 'inside insiders', (in house researchers), 'outside insiders' (former police officers undertaking research), 'Inside outsiders', (Professional researchers working within the police) and 'outside outsiders', (academics researching the police) (Brown, 1996)

The author also acknowledges the existence of a power relationship between himself and potential interview subjects. In some cases these may be police officers holding a rank junior to his own, and in other cases, these may be former employees who have been subject to previous investigations by other Professional Standards Departments. The risks here are mitigated in that serving officers involved in this research will either be of a similar rank to the author, representatives of the National Police Federation[66] or officers from forces other than his own. Whilst dealing with former employees the author made it clear that he only wished to discuss activities in relation to the previous conduct investigated, and not anything that may have taken place since that time. In this way he sought to protect himself, the subject, and the integrity of the research.

Ethical Considerations

In an area such as police corruption, a number of ethical considerations present themselves. These generally are specific to different research subjects and their qualifications for being of interest to the project.

In the first instance, and in relation the organisational perspective of police corruption the author has access to a number of sensitive sources ranging from documents that have been produced purely for internal consumption, and never meant for public discussion, through to high profile individuals who may provide personal insights into matters on the expectation of complete confidentiality. Whilst the contents of these documents and discussions may provide some direction for the research, they cannot

[66] The National Police Federation is the statutory body representing officers. Whilst formally it represents officers between the ranks of Constable and Chief Inspector, such is its size (by virtue of the fact that most officers fall within these ranks), it undoubtedly negotiates and influences on behalf of police officers generally. Whilst Officers of the Police Federation are serving police officers in their own right and retain the rank awarded to them by their force, it is generally the case that the rank structure is not used within Federation circles. This allows for a more level negotiating position between senior officers and Federation representatives.

be relied upon as either primary or corroboratory evidence for any findings, nor can they form part of any conclusions.

In relation to officers who have been subject to criminal and misconduct proceedings different ethical considerations are evident. The author recognises the potential of this research to inadvertently glorify corrupt or even illegal behaviour. Likewise, some subjects who feel that they have been mistreated by an investigation into their conduct may feel that the project presents a platform for them to air their sense of grievance. Finally, and highly significantly for the author who remains a serving police officer, some research subjects may disclose additional offences and misconduct breaches, which have not previously been the subject of any investigations. As such, the author would be bound principally by his personal and professional integrity, but also by legislation, to provide this information to the relevant agency.

Method Employed

Having taken into account all of the previously discussed considerations the author decided that the most effective method of data collection for this research would be face to face interviews with a number of individuals. Whilst the author's position within the anti-corruption arena may present the suggestion that the research borders on ethnography, the author is clear that the studies undertaken are separate from his day to day work where potential conflicts of interest may occur. Other methods, such as focus groups and self-completion questionnaires, were excluded as either impractical to arrange given the subject matter, or too susceptible to low response rates, rendering the data gained of limited value.

The author decided that the interviews should be semi-structured in nature to allow for some direction to be maintained but also to allow research subjects to provide any information they deemed relevant. The use of unstructured interviews was discounted for a number of reasons; primarily to prevent the gathering of irrelevant data, but also to mitigate some of the ethical considerations around glorifying misconduct and the provision of a opportunity to those previously convicted of such conduct to boast of their actions at the expense of providing meaningful data. In order to ensure a consistent starting point for each interview the author devised a set of initial questions to prompt discussion. These are reproduced at Appendix A, and consist of a number of enquires as to potential factors which may be considered or overlooked by officers undertaking computer misuse. The starting points offered were those of ease of misuse, the perceived stigma, the likelihood of being caught, the perceived consequences as well as the knowledge level that the act itself was prohibited.

As a social science research project, the author was conscious that although a variety of research methods were available, the nature of the data sought lends itself towards the softer paradigm of qualitative research method rather than harder quantitative methods. It was, and remains however, the author's firm view that the era of paradigm war (Bryman, 2008. p625) between qualitative and quantitative method is an anachronism.

Having decided upon a primary method of data collection, the author took the view that the data obtained should be subject to thematic analysis. In doing so he considered but excluded, options such as narrative and content analysis. Both were

deemed by the author to be overly structured for the research topic, and whilst undoubtedly valuable in a quantitative project, restricting to one of this nature.

After deciding both the research and analysis method, the author turned to the subject of how to take the project forward. The author identified four distinct perspectives on police computer misuse to provide the greatest opportunity of differing views on impacting factors. Two of these perspectives can be judged to be on the organisational side whilst the remaining two are perhaps greater aligned to the views of those undertaking computer misuse[67].

On the organisational side of the study, the author identified the first perspective being that of 'National Leads', consisting of individuals charged with leading national organisations or the specific corruption aspect of a national organisation. The specific agencies identified were, the 'Association of Chief Police Officers' (ACPO), The 'Independent Police Complaints Commission' (IPCC) the 'Crown Prosecution Service' (CPS) and the 'Serious and Organised Crime Agency' (SOCA). Similarly on the organisational side the author identified the second perspective being that of 'local anti-corruption enforcement leads'. Invariably these are senior officers within Professional Standards Departments with responsibility for anti-corruption resources and operations. In practical terms it is these officers who carry out investigations into corrupt activity and are therefore well placed to provide a perspective on factors contributing to the malpractice.

[67] The author is at pains to underline that whilst the views of the Police Federation and those of officers concerned in police computer misuse are described as 'aligned' this is no way infers that the police Federation support this form of misconduct. The author is clear in his opinion that the opposite is in fact true, with the National Police Federation taking significant steps to dissuade their members from this and any other form of misconduct.

On the reverse side of this 'virtual coin' the author identified the Police Federation[68] as key to representing officers accused of computer misuse. In this position they perhaps hold the second clearest view of impacting factors leading to malpractice, as their relationship with suspected officers is generally built on trust and a reputation for a fair, but robust, defence of their members, even if this can only realistically represent the advancing of mitigation where prior admissions have been made. Whilst the Police Federation is a large organisation with many distinct functions, the area of particular interest for this study is the 'Discipline Liaison Officer' (DLO) function. DLOs are nominated within each force area and provided with training at a national level in order to represent local officers. The final perspective examined in this project is that of officers who have themselves been found guilty of either criminal or disciplinary breaches relating to computer misuse. This last category is able of course, to explain personally the impacting factors as they seem to them, that contributed to their own misconduct.

In order to overcome potential ethical issues previously discussed the author devised a letter of introduction to all potential research subjects. The letter made it clear that the author remains a serving a police officer and that he consequently remains bound to report any previously undisclosed wrongdoing should it be made apparent. The letter also explained how a subject could later change their mind about taking part in the research and an undertaking that should they do so, their interviews would not be used. In all cases the author also provided subjects with a copy of the University's Ethics Committee's clearance for the research to go ahead.

[68] The Police Federation is to all intents and purposes a union representing the interests of its members, who consists of officers up to and including the rank of Chief Inspector. Their influence is significant and arguable beyond that of any other police / staff representative association as their membership in pure numerical terms outstrips that of any other group.

Subject Selection

In the first group (National Leads) there was limited scope for any subject selection, with only one significant individual for each agency. The ACPO National lead for counter corruption is Mr Bernard Lawson, the current Chief Constable of Cumbria. Mr Lawson also chairs the National 'ACPO Counter Corruption Advisory Group' (ACCAG) and is therefore uniquely placed to provide the ACPO perspective in relation to computer misuse. The Chief Executive of the IPCC is Ms Jane Furness. She is also the author of the most recent IPCC report into police corruption commissioned by the Home Secretary last year. As such she is able to provide an insight into the IPCC's view of police corruption both from her personal experience and the research conducted to inform her report. Mr Nick Fox is the current lead for counter corruption within SOCA. In his current position he is responsible not only for the investigation of serious corruption, but also the publication of a three yearly counter corruption strategy and threat assessment which is released to all forces to inform their own counter corruption efforts. The CPS lead for the prosecution of corruption offences is Mr Gaon Hart. As such, he represents the Director of Public Prosecutions in reviewing evidence of corruption against police officers and making the decision as to whether criminal proceedings should take place. His experience allows him to comment on factors put forward both in defence and as mitigation when considering cases. All four national leads were approached and agreed to take part in this research. The author notes however, that had he not been a serving police officer so closely linked to counter-corruption enforcement, it is unlikely that access to these individuals would have been available.

The second research group, that of local heads of investigation provided greater scope for selection. With over 40 Home Office forces and well over half of those having their own counter corruption team, the author sought to find a reasonable geographical spread throughout England in order to avoid the suggestion that any findings were relevant only to a small region. Those who agreed to participate in the research were based in Merseyside, Kent, Essex, Surrey, Lincolnshire, Avon and Somerset, Greater Manchester, Norfolk and Suffolk. In total nine senior officers took part in this research group.

Research group three consisted of Police Federation staff who have represented officers accused of computer misuse. In addition to ten local officers based within forces, the Federation National discipline lead, Mr Steve Evans[69] also agreed to take part. The officers based within forces were again spread throughout England, with representatives from Hertfordshire, Kent, Greater Manchester, Cheshire, Lancashire, Merseyside, Surrey and Cambridgeshire.

The final research group, consisting of officers who had been disciplined and / or prosecuted criminally, was again spread throughout England. This group was perhaps the most difficult to identify and gain agreement from, as in many cases, officers who had left the organisation wanted little further to do with its representatives. In other cases, officers were either embarrassed or just wanted to put the incident behind them rather than revisit the past. Those officers who did agree to participate came from Greater Manchester, Cheshire, Lancashire, Surrey, Suffolk, Norfolk and Bedfordshire. Of the seven participants, two had been criminally prosecuted, (one of

[69] The author is particularly grateful to Mr Steve Evans from the National Police Federation Office at Leatherhead. His support during this project has been invaluable in not only identifying other Federation officers but also encouraging his team members to approach officers subject to misconduct procedures to seek their participation.

these being a serving prisoner at the time of the interview). Of the other five, two were dismissed from the police service with the other three receiving final written warnings at internal misconduct hearings. All of these officers were identified and approached via the Police Federation.

In total thirty one interviews took place, each was face to face on a one to one basis and occurred between the 20th February 2012 and the 23rd of April 2012. Interview notes were taken during each of these meetings and an undertaking given to all participants other than national leads[70] that they would not be personally named within the thesis.

Difficulties Encountered and Amendments

Throughout the research phase the author has generally experienced support and full cooperation from agencies and individuals. As has already been acknowledged, key to gaining access to national leads was his position within law enforcement, without which it is unlikely that the first research group would have been accessible.

During initial interviews with the national leads group it became clear that individuals saw police computer misuse existing on a spectrum ranging from low level to high level. In order to maintain consistency for subsequent research groups the author formalised the view presented and provided it to other research subjects at the start of interviews. The hierarchy, which is referred to in most interviews consists of a low to high scale and relates specifically to the nature of the misuse itself, and not the volume of unauthorised checks or the sensitivity of the individual searched upon.

[70] National Leads here includes Mr Steve Evans from the Police Federation. All national leads have agreed to be named in this work.

Lower level misuse would be associated with nosiness and boredom with searches being undertaken for one's own interest with no information being passed on. As the hierarchy level moves up, it would include the use of information to protect family and friends or in pursuance of localised disputes and at the highest level the nature of misuse would include the provision of information to criminal gangs in order to protect their activities or frustrate police operations. The author is satisfied that by making this point clear to all participants, a consistent view of the hierarchy was understood by those using it to explain their responses to questions.

An issue specific to one group alone, that of officers and former officers, was that of access. Access to hard to reach groups in research is not uncommon (King & Wincup, 2008) and the use of the Police Federation as a *'gatekeeper'* to this group proved invaluable, so much so that it is unlikely that those individuals would have been available to the author without the support of the Police Federation. The relationship of trust built between officers and their Federation representatives make it crucial to initially gain the support of the organisation prior attempting to replicate this research. Without the assistance of the Police Federation research group four is likely to be significantly reduced if not removed.

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 5
Findings

Overview

In this chapter the author seeks to present the empirical data gained from the four identified interview groups; national leads, investigating officers, federation representatives and disciplined officers. Whilst the author has attempted to present the findings without interpretation, leaving discussion and interpretation to a later point, the first part of this chapter deals with both the temporal and political context within which the research was undertaken and outlines the particular background of each of the research groups. This serves both to contextualise later sections of the work and to allow the reader to assess the weight to be given to interview responses.

The second part of this chapter relates to the responses themselves which are provided by theme with each interview group's perspective being presented, examining each of the key factors raised in turn, and how relevant each group believed them to be. In this section the views of 'national leads' are presented as attributable to named individuals, for both investigating officers and federation representatives the interview responses have been aggregated to form a general view.[71] Where marked differences of opinion within a group were evident this is

[71] The only other exception to this being Mr Steve Evans, the Police Federation national lead for misconduct issues, whose views are included within the federation group.

highlighted. [72] For the final group, that of officers who had been disciplined, responses are again shown in an aggregated form, but where specific comments are relevant they have been attributed to anonymised coding (Officer A-G) to allow for the fuller context to be examined through the more in-depth descriptions of the interviews available at appendix C.

In closing this chapter the author moves to a basic comparison between the four groups by presenting the findings in tabular form highlighting significant differences in perspective, providing a firm basis for discussion in the following chapter.

Findings in Context

Temporal / Political

The data collection exercise for this work took place between February and April 2012. The preceding 18 months could fairly be characterised as a period of significant public and political concern at the relationships between the police, the press and alleged criminal activity by both. In January 2011 the Prime Minister's Director of Communications, Mr Andy Coulson, resigned from his post following long standing allegations of his inappropriate conduct whilst in his previous role as editor of a national newspaper during the high profile 'phone hacking' scandal[73]. At the start of July 2011 an independent civil liberties group, 'Big Brother Watch', published a paper claiming to show the extent of police employee's abuse of computer systems, and the

[72] Here the author refers to split opinion between the group rather than one individual holding a particular view contrary to the other interviewees.

[73] The 'Phone Hacking Scandal' as it became widely known in the national press related to allegations that tabloid newspapers had conspired to gain access to celebrities' and other public figures' telephone voicemail messages and had used these to inform investigative journalism and to gain information that they would not normally have access to. A journalist was charged and imprisoned for this type of criminal activity, from the 'News of The World', which at the time of the alleged conduct was under the leadership of Mr Andy Coulson. At the time of the original allegations no criminal action was taken against Mr Coulson and he went on to become the Director of Communications for the Prime Minister, Mr David Cameron.

resultant penalties that they had received. Whilst the organisation is little known and its data was obtained from the police themselves as a result of a series of Freedom of Information Act requests, it was widely circulated among law enforcement agencies and in particular, those responsible for counter corruption. The publication began with a statement from the organisation's director, Mr Daniel Hamilton, stating "*The allegations surrounding Andy Coulson are just the tip of the iceberg*" (Hamilton, 2011. p1).

On the 13th July 2011, the Prime Minister announced a public enquiry into the activities of the press and appointed Lord Justice Leveson to oversee the investigation. Part 2 of this report was to call witnesses and focus on the relationship between the media and the police.

On the 17th of July 2011, the then Metropolitan Police Commissioner, Sir Paul Stephenson resigned after acknowledging accepting £12,000 worth of hospitality at a luxury spa, courtesy of a former 'News of the World' employee.[74] The following day Assistant Commissioner John Yates, the senior police officer with responsibility for the original 'phone hacking' enquiry in 2010 resigned amid criticism that he had failed to properly investigate the allegations at that time. Later that year the Home Secretary commissioned two reviews into police corruption. The first by Her Majesty's Inspector of Constabulary (HMIC) and the second by the Independent Police Complaints Commission (IPCC). At the time of the research gathering exercise, each of these had provided an initial report but both had indicated a second report on their work would be forthcoming.

[74] The receipt of this hospitality and its surrounding circumstances were subject of an IPCC investigation and no wrongdoing on the part of the Sir Paul was identified.

The prevailing political context is likely to have impacted upon the responses provided during this research and this has probably been most notable in interviews with national leads and the Police Federation. Within the national leads interview group the Association of Chief Police Officers are firm in their rejection of widespread corruption, although by virtue of the definition that they have adopted, that of *"The abuse of one's role or position held in the service for personal gain or the gain of others" (ACPO in IPCC 2011, p 14),* and the inclusion of computer misuse within this, there appears to be some question as to how confident ACPO can be on this assertion. The Police Federation however, acknowledge the scale of computer misuse but advance the view that the vast majority of their members operate under misinterpretation of legislation and regulation. Given the organisation's aims and other current negotiations underway in relation to officer's employment terms and conditions, the organisation would doubtless be reluctant in the current climate to acknowledge fundamental flaws in their membership. For the avoidance of all doubt the author does not now or at any point in this work advance that either the national lead for counter corruption within ACPO or the Police Federation have in any way sought to cloud their responses; quite the contrary is true, in that the author has enjoyed frank and constructive assistance from both. He does however point out that as both organisations operate nationally within a highly politicised environment, the prevailing political context is unlikely to have been overlooked by either.

National Leads

National leads for the purpose of this research are individuals who hold senior positions within their own organisations and have been appointed to represent their

organisation at a national level in the area of police corruption. Whilst it is doubtless possible to identify other stakeholders within the national leads arena for police corruption, the author is of the view that the four chosen provide a balanced sample[75]. The national leads who agreed to take part in this research are Mr Bernard Lawson QPM, the Chief Constable of Cumbria and the current Association of Chief Police Officers (ACPO) national lead for counter-corruption, Mr Nick Fox OBE, the head of counter-corruption for the national Serious Organised Crime Agency (SOCA), Mr Gaon Hart, Senior Crown Advocate and Crown Prosecution Service (CPS) lead for corruption prosecutions, and Ms Jane Furniss, Chief Executive of the Independent Police Complaints Commission (IPCC), and author of the most recent IPCC review of police corruption. All four agreed to be named and to have their interviews attributable.

The Association of Chief Police Officers (ACPO)

"The Association of Chief Police Officers (ACPO) is an independent, professionally led strategic body. In the public interest and, in equal and active partnership with Government and the Association of Police Authorities, ACPO leads and coordinates the direction and development of the police service in England, Wales and Northern Ireland." (ACPO)[76]

A key role of the Association is that of the provision of advice to Chief Constables in the governance of their forces. Whilst ACPO holds no power to mandate activity or processes within individual forces, adherence to their guidance, having been issued

[75] The four individuals chosen represent two from the side of law enforcement, ACPO and SOCA, and two from outside the policing arena, the CPS responsible for prosecutions and the IPCC responsible for independent oversight of police misconduct.
[76] http://www.acpo.police.uk/About/AboutACPO.aspx (Accessed 20/9/12)

following agreement at the 'Chief Constable's Council'[77] is generally seen as desirable. ACPO discharges its advisory function through a number of business areas. One of these is entitled 'Workforce Development' and it is this area that the issue of Professional Standards and Counter Corruption falls. In December 2011, after the publication of both the HMIC and IPCC reports the ACPO lead for Professional Standards, Mike Cunningham stated;

"The police service is a highly accountable organisation which must be responsive and trusted by the public. With a dedicated team to investigate allegations of corruption in each force, we have one of the least corrupt police services in the world. This review [...] found no evidence of systemic corruption in policing, but individual cases where police officers let their colleagues and the public down. [...] Leadership has always been an important part of tackling police corruption and the service has worked hard to identify threats and put preventive measures in place. [...] This review highlights the need to continue to develop safeguards and to keep pace with new developments in information technology which expand the potential for vulnerability to corruptors. ..." (ACPO)[78]

Police officer members of ACPO[79] hold a senior rank[80] and have generally not worked in an operational role for many years. Whilst the experience held by its members is doubtless significant and provides great strategic insight in problem solving, it is difficult to argue that their members have a continued direct connection with grass roots policing. In general terms this does not pose difficulties, moreover it can be

[77] Chief Constable's Council is an ACPO forum for discussion and 'signing off' of advisory documents. Its membership consists of all Chief Constables as well as policy advisors.

[78] http://www.acpo.presscentre.com/Press-Releases/ACPO-comment-on-HMIC-police-integrity-report-Without-Fear-of-Favour-133.aspx (accessed 20/9/12)

[79] Police Staff at a senior grade can also join the organisation however the numbers eligible are significant lower than officers.

[80] Members must be of Assistant Chief Constable rank (or police staff equivalent) or above.

seen as a strength in that the command structure of forces combines the strengths of experience at the senior levels with tactical ability at more junior levels. A potential weakness however is the maintenance of contact with junior staff to ensure that what was desired at the strategic level has indeed been correctly translated into operational activity. (Loader & Mulcahy, 2001) In this regard the association is probably no different to any other large hierarchical organisation that promotes from within.

The Independent Police Complaints Commission (IPCC)

The IPCC is a 'Quasi Autonomous Non-Governmental Organisation' (QANGO) whose responsibility includes activity to *"increase public confidence in the police complaints system in England and Wales." And "investigates the most serious complaints and allegations of misconduct against the police in England and Wales....."*[81] *(IPCC 2012)*

Whilst the IPCC aims to investigate serious matters, it is to a great extent dependent on individual forces referring matters to them. In the second of their reports into police corruption published in May 2012 (although prepared and an embargoed copy provided to the author prior to the research interview with Jane Furniss), the IPCC make comment on an apparent disparity between forces referral practices; *"The most striking finding from the analysis of corruption related referrals at force level is the differential rates in which cases are referred to the IPCC. These ranged from 11 referrals per 1000 [employees] to no referrals at all. There are a number of factors that may explain these variations [...] The wide variation is a matter of concern and action is proposed to tackle it"* (IPCC, 2012 p38).

[81] http://www.ipcc.gov.uk/en/Pages/about_ipcc.aspx (Accessed 20/9/12)

It can be seen therefore that the IPCC experience some level of frustration at the point at which they are involved in police corruption investigations. Likewise, for the greater part, they deal with only serious allegations of corruption and are therefore generally some way removed from lower level allegations of misconduct. The organisation therefore has the potential to receive a distorted view of police corruption in that the numbers it is made aware of are lower than the true picture and additionally those that are referred are towards the higher end of the seriousness scale. Despite the inconsistencies of reporting, it is argued that the most recent reports by the IPCC have provided a balanced perspective on both numbers and seriousness of corruption matters and have confirmed that they have found no evidence to suggest that the issue is endemic *(IPCC, 2012 p6).*

The Serious and Organised Crime Agency (SOCA)

The Serious and Organised Crime Agency consists of a number of departments tackling serious crime at either cross boarder or international level. As part of their function they operate a counter corruption command. Due to the nature of the work undertaken by the agency, the corruption work they become involved in is generally at the higher level of the seriousness scale. They also provide a resource to local forces in the investigation of corruption as well as conducting their own operations, and therefore can be seen to be close or directly involved with grass roots operational activity.

The Crown Prosecution Service (CPS)

The Crown Prosecution Service is responsible for criminal prosecutions in England and Wales. Whilst the service holds significant experience in its field it has limited exposure to operational aspect of policing. The Crown Prosecution Service, in determining prosecution decisions, conducts two 'tests' which a case must pass in order to proceed to full prosecution[82]. The first of these relates to the available evidence and the second relates to the public interest. Generally the Crown Prosecution Service is of the view that lower level matters of computer misuse should be dealt with by way of employment provisions internally as they would be for example, by any other non-police organisation. There is however a provision within the 'Code for Crown Prosecutors' which relates to factors which may influence the public interest test, and one of these is whether the subject was in a position of trust at the time of the alleged offence. Consequently significant discussion often takes place between the CPS and investigating officers as decisions are rarely clear cut[83].

Investigating Officers

Heads of Counter Corruption units generally hold the rank of Detective Chief Inspector or above, and work within their force's Professional Standards Department. The units themselves are normally staffed with experienced detectives and hold high vetting statuses giving them access to the most sensitive of information. There is a tendency for the units to see themselves as professional élites and to be seen by others as departments working covertly behind the scenes, which can manifest itself in

[82] This test is known as the 'Full Code Test' and is outlined in the 'Code for Crown Prosecutors'.

[83] Particular discussions take place where an officer has already resigned from the police service and therefore has no continued access to sensitive information. Here the CPS may well suggest that if the offence did not result in detriment to another, the circumstances make it suitable for either no further action or a formal caution as opposed to criminal prosecution.

suspicion of the way in which they operate. Leaders of these teams may justly be seen as guardians of the organisation's integrity and reputation. Performance of these teams is often measured in the number of cases identified and the effectiveness with which they are dealt. Investigating officers who took part in this research are rarely involved in investigations directly, and so are a little way removed from operational policing. The perspective they provide however is based on the cases investigated by their officers and therefore their perspective can be judged to be reasonably close to the issue.

For the purpose of the research, interviewees were heads of counter corruption units. The label used for this group, that of 'Investigating Officers', provides a convenient way to refer to this set. The author points out however that by virtue of their rank, these officers are not involved directly in investigations, but have an overview of all enquiries undertaken by their teams and so are better placed to provide an overall perspective rather than one limited to a small number of cases in which they have had personal involvement. Officers typically spend around three years leading a Counter Corruption Unit, and the officers who took part in this research span this period of experience with some being relatively new in post and others approaching the end of their tenure. In total nine investigating officers took part in interviews.[84]

The Police Federation

The Police Federation is the staff association representing the 140,000 police officers between the rank of Constable and Chief Inspector. They are often referred to as the body representing the *'rank and file'* in the national press. Amongst its aims and

[84] Questions posed to Investigating Officers are again replicated at Appendix Aii.

objectives it records a desire *"To represent and promote the interests and welfare of our members, and to support colleagues to achieve the required professional standards."* by *"Representing our member's interests in matters of discipline..." (Police Federation 2012)*[85]

The Federation has a history of robust defence of both policing nationally and its members and on 18th July 2011 its chairman, Mr Paul McKeever, issued a press statement in relation to recent police corruption allegations; *"... Seeing and hearing some of the recent commentary by some media and politicians I must object, on behalf of all police officers across England and Wales, to the grossly offensive and incorrect assumption that the police service suffers from wide scale corruption [...] This must be kept in context and not become an excuse for political point-scoring. The British police service remains the most open, accountable and professional police force in the world and the men and women who work within it are of the utmost integrity and have every reason to be proud."* (Police Federation 2011)[86]

The Police Federation maintains the position that it will not tolerate police corruption within the police service and experience demonstrates that where officers admit such conduct they are invariably denied legal funding for internal discipline proceedings and are advised as to the appropriateness of their continued employment within the police service. Where the Federation believes however that members have been treated unfairly or have made mistakes due to lack of knowledge rather than mal-intent they are robust in their defence, investing significant sums in legal representation.

[85] http://www.polfed.org/aboutus/3E5F08F74E1A4CFAB3D9C49A43284FB5.asp (Accessed 27/9/12)
[86] http://www.polfed.org/mediacenter/0D5843FE44DC420793D2721ECF38CF90.asp.asp (Accesses 27/9/12)

As the Police Federation representatives often fulfil their responsibilities in addition to their day jobs as police officers,[87] it is fair to say that they are generally close to operational policing. In addition, with the relationship of trust which invariably exists between officers subject to discipline enquiries and their Federation representatives it may fairly be argued that the perspective they bring is very close to that of the officers themselves, but further benefits from being slightly removed from the emotive position of the officer themselves. Therefore, whilst this perspective is not the closest[88], it is arguably the most insightful. Between all ten of the interviewees in this group they had collectively dealt with in excess of 150 cases, some of which involved multiple officers, the most significant involving over 200 officers.[89]

Disciplined Officers

The seven officers who were interviewed as part of this research are of course, the closest to the misconduct they undertook. They have the greatest perspective on the factors that they considered, or were aware of, at the time of their actions. As a result of those actions some had chosen to resign, rather than face disciplinary proceedings, others had been dismissed, and one had been charged and sentenced to a period of imprisonment. A number however retained their position within their force, albeit

[87] In each force a number of Police Federation representatives will be deployed full time on Federation business (funded by the force themselves) these normally consist of the Chair and Secretary. The role of Discipline Liaison lead is often undertaken by one of these posts, whilst the majority of Discipline Liaison Officers actively engaged with members will be officers from other departments within the force but locally elected to represent members as and when required.

[88] The closest perspectives are undoubtedly those of the disciplined officers themselves.

[89] The question list used as a starting point for this group is attached at appendix Aiii.

with an alternative disciplinary sanction. It is easy to assume therefore that the perspectives provided by this research group provide the definitive view.

The author however is conscious that for many, the emotive ramifications of an internal discipline hearing or indeed criminal action may have distorted individual recollection. Likewise from the interviews conducted it is clear that a number of the subjects were embarrassed at their conduct and may have sought to minimise this in their interview responses. Finally for those who had not been dismissed from their force, their remains the possibility that the full facts were not disclosed during a disciplinary hearing, in such cases it is unlikely that the officer would provide these previously undisclosed details in interview for fear of further investigation. Whilst the author does not believe that any officer deliberately sought to mislead him during interview, it is notable that a number provided responses that appeared confused particularly around the responses provided to questions on the awareness of wrongdoing and those relating to the associated potential sanctions. Although this lack of clarity from some members of the group presents the possibility of distortion in this particular area, generally the author is of the view that responses were genuine and considered, demonstrating in almost all cases remorse for the misconduct undertaken.

Findings by Theme

Motivation

In all cases the starting point for interviewees was the question template (Appendix A). In order to provide some context for later responses the issue of motivation and

scale of the problem was firstly explored.[90] All four national leads were of the view that motivations for computer misuse and unauthorised access to data formed a hierarchy of seriousness, ranging from simple access through nosiness and curiosity at one end of the scale through to the obtaining of information and passing it on to third parties with a view to disrupting police operations at the other. Jane Furniss pointed out that the IPCC do not normally become involved in lower level misuse and therefore her experience tended to reflect the more serious incidents. All agreed that the most common motivations were lower level and were based on simple nosiness or boredom, and consisted of searching for personal data of celebrities or friends. A second area featuring highly as a motivation for national leads was the obtaining of information to protect family and friends; a typical example being carrying out checks on a daughter's new boyfriend or new neighbours. In addition to these checks, an additional motivation was noted, that of those going through acrimonious relationship breakdowns, and using the systems to watch what the other party is doing, or to prepare for a custody battle. Only one national lead, Gaon Hart, discussed the issue of third party allegiance or ideological belief as a motivation. He provided an example of officers providing information to the media through an honestly held belief that the public '*had a right to know*'. All four national leads agreed that the higher level misuse for either money or to disrupt criminal investigations was rare.

Investigating officers split motivation into two categories, one interviewee described these as being internally driven and externally driven. Internally driven motivations encompassed an officer deciding of their own accord to misuse systems, whilst

[90] Whilst motivation is not the key focus of this research it is important to consider why officers undertake corrupt practice to put into context the impacting factors.

externally driven motivations related to a third party outside the organisation tasking an employee to carry out checks. All investigating officers agreed with national leads in that most significant in numerical terms were internally driven cases and these tended to be computer checks carried out due to personal relationships, neighbour disputes or nosiness. They were generally of the view that the highest proportion of illegitimate uses were due to nosiness and curiosity, with the protection of family and friends, and enquiries relating to estranged partners also featuring highly. Two investigators highlighted celebrity interest as a motivation, with one providing an example of the arrest within their force area of a high profile footballer. Subsequent to this arrest, the Counter Corruption Unit identified some 200 enquiries on the player's intelligence and custody record, with only a handful being legitimate to the case investigation. A final internally driven motivation raised by investigators was that of kudos within a peer group. Younger officers, it was said, join an organisation where their social friends outside the force are very interested in their work, and in order to maintain kudos within that group, they seek information to discuss or reveal in a social setting to impress. In relation to externally driven motivations, it is notable that the group were of the view that such cases were rare, but where they did occur they were likely to relate to information being passed to the media, or in some cases as a result of an Organised Crime Group (OCG)[91] approaching an officer and tasking them to gain information. Significantly, such motivations were not seen as common, and even where they did occur, the officer's objectives tended to be other than financial. For media leaks, investigating officers believed that the objectives tended to be either ideological with officers believing that the public *'had a right to know'*, or more

[91] The term 'Organised Crime Group' is used in policing to denote a number of individuals working together to commit serious crime.

frequently with a view to mischievous intent as a result of disaffection with the force. For leaks to 'Organised Crime Groups' the issue tended to be third party loyalty, such as childhood friend, gym partner, or social acquaintance asking for assistance. The author points out however, that such instances were seen by the group to be rare, so much so that two of the nine interviewees did not mention them at all.

For the Police Federation, motivations tended reflect the lower end of the previously discussed seriousness hierarchy. All interviewees were of the view that the majority of instances relate to nosiness or boredom, with three mentioning the searching against celebrities' details out of curiosity. Significantly this particular motivation was always spoken about against the backdrop of a lack of awareness on the part of the officer and a general theme that officers did not understand what they could and could not do on police systems. One interviewee stated that this celebrity motivation was probably responsible for about 80% of officers disciplined for this type of breach of regulations in his force[92]. The next motivation advanced by the Police Federation was that of protection of friends and family such as checking on a daughter's new boyfriend. This motivation was frequently discussed with a suggestion that officers sometimes feel that they have a right to know, in that if someone they have regular contact with is of interest to the force, then they may be better enabled to provide valuable information. Whilst the interviewees acknowledged this response on the part of their members, as an organisation they are not of the view that this represents an acceptable defence. Moreover for many DLOs, this reinforced the position that many officers do not truly understand the limits of acceptability. One DLO however stated that there was some awareness but also a belief that as the data is available to

[92] The high percentage referred to relates to one or two single instances involving a high number of officers.

them then *'why shouldn't I ?'* and a perception that if challenged the check can always be dressed up as having a policing purpose as outlined above. This was backed up by the suggestion that some were of the view that if there is no record on an individual then there will be no record searched and therefore no breach of the regulations, whereas if a positive 'hit' is made then that fact alone may retrospectively justify the check. Federation representatives were consistently of the view that activity at the higher end of the hierarchy was very rare, but no percentages were provided.

The responses obtained from disciplined officers did to a great degree reflect the views of the other three interview groups, however the issue of nosiness, although discussed in interviews and regarded as prevalent by others within their forces, was not apparent as a motivation for the officers themselves. Of the seven interviewees, four stated a motivation of either self-protection[93] or that of friends and family, one related to gathering information on an estranged partner to assist in divorce proceedings, one was due to misguided loyalty towards a former friend and one related to disrupting an investigation in exchange for drugs.

Scale

In order to introduce the issue of scale, all interviewees were provided with the 'Big Brother Watch' data set compiled as a result of a Freedom of Information request[94]. This source data is available at appendix B. Interviewees were asked to express a view from their experience, as to whether the data for the three years between 2007 and 2010 showing 904 officers and staff being subject to internal discipline, either

[93] The self-protection relates to an officer checking to see if someone had made a criminal allegation against him.

[94] This Freedom of information request was made in 2011 by 'Big Brother Watch' and circulated to national media.

represented a poor period for policing with an unusually high number of incidents, seemed to reflect the scale of the problem, or was in their view likely to be under-representative of the problem.

All four national leads were of the view that the scale of the issue is far greater than that reported in the data. Bernard Lawson, who perhaps expectedly was aware of the data set and able to expand on specific figures for some forces, pointed to the fact that where high figures appeared they often related to single or a small number of distinct incidents such as the arrest of a high profile celebrity within a force area, and the force subsequently examining who had viewed the resultant data. Mr Lawson also indicated that the number of employees misusing systems was, in his view, falling as officers were better understanding the limitations of authorised use and therefore less likely to inadvertently breach the regulations. He also pointed out that forces were also getting better at detecting security breaches.

Nick Fox compared the data to approximately quarter of a million people UK wide involved in law enforcement and expressed the view that the figures appeared low. Gaon Hart from the CPS was of the view that the data was the *'tip of the iceberg'* and that only the more serious cases were probably caught, with lower level breaches going undetected. Ms Furniss of the IPCC expressed that based on her experience and the work she had done for the Leveson enquiry, she would be surprised if the figures represented a few poor years where a greater than average level of computer misuse had taken place, but that the figures probably feel between being about right and being under representative. Contrary to the view of Bernard Lawson however she was of the view that the problem may be getting worse.

Investigating officers were of the view that the figures presented were under-representative of the true scale of the issue. Sentiments expressed by this group were that the misuse of police systems was *'endemic'*, and *'grossly underestimated'*. One participant gave his personal belief that the true scale of the issue is around 6-10% of police officers undertaking illegitimate computer checks. Two forces had conducted their own research in this area. The first operated a process whereby officers could report concerns relating to family and friends to the Counter Corruption Unit. This proactive approach on their part could serve to protect them later if subsequent information came to light linking them to criminal suspects. At the point of self-referral the Counter Corruption Unit carried out a covert audit on the staff member's computer use. The interviewee reported that approximately 80% of these employees had previously carried out checks on the subject of their referral, i.e. their own friend or family member. A separate force had carried out a covert dip sampling exercise whereby they had selected 100 employees at random and conducted covert audits on their computer usage. The results of these audits showed that approximately 25% of the sample had carried out checks on persons with the same surname as them, or persons living in the same road as they had registered as their own home address.

In keeping with the view of investigating officers, the Police Federation was universally of the view that the figures provided did not represent a true reflection of the numbers involved. In responding to this data responses ranged from *"there must be more, every instinct tells me there must be more"* to *"this is a huge issue and is very under-represented in these figures"*. One DLO was able to provide the author with figures obtained from the National Federation office showing the number of cases for

which the Police Federation had funded legal advice. Generally the Police Federation fund only those cases designated as *'gross misconduct'* rather than simple *'misconduct'* by Investigating Officers. The distinction being that the former is judged to be so serious that dismissal would be justified, whereas the maximum sanction for the later would be a final written warning.

The figures provided show that between January 2010 and February 2012 some 88 cases had been legally funded.[95] Whilst the time period for the Federation data and the source data used is different, it shows that in the four year period of the source data (2007 – 2010) some 47 Officers had their employment terminated (along with some 51 civilian staff), whilst in the 26 months of the Federation data some 88 officers were in jeopardy of dismissal.

A significant point raised by Mr Evans in discussing this data was his surprise at the apparent low ratio of employment terminations compared to the criminal conviction data and the internal investigation figures. It was his view that from a Federation perspective more than 50% of officers subject to this type of investigation leave the force.

The view of disciplined officers as to the scale of computer misuse was perhaps the most extreme, in that whilst they agreed that the data appeared to significantly under-represent the reality, they were more aligned to the view that the practice was extremely common. Responses ranged from the suggestion that *"I don't think any communicator (control room operator) can put their hand on their heart and say that*

[95] The data provided by the Police Federation is for those cases which they have deemed suitable for legal funding. The Decisions as to whether to grant such funding are dealt with centrally and are not automatic, moreover they rely on a realistic prospect of success and generally the fact that an officer denies wrongdoing. The figures shown here therefore represent only those where funding was agreed, not those where it was not approved.

they have never looked at an incident that they shouldn't have" (*Officer A*), to an estimate that between 80 and 85% of people misuse the system (Officer C), to the assertion "*there must be thousands more doing what I did*" (Officer E). Significantly, the disciplined officers' view although very clear that the practice is widespread, reinforced the position that the vast majority of such activity is at the lower end of the seriousness hierarchy, with one officer maintaining, that "*there is lots going on, but not for malicious reasons*" (Officer D).

Greatest Inhibitor

In focusing more on the specific impacting factors involved in computer misuse, all interviewees were asked for their view on the greatest inhibitor to this type of malpractice. Almost all universally expressed that in the majority of cases, it was an individual's own conscience and integrity which resulted in most officers having no desire to breach any aspects of regulations. The responses given by the interviewees therefore should be seen as relating to the remaining limited number of officers whose own ethical values were not a personal barrier. Bernard Lawson spoke of the general fear of being caught as being a significant inhibitor, and this was further advanced by both Nick Fox and Gaon Hart, both adding that the consequences of being caught also featured highly as a deterrent factor. For Mr Fox, the consequences were seen to be the potential criminal prosecution and sanctions but Mr Hart was of the view that officers are far more fearful of employment sanctions such as the loss of pension rights, rather than in many cases at the lower level, the likely criminal outcomes.

Investigating officers generally held a similar view to national leads in that the fear of being caught and the consequences associated with capture deterred many from computer misuse. A number of the group raised the point that their force publishes the result of gross misconduct hearings along with the sanctions received, and this has led to an increased awareness of the potential sanctions, as well as the realisation that people are routinely caught for this type of activity. One investigating officer explained that most people in his force know someone or certainly know of someone who has been disciplined for misusing systems.

Whilst this was the consistent view of the group, it was in contrast to some of the responses obtained when the issue of risk and likelihood of being caught were explored in more detail. In this area the group was split. Some investigating officers were of the view that the risk of being caught was reasonably high within their force and that this was appropriately perceived by employees. Officers with this view invariably came from forces who used technological solutions to identify potential misuse either overtly, or covertly[96]. The majority of interviewees however were of the view that unless intelligence came in from another source directing attention towards a specific officer, the likelihood of detection was low. This was said to be due to the inability of Counter Corruption Units to carry out many speculative audits in comparison to the huge computer usage within forces.

Generally investigating officers were of the view that there was a greater perception of the likelihood of being caught than actually existed, and that this perception worked to the advantage of the organisation in reducing the number of cases of

[96] Increasing forces are making use of Protective Monitoring Software to identify computer misuse. This was identified as best practice by HMIC in their most recent review.

misuse. An officer who did not feature for any other reason within the sphere of interest of a Professional Standards Department (PSD), who carried out the occasional illegitimate computer check was said to be highly unlikely to be caught. On the subject of sanctions it was generally felt that officers were aware that computer misuse would constitute gross misconduct and could lead to dismissal from the force.

A consistent response was also obtained from the Police Federation who agreed that the consequences and the fear of being caught featured most highly as a deterrent. Chief among these consequences was the idea of a criminal conviction and the loss of job which would necessarily go with it. It should be noted however, that the Federation officers generally reinforced the view that that these inhibitors related only to those who knew what they were doing was wrong, or those who were acting so far outside the scope of reasonableness that they were unable to put forward any pseudo-rationale for their misuse.

Fear of being caught

When the issue of the fear of being caught, sanction and the actual likelihood of being caught were explored, slight differences in views appeared between the four research groups and indeed, within some groups themselves. In relation to national leads, Bernard Lawson, in keeping with previous responses from investigating officers, assessed the risk of being caught as reasonably low, on the basis that a force's capacity to carry out random audits and checks is limited and other than by intelligence led checks on individuals, system misuse was not likely to be identified. This he believed was in contrast to the perception of officers, who were under the impression that significant and sophisticated methods were used to identify misuse.

He was of the view that a greater fear of being caught would dissuade even more people from misuse at the lower end of the hierarchy. He also expressed that those at the higher end of the seriousness hierarchy probably believe that they are covering their misconduct sufficiently to avoid detection and so anything done to raise the perception of being caught may be of limited value here. Nick Fox expressed the view that the likelihood of being caught was probably around 60% but that it very much depended on individual force supervision and governance. He was of the belief that officers knew of audits taking place and that those operating at the higher end of the hierarchy went to great lengths to cover their tracks. Mr Fox was of the view that a greater perception of the likelihood of being caught would reduce the issue. Gaon Hart felt that at the lower level the likelihood of being caught was probably somewhere in the region of 5% but that for the higher end, involving the provision of information to criminal gangs and organised criminality where more work was done to prevent intelligence leakage, the likelihood was about 60%. He was also of the view that the greater the likelihood of detection, the less likely employees were to misuse system, but he qualified this by adding the proviso that sanctions also needed to be significant and that these should be employment sanctions rather than criminal in most instances.

The Police Federation went further than the previous research groups and suggested that fear of detection and consequences applied only to a middle ground on a seriousness hierarchy. The example provided, in keeping with Bernard Lawson's and Nick Fox's view, was that officers who operate at the higher end and misuse police computer systems for financial gain or to assist criminals invariably hold a belief that

they are able to cover their tracks to such an extent that they will not be discovered. In this way the fear of being caught is reduced or removed. When asked specifically if the fear of being caught is something that could be manipulated to discourage computer misuse, the general response reflected a need to impact not on fear itself but the likelihood of being caught coupled with the potential sanctions that an officer may face. For the greater part it was agreed by federation representatives that the likelihood of being caught for carrying out a single unauthorised check by an officer who was not subject of any other PSD investigation was relatively low. Albeit low, it was again felt by the interviewees that the perception of the officer on the street was that they were very likely to get caught, and it was this misperception on their part that limited the number of officers knowingly breaching the regulations. A number of DLOs provided an example here of the use of the Police National Computer[97] (PNC). This system is audited every eight hours with a team's supervisor dip sampling the checks undertaken during that period and proactively asking officers the reason for the checks. Whilst the effectiveness of this practice is limited in its depth, it provides the perception that the system is highly policed and results in the experience of federation representatives, in very limited allegations of misuse of that particular system.

The responses from disciplined officers in relation to the likelihood of detection are unexpectedly similar to those of the former three groups. Whilst interviewees from the first three groups acknowledged that the likelihood of detection was very low, they believed that the average officers on the street considered themselves very likely

[97] The Police National Computer (PNC) is a long standing system introduced over 35 years ago. It contains details of criminal conviction data as well as a link to the Driver Vehicle Licensing Agency (DVLA) systems.

to be caught if they did misuse computer systems. This, they advanced, was due to a common perception that the systems were highly policed. By contrast however, almost all disciplined officers recognised the low likelihood of detection and were often able to explain the circumstances which led to their identification, and rationalise these as rendering them unlucky. For the greater part officers felt that unless they were being investigated by the Professional Standards Department for some other reason, or someone had reported them for misusing the systems, they were highly unlikely to be caught.

Awareness

The issue of police officers' awareness of what computer usage is acceptable and what is not was explored, along with whether forces have done enough to ensure employees are educated on the subject. At the higher end of the seriousness hierarchy such as the obtaining of information and passing it to criminal gangs, there was a consistent view across all groups and interviewees that officers knew that this was totally unacceptable and the organisation would not tolerate such activity, with criminal sanctions likely. At the lower end of the hierarchy however opinions were divided. Bernard Lawson for ACPO expressed that employees are far more aware of what police systems should be legitimately used for now than they had been previously, this was as a result of forces generally doing a good job in handling the issue through training programmes, education and the publication of the disciplinary sanctions of others. He was therefore of the general view that staff understood that it is wrong to conduct checks founded on idle curiosity and nosiness.

Nick Fox shared the view that most employees were aware of what was acceptable but that organisations could do more in the area of awareness raising. He pointed out the constant turnover of staff into and out of sensitive roles, and that more emphasis should be placed on specific instances of what constitutes breaches. He advanced that most people believe they are aware of what they cannot do but in some instances convince themselves that their particular act is ok because of a set of unique circumstances. In this way they self-justified it as outside the scope of a breach of the regulations.

Gaon Hart was of the view that at the lower level there was confusion, particularly in the area of understanding the concept of a *'Genuine Policing Purpose'*[98] when considering why a computer search was conducted. For him this did not appear to have been dealt with effectively by forces, although he acknowledged that all forces provided some reminder at the point of logging onto a sensitive system as to the limitations of legitimate use. Jane Furniss was of the view that she was not at all confident that officers understood the limitations of acceptable police computer use, and pointed to the cultural relationship young people now have with computers and their expectation of the right to data. At the lower level of misuse, she expressed that she did not think employees even considered whether it was right or wrong, moreover they accepted the ability to use computers as a right and did not draw any distinction between their professional and private lives and the use of computers as a source of both information and entertainment.

[98] The Concept of a 'Genuine Policing Purpose' is used in policing to determine whether or not a check on police computer systems is legitimate or not. As the primary basis of disciplinary findings against officers, the author was surprised to find that no firm definition of this exists.

In this area, investigating officers were also divided in some of their views. Again, these differences of opinion occurred in relation to lower level misuse motivations such as nosiness or the protection of family and friends. Some investigating officers were of the view that most employees were aware that the systems cannot be used for anything other than a *'Genuine Policing Purpose'*, and that this had been achieved by training and constant reinforcing through the use of computer 'pop up' messages and campaigns. When pressed however, it became apparent that the issue of *'Genuine Policing Purpose'* was itself unclear and although employees may be familiar with the term, its interpretation is very much clouded.

The majority of investigating officers however, were of the view that there remained a significant lack of awareness of what was permitted and what was not. One officer raised the issue of cultural norms within the workforce being split by service bands or age groups. He explained that officers towards the end of their service were in the force prior to the widespread introduction of computer systems and had grown up having access to all the information they wanted from record cards. At this time they were encouraged to review these to increase their professional knowledge, and this has been a hard culture to break out of following the introduction of electronic data storage. This group, he explained, did misuse systems, but rarely saw any issue in doing so.

The second group consisted of officers mid-way through their service who had joined at a time when computers had already been introduced and had been trained from the start as to what was and what was not acceptable. Misuse in this area was reduced, but those undertaking it were well aware of the regulations and that they

were breaching them, although they may often seek to justify to themselves or others by wrapping it up in legitimate reason.

The final group was that of newer officers who not only had joined a force which made routine use of computer systems, but had also grown up with systems at home and college, for whom instant access to information was an expectation. This group tended to misuse systems out of curiosity, and due to a blurring of the lines between their personal and professional lives, often saw police systems as no different to publicly available data systems.

A great deal of discussion took place with investigating officers on the subject of a 'Genuine Policing Purpose' and the fact that no clear definition for the term existed. They expressed the fact that it is so ambiguous that a frequent defence in disciplinary hearings is that the officer was checking on friends or family to see if there were any police records on them, as if there were, the officer would then be able to assist in providing further information. Whilst at first glance this defence may seem so wide ranging as to make it implausible, it is given some credibility by the existence of force's 'Notifiable Association Policies'[99], which require officers to notify their force if they are in regular contact with anyone who may be the subject of police operations or has been convicted of certain criminal offences. Whilst these policies invariably place an obligation on officers, they do not provide a provision for an officer to carry out checks to identify whether a friend or relative falls into such a category, and therefore advice is limited to reporting suspicions to supervisors to allow them to make enquiries.

[99] A Notifiable Association Policy seeks to protect individuals and forces from social or family contacts which may pose a corruption or other threat. An example would be an officer needing to disclose to his or her force the fact that their friend had been convicted of a criminal offence, or that their new son in law was believed to be involved in criminality.

Investigating officers were of the view that a greater awareness particularly in the area of a '*Genuine Policing Purpose*', would reduce computer misuse, either by way of people making less mistakes, or by people being less likely to deliberately misuse knowing that they would be unable to put forward a defence of misunderstanding.

Responses from the Police Federation left no doubt, that for them, at the lower level of the seriousness hierarchy, the lack of staff awareness as to what is and is not acceptable is the most significant factor in the commission of computer misuse. Mr Steve Evans is clear that there exists a "*huge lack of knowledge*" in this area. He advances that officer's awareness ranges from a few who fully understand the limitations to the majority who are of the view that, provided they do not pass information on to a third party it is acceptable to search and view any available intelligence in case it becomes relevant to their duties. Generally the view from the Federation was that the organisation has failed to provide adequate guidance to officers as to the limits of acceptability, and whilst officers are aware of aggravating factors such as the sale of information, or criminal motivations, misuse without these aggravating factors tends to be a grey area. To quote one DLO "*People are not aware [of what the limits are]. I'm not, and I represent them. I can't get a definitive answer*".

Interviewees were of the view that organisational communication in this area was critical in raising awareness. To reinforce this, the example of the lack of misuse of the PNC was again highlighted. From the day an officer joins the force they are informed that data on the PNC can only be used in connection with one's duty, a position that is backed up by daily supervisor checks. The view of interviewees was that this is a

significant contributing factor as to the lack of cases involving PNC misuse, as the vast majority relate to intelligence and other internal force systems.

Mr Evans highlighted that within the last two years, the National Police Federation had produced an information circular to all of their members giving guidance from their own legal advisors as to what police systems may and may not be used for. This also gave information as to the potential consequences of computer misuse. Whilst the views of the interviewees was that it was important and beneficial for the organisation to do this, it could only go some small way to reduce the problem and that the main responsibility for education rests with forces.

Of particular note by the majority of DLOs interviewed was once again the concept of a *'Genuine Policing Purpose'*. This was invariably seen as too open to interpretation. Many were of the view that whilst some officers may seek to exploit the lack of a definition to self-justify their computer misuse, many officers fell foul of the regulations due to genuine ignorance. It was advanced by two DLO's that many officers are of the view that checking on neighbours and social acquaintances is acceptable as the officer would firstly be able to ensure that they were not putting the organisation at risk through an undesirable social contact, but also, if the person were of police interest, then they would be able to assist with further information. Additionally it would assist in complying with any 'Notifiable Association Policy.'[100] Without doubt the view expressed by this group was that the lack of firm definition of a *'Genuine Policing Purpose'* had contributed to the number of officers disciplined for

[100] A Notifiable Association Policy seeks to protect individuals and forces from social or family contacts which may pose a corruption or other threat. An example would be an officer needing to disclose to his or her force the fact that their friend had been convicted of a criminal offence, or that their new son in law was believed to be involved in criminality. No provision is made however for officers to proactively find this themselves, moreover it is generally suggested that they should, report any suspicion.

breaching the regulations and consequently therefore a definitive position would reduce incidences of computer misuse.

Disciplined officers themselves provided responses reasonably consistent with those of the Police Federation. Of the seven interviewees, five claimed that they did not really understand the limits of what they could use police systems for, and stated that had they categorically known that their checks were not allowed they would not have conducted them. Significantly one of the officers who stated that he did know what he was doing was wrong (Officer B), also maintained that he believed the vast majority of officers did not have such an understanding. A common perception was that provided by Officer E, who advanced that as he was a policeman 24 hours a day he was entitled to look at any information in case it assisted him in policing. Some officers acknowledged that they had undertaken some training in relation to computer usage but that it was some time ago and that no refresher training had ever been offered. Significantly officers drew a distinction between misuse of the Police National Computer and other internal intelligence systems, suggesting that there were different limitations on use, and that they would never dream of using the PNC to check on family or friends as they were very clear that it was prohibited. This they suggested was as a result of continual training and audits that they were aware of taking place on this system.

Ease

On the subject of ease of computer misuse within the police service, the activity itself was universally accepted to be incredibly easy. There was however some discussion by Nick Fox regarding different levels of access, and that as information relating to

current covert operations was not widely available, at the higher end of the hierarchy it is probably more difficult to obtain information worthy of sale to criminals. At the lower level however, it was consistently believed that information was freely available and could be accessed by the majority of staff within police forces with very few safeguards. Far from being seen as a weakness in processes however, three of the four national leads explained that with information and intelligence being so important to the crime fighting effort, the ease of access was a requirement of the way in which forces do business.

Police Federation responses ranged from remarks as to how easy it was to misuse systems in one's own right, through to the ease at finding a terminal where someone had left themselves logged on, to carry out checks. Two of the interviewees remarked on the fact that the systems have quite rightly been designed to be user friendly and on each record viewed there is invariably a link to take you to a related subject. It was stated that if not careful, an inexperienced user could click on a few links and find themselves viewing a page totally unrelated to their initial search. This sentiment was echoed by Mr Evans who was clear that for the ignorant or naïve you "*could click yourself out of a job*".

When discussion moved to whether making it more difficult to access information would reduce the incidences of computer misuse, there was agreement that it would be unlikely to impact at the higher level, as those involved generally have higher access levels to the data and are determined to gain particular intelligence. At the lower level where misuse may be fuelled by ignorance of acceptability, or just nosiness, the fact that access was harder would be likely to reduce misuse. All were,

however, of the view that making access harder without impacting on the ability of officers to carry out legitimate functions would be very difficult and what would be lost would probably outweigh any potential gains. In particular the Police Federation's pointed out that rather than focusing efforts and making legitimate use of computer systems more challenging, resources would be better employed in training on the limitations of use rather than attempting to make an essential system difficult to use. The Police Federation sentiment is generally reflected by the analogy provided by Mr Evans, in that making it harder would be like putting speed bumps in a road; those who were determined to drive fast would find another route; those that drove within the regulations would be slowed down even further.

All disciplined officers held the view that the misuse they made of the computer systems was incredibly easy to conduct and involved no more than accessing systems they would be expected to use on a daily basis as part of their legitimate roles. The officers did however maintain that making use of the systems harder or more bureaucratic (such as requiring supervisor permission to conduct checks) would undoubtedly have prevented them from undertaking the computer misuse, if only by virtue of the fact that someone would have had to review their planned course of action and would then have told them that it was not allowed. They do however note that such a process would also make their legitimate jobs very time consuming and near impossible.

Stigma

All interviewees were asked whether in their view there was any stigma[101] attached to the issue of computer misuse in the police service. Responses from national leads generally fell into two categories. Bernard Lawson and Nick Fox were of the view that the issue was stigmatised particularly at the higher level, but that some level of stigma did exist at the lower levels too. For Mr Lawson this also consisted of the stigma of stupidity at the lower level for carrying out the activity. For Ms Furness and Mr Hart stigma was not evident in their experience, other than for Mr Hart at the very top level of the hierarchy. At the lower levels, no national leads could envisage a situation whereby officers were reluctant to work with a colleague due to him or her having been found guilty of computer misuse.

For investigating officers it was apparent that at the higher level of criminal disclosure significant stigma was evident, but at the lower level of curiosity and enquiries on friends and families, there did not appear to be any evidence at all. One interviewee expressed that there was far more a sentiment of "*There but for the grace of God go I*", indicating that people saw those who were caught as unlucky. Another explained that for many it was seen as *'a perk of the job'* and certainly nothing to be ashamed about.

The Police Federation interviewees saw any stigma attached to computer misuse as coming from a criminal conviction rather than internal discipline, and for the greater

[101] The word 'stigma' is used throughout this work both here in the interview questions to interview subjects and formerly in the selection of research parameters. Academically the concept of stigma has been explored in detail by Erving Goffman who explains "*By definition of course we believe that the person with a stigma is not quite human. On this assumption we exercise varieties of discrimination*" (Goffman 1963, p5). For the purpose of this research the terms is used to describe any sense of disgrace or shame either on the part of the subject and his or her own perception, or on the part of others who know or work alongside the subject as a result of their actions. A Typical manifestation of such stigma maybe reluctance by others to work with a subject or to provide a subject with information that they would otherwise be entitled to, due to a lack of trust.

part restricted to the higher end of activity. One interviewee suggested that stigma could be rank dependant and that although there was no evidence of it at Constable or even Sergeant level, above that there did seem to be some. This he suggested, was more akin to organisational stigma rather than peer group and possibly the perception of the resultant impact on career prospects.

Disciplined officers for the greater part reported no stigma attached to their computer misuse, with only one (at the lower end of the seriousness hierarchy) expressing that she felt that people treated her differently on her return to work (Officer C). The officer did however acknowledge that this may have been her perception and that she was not aware of stigma against any other officer who had been disciplined for computer misuse. All officers did however agree that at the higher end of the seriousness hierarchy there would be significant stigma upon officers who had been found guilty of computer misuse, so much so that it would be difficult for others to continue to work with them.

Perception of seriousness

As a closing point each of the interviewees was asked their view of the perceived seriousness of computer misuse compared to other forms of police misconduct. All were of the view that the level on the seriousness hierarchy was all important: High level misuse was very serious; with significant sanctions from both employment and criminal perspectives available. At the lower level however national leads believed

that there was generally a view that staff saw it more akin to a human frailty rather than corrupt or criminal activity[102].

Investigating officers agreed with the views of national leads expressing that they held the perception that employees saw it as very low level. One interviewee expressed the belief that it was seen similar to speeding, in that everyone does it and some people get caught. When asked whether they believed fewer people would misuse systems if it were seen as more serious, all investigators were of the view that this would have an impact.

The Police Federation again provided a reasonably consistent view that at the lower level the matter was not seen as serious at all, certainly below other forms of misconduct for which one could potentially lose one's job.[103] This led onto discussions around sanctions and it was notable that for lower levels of misuse, such as nosiness and friends and family checks, if officers did understand what they were doing was prohibited, they were unlikely to draw the connection between their own activity and the potential consequences. It was felt that this confusion was magnified by a lack of consistency nationally in dealing with computer misuse with different forces (and sometimes different chief officers within a force) providing varying sanctions for similar conduct. The Federation view however was that if there were greater understanding of the sanctions, criminal implications, and the loss of employment possibilities of lower level misuse, it would lead to a reduction in unauthorised checks.

[102] Whilst lower level misuse is likely to be dealt with internally, due to the wide parameters of the Computer Misuse Act 1990, it may also constitute a criminal offence.
[103] The analogy provided by many was that of drink- driving. Whilst individual circumstances are considered it is generally the case that officers convicted of this criminal office are dismissed from their force.

All of the disciplined officers interviewed recognised that for conduct at the higher end of the seriousness hierarchy computer misuse was very serious and could lead to dismissal and criminal prosecution which may result in imprisonment. At the lower level of the hierarchy the converse was true, with the majority of interviewees stating that at the time of their own misuse they did not appreciate that what they were doing was particularly serious. A number of interviewees provided confused responses in this area, as whilst they had previously maintained that they did not know what they were doing was wrong, here some stated that they believed the maximum sanction, if they were caught, could be a telling off, and they had been surprised to be served with notices telling them they were under investigation for Gross Misconduct. Generally the officers reported that having seen what had happened to them, some of their colleagues were now more conscious of the seriousness of computer misuse, but they maintained their view that the vast majority of officers still had no idea of the potential consequences of their actions.

Interview group summaries

National leads provided a generally consistent view on impacting factors albeit with some disagreements. They were, for the greater part of the view that seriousness of computer misuse depended on the level within the hierarchy, ranging from general nosiness as a motivation at the lower end being the least serious, through to the selling of information to criminals at the higher end being very serious. Generally they saw the risk of being caught as a significant inhibitor to computer misuse and that employees were for the greater part aware of what they could and could not do due to education and training provided by forces. For those who were caught at the lower

level of the hierarchy and who had retained their positions within policing very limited stigma was perceived.

Investigating officers provided consistent views in some areas such as their perceived scale of the problem and motivations, all agreeing that the reported incidences were likely to be significantly under estimations and that the most prevalent motivation was curiosity or the protection of family and friends. They were likewise all of the view that the greatest inhibitor to misuse was fear of detection and the potential consequences. The interviewees were less cohesive when it came to the matter of the likelihood of being caught but did agree most employees believed this to be greater than it actually is. The group again identified different levels of seriousness in misuse with different responses in areas such as stigma and ease, depending on the perceived level. The group were consistent in their view that the concept of a '*Genuine Policing Purpose*' was not well understood and that clarity in this area would be likely to reduce incidences of computer misuse, albeit by removing a potential defence rather than it being purely an educational issue resulting in less people making a mistake.

The Police Federation's view as provided by this interview group is firmly that the biggest impacting factor in computer misuse is that of knowledge and awareness by officers. They advance that the majority of misuse is at the lower level and within this subset the majority of this is due to officers failing to understand the limitations placed on them by the requirement for a '*Genuine Policing Purpose*'. Investment in this area is something that they see as key to impacting upon the issue. Whilst the Federation acknowledge that the likelihood of being caught carrying out a few unauthorised checks is quite low, they believe that generally officers on the street are

of the view that it is in fact quite high. Raising the perception higher has the potential in their view, to deter more officers. Significantly and in support of both of the above views, the Federation point to the difference in attitudes towards misuse of the PNC compared to other intelligence systems; the limitations of PNC use being subject of in depth training and repeated reminders from the moment an officer joins a force as well as overt daily audits.

Those officers who have been subject to disciplinary investigations generally portray a consistent view in a number of areas, this is most notable in the 'awareness' factor, where the view is that prior to being disciplined they had a very low awareness of what they could and could not use police systems for. Significantly disciplined officers report that both they, and their colleagues, are very well aware that the likelihood of being caught for computer misuse is very low, and that they themselves were unfortunate in this respect to be investigated for some other matter, which led to their own detection. They are likewise clear that the majority of their colleagues have no understanding of how serious computer misuse is and the potential consequences.

Summary

Having examined each of the groups individually it is helpful to pull together the responses from each interview set in table form to consider the '*headline*' responses.

Table 6- Comparison of impacting factors by research group

	National Leads	Investigating Officers	Federation	Disciplined Officers
Perceived scale of misuse compared to source data	Much Higher	Much higher, one estimate ranging from 6% to 10% of employees, another putting the figure at 25%	Much Higher	Much higher
Perceived awareness of wrongdoing	Split – BL and NF of the view that staff were aware of acceptable use, JF and GH of the view that at lower end some confusion existed	Split – generally staff aware but the group did believe that there was some confusion around the term 'Genuine Policing Purpose'	Low – Generally officers not aware that what they are doing is wrong at lower level. AT higher level all aware	Lower level – low, higher level high
Perceived fear of being caught	High	High	High at middle ground. Lower level no awareness, higher level general arrogance that won't get caught.	Low – those at lower level had limited awareness at higher level , an acceptance that will get caught at some point
Perceived Awareness of sanctions	High	High	High – Fear of criminal conviction and loss of job being shown as main inhibitor. Low- Limited understanding	Prior to misconduct – Low, but currently high
Perception of likelihood of being caught	Generally employees feel that there is a high likelihood of being caught and are aware of audits taking place.	Generally High, in contrast to the reality	General perception that likelihood is high, in contrast to reality	Low
Ease	Very Easy	Very Easy	Very easy	Very easy
Stigma	At high level some agreement that stigma was evident. Lower level split, BL and NF says, yes some, GH and JF say not.	At high level yes, at lower level none "There but for the grace of God go I" attitude.	Some but generally rank dependant and more organisational than from individuals.	Some evidence at lower level, Yes ta higher level
Perception of seriousness	Dependant on level. At high level very serious, at lower level not taken seriously at all	Dependant on level. At high level very serious, at lower level not taken seriously at all	Low level not at all serious. High level very serious	At time of misconduct generally low (other than high level). At time of interview universally high

As can be seen at the '*headline*' level there are a number of similarities in the responses by each group. Even at this high level however it is possible to see a number of differences in opinion.

In the next chapter the author seeks to explore in greater detail each of the impacting factors in turn, discussing each group's response against the backdrop of their own sub-set's position within the organisation, their culture, their proximity to those who actually commit the disciplinary breaches, other factors which may influence their perspective, as well as existing theory in this arena.

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 6
Discussion

Overview

In this chapter the author draws together the previous findings and discusses the competing or consistent positions advanced by interview subjects in order to inform his assertions in the final chapter by way of conclusion. The data gathered will be considered against the backdrop of a number of factors including the cultural perspective of the individual or their organisation, the proximity of the individual to the 'coal face' of corrupt acts, differences and similarities between groups, and established theory already discussed previously in this work.

In the first section of this chapter the author formalises the impacting factors raised during the interviews and compares these to draw out similarities and differences put forward by different interview subjects. In the second section, the views of interview subjects are compared to previous studies into both police corruption and computer misuse by returning to the three areas of 'definition and understanding', 'types and typologies' and 'causes and recidivism' that were explored in the literary reviews. In the final part of this chapter the author seeks to draw all aspects of the discussion together and categorise the identified impacting factors according to the weight and benefit they may afford in preventing police corruption, to provide a platform for the conclusion of this work in the following chapter.

Impacting Factors

Throughout the data collection exercise a number of factors were identified and explored which had the potential to impact on the propensity to the misuse of police computer systems. These have already been presented in a table towards the end of the previous chapter, but are reproduced here for ease of reference;

Table 7 – Impacting Factors identified by this research

Impacting Factors
Awareness of the fact that a check was prohibited
Perceived fear of being caught
Perceived Awareness of Sanction
Perception of the likelihood of being caught
Ease
Stigma
Perception of seriousness

The author now moves to examine each of these in turn to discuss the different perspectives offered on each by the different subject groups.

Awareness of the fact that a check was prohibited.

The issue of awareness as to whether particular use of a police computer system is allowed is one that splits neatly between the seriousness hierarchy which has previously been outlined. From data gathered during the interviews it is clear that all respondents are of the view that activity at the higher end, such as gaining information to pass to criminals to assist them in their crimes is unlawful and itself a

criminal offence. There was no confusion as to the fact that the organisation would prosecute officers for such behaviour and that officers would lose their jobs. The Police Federation perspective on this end of the hierarchy is understandably clear in that those engaging in this level of misconduct are fully aware of what they are doing and are justifiably labelled as corrupt. This firm perspective from an organisation whose responsibility includes representing officers in such circumstances, may seem to prejudge some of their members and even deny them the opportunity of a defence in certain circumstances. Any other position however, is likely to be seen as tenuous and may have the potential to discredit other more viable positions for which the organisation seeks public support.[104]

At the other end of this hierarchy sits the lower level computer misuse for which opinions are noticeably divided. The national ACPO lead is of the view that forces have undertaken work such as training programmes, education and the publication of disciplinary sanctions which has led to staff understanding the limits of the checks that they may undertake. This was a view shared by the SOCA lead for counter corruption, although he did believe that organisations could do more to raise awareness. Both ACPO and SOCA represent the 'internal' perspective of corruption at a national level and must be seen against the temporal backdrop of concern and to a certain extent, criticism of forces for the high profile cases that have recently attracted public and political attention. Whilst the position advanced may well be accurate, it is difficult to see how 'internal' national leads could put forward any different position without an acknowledgement of failings in this area. This position does however conflict with that of the other two national leads who can be seen as external to law enforcement.

[104] The Police Federation frequently seeks public support in areas such as members working conditions.

The CPS view was that there was confusion as to the meaning of the term '*Genuine Policing Purpose*' and that this may lead individuals to unknowingly breach the regulations. Their view is that cases towards the serious end of the hierarchy are the only ones which, in the absence of significant aggravating factors, they would wish to prosecute, leaving less serious matters to internal discipline. Their position around awareness therefore is all important when advancing the view that lower level misuse, whilst still constituting a criminal offence, does not meet the public interest test and therefore should not be subject to prosecution.

Ms Furniss for the IPCC went a step further still, in advancing that she did not believe officers even considered the matter, much less considered their activity against any 'policing purpose' test. This she argued was more to do with current culture and people's relationship with computers and data generically. Ms Furniss' view is somewhat supported by the perspective of investigating officers, as while some held the view that by constant training, along with computer 'pop up' messages, officers generally held a good understanding, the majority were of the view that knowledge was still clouded. Investigating officers also drew a distinction between the cultural norms of different age groups and service bands, again reflecting the view of Ms Furniss that an officer's relationship with modern technology was a significant factor.

Throughout the interviews it was clear that the concept of a 'Genuine Policing Purpose' was poorly understood. Whilst two national leads and a minority of investigating officers were of the view that awareness in this area was satisfactory, the overall position was clearly to the contrary. The Police Federation are robust in their view that there exists no firm definition and the author acknowledges that despite

attempts to identify an existing definition in the course of this research, none has been forthcoming. The Police Federation perspective gains further weight from the views of officers who had been disciplined for computer misuse. Of the seven interviewed only two stated that at the time of their computer misuse, they were aware that what they were doing was a breach of the regulations. One of these officers was a Police Federation representative at the time of this breach.

The author is of the firm view that apart from alleviating a potential embarrassment factor, the disciplined officers had very little to gain or lose from providing anything other than frank responses during their interviews. A number of the interviewees also drew a distinction between misuse of the Police National Computer (PNC) and other systems, stating that they were aware of the limitations of use of that system, but not other local databases. Both the Police Federation and the officers concerned suggested that this was due to long standing training and awareness raising from the day an officer joins the service, along with regular overt supervision and auditing.

Of particular significance to this research were the views of disciplined officers on the subject of awareness. Firstly, none were able to demonstrate any understanding of the concept of a *'Genuine Policing Purpose'* despite the views of some investigating officers. Secondly, as the group closest to the activity itself the author is of the view that perceptions provided here have a greater likelihood of accuracy. Significant among this group's perceptions is the fact that the scale of computer misuse across their forces is indeed endemic, but equally significant is the perception that the vast majority of officers who carry out unauthorised checks are unaware of the fact that they are breaching the regulations. Additionally of the seven interviewees five held

the view that had they been fully aware that what they were doing was prohibited, they would not have undertaken the checks.

Being caught and the sanction

The subsequent three identified impacting factors; those of the fear of being caught, the likelihood of being caught and the fear of potential consequences, are closely aligned and therefore can be dealt with together at this point of the discussion.

Whilst some interviewees saw the fear of being caught as ranking highest as an inhibitor to computer misuse, this view tended to be held by national leads and investigating officers. Of the two 'internal' national leads, both believed this fear to be significant, but mainly due to the potential criminal consequences which could follow rather than any employment sanctions that were possible. For the CPS however whilst the fear of being caught ranked highly, this was due to the potential internal sanctions that could follow, most notably, the loss of job and pension entitlements. This is in keeping with the previously discussed position of the CPS, that criminal prosecution should be reserved for the most serious breaches and lower level activity (albeit still criminal) should be dealt with by way of force misconduct procedures.

For investigating officers the fear of being caught along with criminal prosecution and the resultant loss of job were the greatest dissuaders to computer misuse. Whilst this may indeed be the case, the author notes that for a group of people who have responsibility for identifying and effectively pursuing those guilty of misuse, it would be difficult to put forward an alternative view without acknowledging a lack of effectiveness on their own part. The same observation cannot however be made

towards national leads who hold a far wider remit of prevention rather than just enforcement. Of importance however is the ACPO view that a greater fear of being caught would dissuade more officers. This tends to suggest that officers committing breaches at the lower level of the seriousness hierarchy are prepared to 'run the gauntlet' against a fear of low level consequences. The Police Federation is also of the view that fear of being caught is a significant factor and similar to the views of the Crown Prosecution Service, believe this is due to the potential employment consequences.

The first three groups interviewed were consistent in their view that whilst the actual likelihood of being caught misusing police systems is low, the actual perception by the officer on the street was that it was high due to sophisticated technology and regular audits of computer systems, this in turn influencing the fear of being caught. The author is of the view that this is a particularly important point as intrinsically linked to the fear of being caught is the perception of the likelihood of being caught. If the views put forward by national leads, investigating officers and the Police Federation are correct then the perception of risk coupled with the fear of consequences should be sufficient to influence officers away from misconduct. From information gathered from the final research group, this however does not appear to be the case.

Officers who have been disciplined for computer misuse do not share the views of the other three groups. Firstly the majority of interviewees held very low perceptions of the potential consequences of their actions and were generally of the view that it would warrant a 'telling off' or perhaps a warning, but certainly did not consider it to be job threatening. By definition, in policing circles, if conduct is not seen as job

threatening it is not seen as criminal, as the assumption by most in policing is rightly that a criminal conviction by definition places one's job in jeopardy[105]. The view from this group therefore seems to rebut the views of national leads and investigating officers, as the consequences of being caught do not appear high in the minds of the officers. Additionally at the time of his misconduct, one officer was a Police Federation representative and had been trained specifically in this area to assist others. It is difficult to gauge whether this extra knowledge on his part impacted upon his decision making, as the officer asserts that at the time of his computer misuse he was not aware that the checks he was doing would fall outside a *'Genuine Policing Purpose'*.

The second way in which disciplined officer's views differed from the perception of the other three groups was the likelihood of being caught. Whilst other groups acknowledge the likelihood of being caught is low, their perception is that officers on the street are of the view that it is high; a position it has been suggested is useful to the counter corruption effort. From the data collected from disciplined officers, two points are clear; firstly the officers are aware that the actual likelihood of being caught if one is not being investigated for other matters is very low, they are aware that routine audits are rare and perhaps with a misguided view on the seriousness of their own actions, they are of the view that Counter Corruption Units have greater priorities. The majority of the officers even gave reasons as to why they had been caught such as complaints being made or anonymous information being given to the Professional Standards Department warranting some kind of investigation. Secondly,

[105] The National Police Improvement Agency (NPIA) issues a circular in 2011 reinforcing the standards required for police officers. Page 5 of this circular states *"Police Forces should not recruit those with [criminal] cautions or convictions which may call into question the integrity of the applicant..."* (NPIA, 2011). Whilst this relates to recruitment of officers a similar standard is applied to serving officers.

if the views of officers who have already been disciplined for computer misuse (and therefore by definition have been caught) remains that the likelihood of capture is low, then this is likely to be replicated or even inflated in other officers who have never been caught.

Investigating officers point out that many forces publish details of those officers who have been disciplined and this serves to highlight the issue. The responses from the disciplined officers themselves however, tends to suggest that this has limited impact in that there is a general assumption that those people named were caught because they had come to the attention of the Professional Standards Department in some other way, rather than due to any sort of speculative audit process. Here also the author raises the difference in the overt audit processes of the Police National Computer which it has been argued influence against misuse of that particular system. Officers themselves are conscious of the checks that take place and have probably been asked by a supervisor to account for checks they have conducted. Whilst it would doubtless be easy to fabricate a reason for a particular search this would involve direct interaction with another person in authority, rather than ticking boxes on a computer screen, and may of course be subject to further investigation.

Again of significance from the disciplined officers group is the perception that most people within their peer group are unaware of the likely sanctions of computer misuse. They also state that they do not give the matter much thought, firstly because many do not believe that they are doing anything wrong, but for those who do understand the wrongdoing, they do not believe that there is a high likelihood of being caught. This group were of the view that if the risk of being caught were higher

it would dissuade more people. This is consistent with the view of the ACPO lead, and whilst it tends to suggest a potential solution, it also demonstrates a difference of view in current understanding.

Ease of access

Generally the perception across all four research groups was that computer misuse within the police service is very easy. Some reasons for this were given by both the national leads and the investigating officers in that policing organisations operate on the basis of effective information sharing and therefore this information must be available to individuals for legitimate use. This position is very much borne out by the disciplined officers' group who stated that during their particular activities they used systems to which they had access on a daily basis and would be expected to use as part of their work. Whilst the view that the activity itself is easy was clear, national leads did draw a distinction between matters at the higher and lower ends of the seriousness hierarchy. Here the interviewees were of the view that it is more difficult to gain access to more sensitive information, firstly because in order to gain access to the more sensitive systems, officers are vetted to a higher level, with enquiries made into their backgrounds, finances and associates.

Likewise, at the higher levels of criminal investigation not all information is readily available, and information relating to sensitive investigations is not routinely searchable, and is generally only available to those actively engaged in an enquiry. An additional safeguard here, being the flagging system which alerts investigating officers

to anyone else's interest in their work.[106] Whilst the author has some sympathy for the second point made, it is clear that vetting levels alone do not provide a safeguard against computer misuse. This is apparent from the fact that one of the disciplined officers was at the time of his misuse, an officer within Special Branch, an area of policing with the highest vetting levels.

The Police Federation group also raised the issue that ease related not only to an officer's ability to conduct a search but also to their ability to cover the fact. Interviewees highlighted the fact that it would be very easy to find a computer terminal where a colleague had left themselves logged on, and conduct a search on another user's account if one were of a mind to do so. The author is of the view that if this point is correct it adds significant weight to the Police Federation's argument that the vast majority of officers who breach the regulations do so through lack of knowledge, as if officers were aware that a search was prohibited it would be prudent to conduct it using someone else's account. This point was not made by either national leads or investigating officers.

The fact that the vast majority of interviewees were of the view that the scale of computer misuse is high, ranging from 'beyond the source data presented' to 'endemic' would in itself suggest that the practice is relatively easy. Likewise the assertion by the Police Federation and confirmed by disciplined officers that they had undertaken checks in some cases by accident, by 'clicking on links' again adds weight to this suggestion.

[106] The flagging system is widely used in sensitive investigations in that it allows officers to be informed if anyone else does a check of the subject of their enquiry, but does not provide any information to the person conducting the search. This allows investigating officers to make contact with the searching officer to ensure no conflict of enquiries has emerged.

Whilst interviewees were split as to whether making access to computer systems would deter misuse, it was generally advanced that it would be difficult to do so without hindering legitimate use and therefore the disadvantages of such action may outweigh any potential benefits. Additionally the Police Federation were of the view that officers are generally resourceful and for many, once they had set their minds on abusing a particular system they would generally find a way.

Disciplined officers themselves echoed the views of the Police Federation, that *"you could put a brick wall in front of some officers and they would still get through it"*, but for the greater part they were of the view that if it were more difficult it would prevent some of the lower level computer misuse, particularly if a reason had to be provided for each check as is the requirement for the Police National Computer. This prevention could be due to a reduction in the number of officers ignorantly falling foul of the regulations, likewise it is possible that with the removal of the 'defence of ignorance' officers may feel that it is more risky to carry out unauthorised checks. If the Police Federation's view is correct and the majority of misuse is due to a lack of awareness however, the former is likely to account for the greater part of any reduction.

Stigma[107]

The issue of stigma was discussed with all interview groups. For the greater part it was felt that there was very limited stigma attached to those guilty of computer misuse, other than at the higher end of the hierarchy. Disciplined officers who had

[107] For the purpose of this research the terms is used to describe any sense of disgrace or shame either on the part of the subject and his or her own perception or on the part of others who know or work alongside the subject as a result of their actions. A Typical manifestation of such stigma maybe reluctance by others to work with a subject or to provide a subject with information that they would otherwise be entitled to, due to a lack of trust.

remained in the police service however provided a slightly different perspective, in that whilst they were not aware of any stigma towards them personally and did not feel that they had been treated any differently by colleagues following their misconduct case, they did report their own feelings that people had lost trust in them and that they held concerns at being seen as corrupt. Whilst stressing that nothing said or done by other officers reinforced these feelings, one officer stated that returning to work following a period of suspension was '*the hardest thing she had ever done*'. (Officer 'C')

In addition to individual stigma the Police Federation were of the view that organisational stigma could be an issue. All of the disciplined officers interviewed as part of this research were Constables and none indicated any view that they held career aspirations which had now been damaged. The point is however well made in that whilst a disciplinary sanction may be counted as 'live'[108] for a finite period of time, the fact that an officer has been found guilty of computer misuse may well have a bearing on his or her ability to obtain higher levels of vetting clearance for the rest of their service. Whilst this would not necessarily impact on promotion prospects in any but the most senior of ranks, it could prevent work in any department dealing with sensitive intelligence. The author acknowledges however that where such a discipline history is legitimately applied it may be rightly seen as a consequence of the original misconduct. Where it is applied illegitimately by individuals in selection processes on the basis of prejudice it may more properly be viewed as 'organisational stigma'.

[108] Generally a finding of misconduct remains 'current' or 'live' for a period of 18 months. During this time restrictions are placed on the officer's ability to transfer between roles as well as apply for promotion.

Whilst the author acknowledges the lack of stigma reported by interviewees, the internalised feelings reported by some may be of significance to preventing future computer misuse. Disciplined officers' experiences, if shared, may have the potential to deter other officers and although perhaps better described as a legitimate consequence of misuse, the resultant impact on careers for those who do remain within their force could also provide a disincentive.

Perception of seriousness

The issue of seriousness goes to the heart of the hierarchy discussed in virtually all of the interviews conducted. At one end of the scale, conduct which involves assisting criminals is seen as highly serious, whilst at the other end of the scale nosiness and checks on one's own family are generally seen as less serious. For the greater part, the first three research groups were consistent in their perception as to how seriously officers on the street believe the matter to be. Some drew distinctions with human frailty rather that wrongdoing, and one investigating officer suggested officers' attitudes towards those who are caught is similar to a *"there but for the grace of God go I"* attitude, indicating that it is not taken particularly seriously at all, a position which is given some weight by the view of the Crown Prosecution Service that lower level conduct should be dealt with internally. Other interviewees compared it to speeding, in that everyone does it but some people get caught. To provide some sense of measure the Police Federation commented that it was seen significantly below the level of drink-driving, an offence for which police officers have traditionally lost their jobs. This parallel may be valuable in preventing computer misuse, in that the issue of drink-driving has not always been seen as seriously as it is today. Some 25

years ago the practice was widespread but with more and more officers losing their jobs as a result of conviction the practice became less acceptable and frequent. The similarity ends of course when the issue of awareness is considered.

Disciplined officers themselves bear out the views provided by the first three research groups in that almost universally they did not appreciate the seriousness of their actions and certainly did not realise that they put their employment in jeopardy. One officer in particular was firm in his view that at the time of his misconduct he believed that provided he did not give the information he found to anyone else or act upon it, the matter was not a serious one at all. Both the Federation and disciplined officers were of the view that forces had not done enough to communicate the seriousness of computer misuse to employees.

Whilst national leads and investigating officers were not asked directly if they felt this was a fair criticism, it is apparent from responses provided to questions around general awareness that they hold a perception that organisations do effectively provide this message, if only by publicising sanctions given to other officers in computer misuse cases. This therefore raises the question as to whether the issue of seriousness and its impact on the number of people misusing systems is an extension to the issue of general awareness. Taken at face value it may appear that the issue of seriousness can be categorised as an extension to the awareness factor previously discussed, in that whereas a number of officers maintain that they breached regulations due to a lack of awareness of the limits of permitted use, others have breached the system due to a lack of awareness as to the seriousness of such conduct. The author is clear in the view however, that there exists a significant difference in

thought processes between those officers who have no knowledge that what they are doing is wrong, and those officers who recognise what they are doing is wrong but continue regardless due to the lack of knowledge as to the seriousness of the action.

The matter of perceived seriousness is an important one for this research as all four research groups are of the view that if the seriousness level of computer misuse were more widely understood it would result in fewer people breaching the regulations.

Having considered the impacting factors against the responses given by the four research groups it is now useful to examine the different perspectives against previous research in this area to see if existing theory provides a greater insight into the validity of the views expressed or whether it calls them into question.

Existing Theory

In order to provide an effective interpretation of the data collected for this research the author now turns once again to the relevant literature already outlined within chapters 2 and 3. Here he compares responses given by interviewees to previous findings and draws comparisons and differences to further advance this area of research. Before examining in detail previous theory however, the author notes a number of significant differences between past work and this particular research.

Firstly in all of the previous studies the nature of police corruption appears to be a group activity, with a number of officers, (or even whole teams) being involved in relatively well organised systemic operations. This is the case for academic work, internal reviews and journalistic material, and is likely to have impacted upon the popular perception of police malpractice in the eyes of the public. From the responses

obtained in this work the author is clear that computer misuse is for the greater part a lone activity and even where those responsible have been fully aware of their actions, there has been no suggestion of collusions with others within the police service. This is significant because whilst there may be some group acceptance of the activity which fosters an environment of acceptability, there is no evidence that peer group pressure features as an impacting factor in this type of malpractice, whereas for previous studies this has been a core tenet.

Secondly the greater part of previous research has involved a financial motivation. This is seen in most work, but is particularly noticeable in the journalistic material, with other evidence coming from academic studies. This again has undoubtedly shaped the popular perception of police corruption. The one exception to this being Stoddard's 1968 study of a single corrupt officer, who was firmly of the view that money was not a great motivator. (Stoddard, 1968). This work has shown that financial reward was consistently absent as a motivating factor from all interviewees. The idea of financial motivation cannot however be dismissed out of hand, particularly in light of recent public concerns and apparent media leaks to the press involving the investigation or detention of famous people. Likewise it is significant that both the ACPO national lead and investigating officers indicated spikes, (sometimes by hundreds of officers) in computer misuse surrounding the arrests of celebrities.

The issue is however placed back into perspective by the findings of part 2 of LJ Leveson's enquiry. Here Leveson clearly expresses that the perception of police officers selling information may have been exaggerated in the minds of the public; *"Taking the subject of 'leaks' generally, I must start by making it clear that although*

Operation Elveden (concerned with bribery of public officials) is proceeding, the Inquiry has not unearthed extensive evidence of police corruption nor is there evidence satisfying the standard of proof that I have adopted, namely the balance of probabilities, that significant numbers of police officers lack integrity in one or more of the respects I have examined. Speculation, suspicion and legitimate perceptions may abound and troubling evidence has been identified in a limited number of cases (with journalists tenaciously protecting their sources), but the notion, as a matter of established fact, that this may be a widespread problem is not borne out. The scale of the problem needs to be kept in proportion." (Leveson LJ 2012. Exec Summ. para 91. P21). It would appear therefore that other explanations for spikes in computer misuse relating to celebrities are more likely, namely the ideas advanced by investigating officers and the Police Federation, such as kudos within a peer group or nosiness, coupled with a lack of appreciation as to the legitimate limitations of computer searches.

Finally it is apparent that the majority of academic work in this arena is dated, and whilst recent efforts have been made to modernise some of the work to incorporate new deviant practices, *(Punch, 1985 and 2009),* it is clear that practices involving new technology are not fully integrated into corruption theory. This work however is focused purely at the misuse of new technology. This point may or may not be relevant depending on one's view of the significance of motivation in defining corruption and whether one takes the view that new technology is a means to conduct traditional corrupt practices more effectively, and therefore represents one of Wall's 1st or 2nd generation misuses, or whether the practice is a corrupt activity in

its own right and therefore an example of a 3rd generation offence. This is explored further in the coming pages.

Whilst a number of differences are apparent, an overriding number of similarities such as the consistent nature of the policing function, the organisational structure, hierarchy and makeup, the unique position of trust within the community and the close knit working environment of officers, lead the author to the firm view that previous studies do remain relevant, but in need of some interpretation against the backdrop of modern technology and working practices.

With these factors in mind it is now useful to examine the interview responses against the backdrop of the three principal areas of previous academic study already examined; definition, typology and causes.

Definition and Understanding

Earlier in this work the author outlined the fact that there did not appear to be any agreed working definition of police corruption in existence and whilst a number had been put forward these tended to relate to individual studies rather than being universally accepted. In this research, which represents a small and distinct area of deviant practice, a similar position is evident, in that there does not appear to be an agreed definition of a *'Genuine Policing Purpose'*, a fact which has been argued by many as contributing to the number of officers who had unknowingly breached the regulations. This similarity appears to end at this point as in none of the previously reviewed research is it argued that officers have entered into corrupt practice because they were unaware that it was wrong.

The issue of computer misuse however is clearly not restricted to policing and is apparent in other areas of the public sector as well as private industry. Whilst the lack of a firm definition for either police corruption or a *'Genuine Policing Purpose'* is evident in the policing domain, this is in stark contrast to the 'black letter law' definition of computer misuse provided in legislation and readily available to all. At first glance this may seem to present a solution, but with the key requirement of a legislation breach being that the activity is *unauthorised,* and the matter of authority being dependant on whether the computer use was for a *'Genuine Policing Purpose'* it can be seen that this does not move the argument any further forward. The criminal law may however hold a potential answer.

The assertions by the Police Federation that officers generally are unaware of the restrictions placed upon in the use of computer systems could be overcome if one takes the view that the practices fall in the criminal arena rather than the internal misconduct arena. This view is taken by both Wilson and Stoddard in their previous studies. (Wilson, 1963),(Stoddard, 1968). Using the conclusions of Wilson's work computer misuse would constitute a criminal offence and therefore be outside any internal definition of corruption. Likewise, whilst Stoddard would argue the fact that the subject is a police officer is relevant, this would only be to further categorise the offence as 'Blue Coat Crime' in that it depended upon one's position in the police force to undertake it (Stoddard, 1968). Both however are clear that the activity is a crime and should be dealt with criminally. This rather clinical position poses a greater risk to the Police Federation's position and in particular its members, in that an established principle of English jurisprudence is that ignorance of the law does not

constitute a defence.[109] This position would tend to push the emphasis back onto officers themselves and the Police Federation as their representative body to ensure that they take responsibility for their own knowledge in this area.

The author makes three points here which lead him to some sympathy for a slightly different perspective; firstly, in many instances organisations provide requirements for officers which have a tendency to blur the otherwise clear boundaries. Such requirements may be the compliance with a 'Notifiable Association Policy' or even a necessity to learn how to use the computer systems and conduct searches to familiarise oneself with it. Secondly, the two principal pieces of legislation that relate to computer misuse are section 1 of the Computer Misuse Act 1990 and section 55 of the Data Protection Act 1998. Both of these pieces of legislation contain requirements that for a person to be convicted they must be either aware that the access is unauthorised (in the case of the Computer Misuse Act) or hold no reasonable belief in law that they had no right to obtain the data (in the case of the Data Protection Act).

These provisions appear to work in the favour of officers who claim ignorance of the provisions, and they doubtless influence the decision making process of the Crown Prosecution Service in coming to prosecution decisions. Forces are however generally able to demonstrate some knowledge from initial training, that officers were aware to some degree of the limitations placed upon them. This is particularly the case when individuals search on celebrities as it is difficult to argue any lawful purpose or authority in such circumstances. As a third point, the author highlights the previously

[109] "ignorantia legis neminem excusa". Whilst ignorance may not constitute a defence it is likely to constitute mitigation in certain circumstances.

discussed principle of English law of *'De-mimimis'*[110], and that the vast majority of computer misuse in the police service occurs at the lower end of the seriousness hierarchy. These three points lead the author to the view that the balance of responsibility should be pushed back towards the organisation to a position where the burden is at least shared rather than falling solely on the individual. The author believes that whilst not discussed in interviews, the Police Federation at least acknowledges some responsibility in making its members aware of the limitations of computer use, as within the last three years they published a document providing legal advice as to what would and would not constitute lawful access. The document also indicated that where officers had deliberately undertaken a course of action against the advice contained within it, the Police Federation would not provide legal representation. The document itself was published by the Police Federation centrally but there is some evidence that not all force's local Federation offices circulated the guidance. Whilst not all officials of the Police Federation may have agreed with the National Executive position the initiative itself reflects the responses provided during the interviews for this research in that rather than trying to make access to systems more difficult, efforts would be better employed in training and education.

The issue of definition however, appears to be twofold in the case of computer misuse, in that all interviewees acknowledged a hierarchy between higher and lower levels of corruption. This is in keeping with a number of existing views, most notably that of Kleinig in his 1996 paper. In this he asserts the view that police corruption relates to motivation rather than any act itself (Kleinig, 1996) and this lends itself neatly to the distinctions drawn by the four interview groups. Activity seen at the

[110] [110] 'De-minimis non curat lex' – *The law does not deal with trifles.*

higher end of the seriousness hierarchy by participants in this research related to the sale of information to assist criminals by disrupting police enforcement. The author is of the view that any activity with this motivation is plainly, and as a matter of common sense for police officers prohibited. This therefore explains the significant difference in understanding between the higher and lower levels of computer misuse, in that the actual computer misuse itself is incidental to the objective or motivation. This allows computer misuse within the police service to be categorised according to Wall's *generations of crime. (Wall, 2007:Revised 2010).* Offences which take place at the most serious end of the hierarchy such as the disruption of justice or the sale of information to criminals would probably fall into the 1st generation, in that those crimes which would still be committed without a computer, albeit they are made easier due to the instant access to information as opposed to painstaking search through manual records.

At the other end of the scale offences lower down the seriousness hierarchy such as browsing information with no further intent would probably constitute 3rd generation crimes, in that they are only committed in 'cyberspace'. A difficulty arises however when considering offences midway in the hierarchy such as the accessing of information to protect friends and family or to assist in personal crises such as divorce. These practices do not conformably sit within the 2nd generation of crimes which Wall states are traditional crimes with new opportunities due to the information age.

The author advances however that if the word '*crime*' is removed from Wall's commentary and replaced with the word '*action*' it may be sufficiently open to encompass such activity as 2nd generation; Protection of friends and family, and

actions to prepare for divorce and custody battles are traditional, but new opportunities have now developed. For consistency, the word 'crime' can also be replaced in both the 1st and 3rd generations, with limited impact on the definition in these circumstances. The division of incidents of computer misuse in this way is borne out not only by the consistent views of interview participants but in particular by investigating officers who drew a distinction between external and internal influencing factors; external relating to assisting criminals and internal relating to the officer themselves.

If one accepts the position that police computer misuse does fall onto either a higher or lower end of a hierarchy the position of Her Majesty's Inspectorate of Constabulary (HMIC) in both the 1999 and 2006 reports is relevant. In the 1999 review the organisation was firm in its view that lower level corruption was as significant an issue as higher level asserting; *"... some people expressed the view to the Inspection Team that the Service should be concentrating on combating hard-edged corruption, and not be concerned about minor perks. The Director General of The National Criminal Intelligence Service, however, expressed his belief that, 'Corruption results from a failure to maintain integrity.' Her Majesty's Inspector firmly shares this view and considers it will be far more difficult for corruption to flourish if gifts, gratuities and perks are seen as totally unacceptable within the Police Service." (HMIC 1999, p48).* In the 2006 review HMIC outlined for the first time that *"the rise of information leakage was a significant problem" (HMIC 2006, p7).*

From the interviews conducted for this research, the author has already identified that lack of awareness as to the prohibition of an activity is a substantial impacting factor

in computer misuse. Likewise, the issue of lack of awareness of the seriousness of the act featured highly. These two impacting factors coupled with the existing research undertaken by others lead the author to the view that computer misuse falls into categories of higher and lower level seriousness but this is based on motivation rather than the act itself. By extension the author is of the view that any number of checks without the required motivation cannot constitute a higher level of seriousness or the '1st generation' label.

The author is at pains to point out however that this does not mean that repeated checks are no more severe than a single check or that repeated lower level abuse of the system cannot be considered gross misconduct, (as other variables such as public confidence and the reputation of the organisation come into play here), merely that in the definitions used within this research, motivation is all important in deciding a position within the seriousness hierarchy. Whilst the issue of awareness as to the legitimacy of an act at the lower end of the scale is significant the author believes that responsibility for raising awareness should be shared between both the organisation and the officers themselves.[111] A firm definition of a *'Genuine Policing Purpose'* would doubtless assist in this area but the author acknowledges that such a definition would need to come from or at least be accepted by the organisation in the first instance to hold any validity in future disciplinary enquiries.

[111] Here the author refers to the 'Organisation' and 'Officers' but includes investigating officers as representatives of the organisation and the Police Federation as representatives of the officers.

Typologies

Whilst a number of typologies exist for police corruption and have already been discussed earlier in this work, the author is of the view that only a limited number are relevant to this research.

In the area of police corruption, those provided by Barker and Roebuck in 1973 (as amended by Punch, 1985), examining types of corruption, Punch 1985 examining different characteristics of deviant officers, and that provided to the Knapp commission during their enquiry in 1972, looking at the broader types of officers involved are significant. In the area of computer misuse the previously discussed generation typology of David Wall *(Wall, 2007)*, is relevant.

Barker and Roebuck (as amended) provide nine types of police corruption ranging from the receipt of free drinks up to the planting of evidence to 'frame' suspects for offences. The categories appear strongly aligned to the idea of personal gain either through theft or as a reward from third parties for misconduct. The typology itself includes one category of particular relevance to computer misuse and is denominated 'The Fix'. This individual is involved in the undermining of criminal investigations or the losing of evidence. The author is of the view that whilst this category may reflect those officers undertaking computer misuse towards the serious end of the hierarchy, lower level misuse does not appear to feature. The author notes however that this typology was last updated in 1985 when Maurice Punch added the ninth category to allow for the planting and adding to evidence. *(Punch, 1985).* This was seen as necessary to account for developments in drugs enforcement. With further

developments since then in the area of information technology further amendments are required to incorporate new types of police deviance.

In addition to amending a previous typology Punch provides his own view of the different characteristics of officers involved in corruption. Of the ten profiles outlined by Punch, it is apparent that none are an exact fit for those undertaking computer misuse. One category however is denominated 'Mister Average' who according to Punch was *"typically laid back, but did undertake some mild 'grass eating' (see post) but stayed out of relations that could lead to more serious forms of deviance" (Punch, 2009 p23.)* The author highlights two points from this classification; firstly, the suggestion that this characterises 'mister average', tends to suggest a more widespread and customary view of low level corruption, reinforcing the views of Stoddard and a number of the interviewees. Secondly, the description highlights the fact that low level corruption can be an individual activity and need not be associated with group deviance. This firmly reflects the nature of computer misuse which from the findings of this research is invariable a solitary act.

The 1972 Knapp commission heard evidence from a number of sources, but one officer in particular provided an analogy of officers to different animals. In this he outlined three categories, 'grass eaters', 'meat eaters' and 'birds'. Officers seen as 'grass eaters' were involved in the lowest levels of corruption, perhaps accepting small gratuities. 'Meat eaters' were seen as hard core corrupt officers seeking to capitalise on their position for financial gain at every opportunity, whilst 'birds' soared above corruption but did nothing to prevent it. Within this category were supervisors who were wilfully blind to the activity of their subordinates.

The author is of the view that the analogy to 'grass eaters' and 'meat eaters' is effectively a comparison to the seriousness hierarchy for computer misuse. The position of 'birds' in this analogy is less clear but would include those disciplined officers who reported that, having been through the process themselves, notice far more of the activity in others, but do nothing to advise against it or report it. With the practice of computer misuse being reportedly so widesprerad, it would seem credible that a number of those who either continue to do so, or have previously done so, have been promoted to supervisory ranks. The analogy of birds would also incorporate supervisors who chose to ignore the practice.

This typology is relevant not only to the officers who undertake computer misuse but also the impacting factors discussed during interviews, most notably that of ease and stigma. If a prevailing 'bird' attitude is apparent, (or even perceived) it adds weight to the idea that the practice itself is stigma free, even when caught. Likewise, whilst the act itself has universally been categorised as easy by all interview groups, the absence of any overt checks to prevent it has been highlighted as contributing to this ease, by the distinction made between local databases and the Police National Computer which is subject to regular overt audits.

The Knapp commission also explored the suggestion of 'bad apples' as a type of officer who undertakes corrupt practice. The commission was fierce in its rejection of this idea; *"According to this theory, which bordered on official department doctrine, any policeman found to be corrupt must promptly be denounced as a rotten apple in an otherwise clean barrel. It must never be admitted that his individual corruption may be symptomatic of underlying disease..." (Knapp, 1972 in Newburn 1999. p15).* This

position has been subsequently supported by academic research, most notably Punch in 2009 where he is firmly of the view that *"The police organisation is to 'blame' for much corruption; it has failed to see it, to prevent it, to control it and to stop segments of the organisation entering recidivism" (Punch, 2009. p48),* reflecting his ideas that bad cops are not born but are made by the environment in which they operate.

Whilst it may expected that thinking had moved on since the Knapp commission and the 'bad apple' analogy the author notes that it can still be seen in official statements such as the ACPO response to recent HMIC and IPCC reports *"This review [...] found no evidence of systemic corruption in policing, but individual cases where police officers let their colleagues and the public down.".* (ACPO 2011)[112]. It is likewise evident to a lesser extent in Police Federation response to allegations from national newspapers *"I must object, on behalf of all police officers across England and Wales, to the grossly offensive and incorrect assumption that the police service suffers from wide scale corruption".* (Police Federation 2011)[113].

Here the author does not advance the view that either agency is wrong, moreover that with the nature of computer misuse being for the greater part a lone activity, the police service may be seeing the re-emergence of the 'bad apple' as opposed to group deviance. This is a difficult concept to fully integrate into existing theory as traditionally 'bad apples' have been seen as individuals working alone and in particular, in the minority.[114] In this thesis it is argued that whilst the idea of lone working remains consistent, the scale suggested by interviews in this work is far

[112] http://www.acpo.presscentre.com/Press-Releases/ACPO-comment-on-HMIC-police-integrity-report-Without-Fear-of-Favour-133.aspx Accessed 20/9/12)
[113] http:///www.metfed.org.uk/news?id?1378 (Accesses 20/9/12)
[114] *".... as a rotten apple in an otherwise clean barrel... " (Knapp, 1972) ante.*

greater. This need not present a problem if one is prepared to extend the traditional understanding of the 'bad apple' and consider that rot may occur in each fruit individually rather than as a result of contagion. If this is the case then it is difficult to advance that there is no underlying organisational cause or disease to explain the separate and individual emergence of deviant practice on such a scale. In this respect the views of Punch on corruption prevention appear evermore relevant and focused at the policing organisation as opposed to individuals, as he asks *"whose duty was it to inspect the fruit and who neglected to apply the insecticide?" (Punch, 2009. p9)*

Causes and Recidivism

In the review of existing literature the author identified a number of competing views as to causes of police corruption. With the benefit of data gathered in this research he now discusses whether any of these lend themselves in particular to computer misuse. Significantly from the research it is apparent that computer misuse at the lower level is perceived by many to be at near endemic levels within the police service. With the suggestion of such wide spread misconduct, the author is in the first instance drawn to 'blanket' [115] theories, such as those advanced by Stoddard in his 1986 work. Here Stoddard put forward three possibilities as to causes of police corruption, firstly that the position is a social norm and is only seen as corrupt in the policing environment where higher standards are expected, secondly that for the average police officer it is not possible to do one's job effectively without breaking the rules, and thirdly that the practice is contagious and brought about by peer group pressure. (Stoddard, 1968)

[115] The author uses the term 'blanket' meaning 'all-encompassing' and explaining root causes rather than individual acts.

Of the three different possibilities the author notes that at no point in this research did any interviewee put forward that officers breached computer usage regulations in order to allow them to carry out a legitimate duty. He therefore considers the second of Stoddard's possibilities not to apply in these circumstances. The first and third ideas however do warrant further exploration.

The idea that computer misuse, or the motivations behind it, may be a social norm again needs to be seen against the backdrop of the seriousness hierarchy. Out of the disciplined officers research group only one was involved with activity at the serious level of the hierarchy and indeed both she and other officers highlighted in their interviews that such activity was rare. Were this view restricted to just the officers themselves and the Police Federation there may be some room to questions its accuracy, it is however shared by both ACPO and investigating officers and the author therefore takes this at face value. With such evidence of limited occurrence it is difficult to advance that it is in fact a normal position, particularly when one considers the motivation associated with the higher level of seriousness.

When considering the lower level offences however some credence may be given to Stoddard's first theory as many of the interviewees indicated that motivations at the lower level included nosiness, general interest and the protection of friends and family. It is harder to exclude these motivations from the general public and therefore the recruitment pool of police officers. Whilst the accuracy of Stoddard's assertion is outside the scope of this research, if it were correct in these circumstances then this, coupled with the access to significant amounts of data that most police officers enjoy, could go some way to explaining the apparent wide spread nature of the activity.

The normality position advanced by Stoddard is consistent with David Wall's view that the information age has created a generation of young people for whom the existence of the internet is a natural state which *"made them feel free to explore, to roam freely, see and experience new things in what seemed to be a new public commons" (Wall, 2008. Pp876)*. This position is supported by Fafinski's demonstration of the rise in internet usage and subsequent rise in computer misuse reports. *(Fafinski, 2008).*

The only interview group to rebut this position was that of national leads who maintained that the biggest inhibitor before considering any other impacting factor was that of individual officer's integrity, which led, in their view to the vast majority of officers having no desire to breach the regulations. If Stoddard's theory is correct then the views of the national leads is in some doubt. Stoddard's view is given more credibility when considered against the comments of the IPCC lead, Jane Furniss in that the problem is amplified by the modern day relationship with computers and information. Ms Furniss suggested that officers do not even consider their actions against what is right or wrong, as the culture within which they have grown up suggests to them that access to data is a natural right whether it comes from open source or internal work systems. Again this is very much in keeping with Wall's assertions and is given further credence still by investigating officers who split officers into service bands suggesting that younger and more recent additions to a force are more likely to abuse computer systems.

Stoddard's third suggestion, that corruption is in fact contagious and brought about by peer group pressure, may have some accuracy but the author does not believe it is a natural fit for the matter of computer misuse and better suits incidents of group

corruption rather than an activity where one acts alone. The author is also of the view that from the data gathered there is limited evidence of officers getting together to search on interesting people or incidents, and whilst a general group acceptance may exist of such behaviour, it would still require an individual motivation such as nosiness or family protection. The author is not therefore of the view that the third suggestion is convincing in the area of computer misuse.

Lawrence Sherman in his 1974 'Sociological Perspective' of police corruption put forward a number of constant and variable features that he maintained came together to create an environment where police corruption could exist (Sherman,1974). Again, the author does not intend to examine the accuracy of Sherman's work, but consider if the features he identified are evident from this research, as this may provide an indication as to the general propensity to computer misuse fostered by the prevailing circumstances and culture.

Sherman's features are broken down into both 'Constant' and 'Variable', with the constant features (Discretion, Low managerial visibility, low public visibility, peer group secrecy, managerial secrecy, status problems and association with lawbreakers) being advanced as always present in a policing environment. Whilst the features themselves were identified in 1974 the author's experience is that these remain current and are therefore taken at face value. The author therefore concentrates on the variable features of 'community structure', 'organisational characteristics', 'legal opportunities', 'corruption controls', 'social organisation' and 'moral cynicism' (Sherman, 1974).

Sherman's 'community structure' relates predominantly to the prevailing political context and officer's 'capture by the political environment'. The author notes that at no time during this research did an interviewee suggest that their misconduct was related to any ideological belief. This was in fact only mentioned by the Crown Prosecution Service national lead as a possible motivation. Whilst the author acknowledges the limitations of this research in the involvement of only one individual at the higher end of the seriousness hierarchy, he is of the view that as the higher end appears to be in such a minority compared to the lower end misuse the feature can be reasonably excluded.

The 'organisational characteristics' of a police force in this context relate to the prevailing culture. Whilst at first sight it is tempting to see this as irrelevant, Newburn in his review of Sherman's' work includes such factors as what the organisation has done to encourage personal development and avoid boredom. *(Sherman, 1974 in Newburn, 1999).* He also reiterates the strong link identified by the Wood commission between the absence of professional pride and the development of corruption. *(The Wood Commission, 1997 in Newburn, 1999).* These issues do appear relevant at both the higher and lower levels of the seriousness hierarchy.

At the lower level, a number of interviewees raised the issue of boredom and nosiness as a reason for computer misuse and whilst this was however always coupled with the lack of awareness factor it remains a valid feature. At the higher level the author is of the view that the sale of information to third parties, or the passing of information to protect criminals and frustrate policing operations, necessarily requires an absence of professional pride, irrespective of what other factors may be present.

The issue of 'legal opportunities' in Sherman's original study related to officers working on the 'invitational edge' of corruption, by which he meant prostitution and gambling. Whilst slightly different in context the temptations outlined in the 1974 study may be seen as akin to the modern day temptations posed by information. This is of particular relevance when seen against the suggested motivation of kudos within a peer group which was advanced by the investigating officers research group. The author is of the view therefore that whilst not an exact fit, allowing for modernisation in interpretation this feature is evident from the research data collected.

The matter of legal opportunities is likewise consistent with causes of computer misuse outlined by Wall in his 2008 work. In this he highlights three potential causes; firstly the perception of anonymity, secondly the perception that perpetrators go unpunished and thirdly the view that victims are vulnerable. *(Wall, 2008)* These three ideas can all be seen to greater or lesser extents in the responses given by interviewees. In the first instance most interviewees recognised that the likelihood of being caught was low in that speculative audits are rarely carried out by forces as they do not have the resources to do so. In this way there exists a perception of anonymity, in that unless an officer is named and suspected for some other matter, there is a very low likelihood of capture. The idea of total anonymity is however not present, as the majority of officers are aware that should attention be directed towards them, audits on their computer usage are possible. In the second instance, and linking firmly to the likelihood of detection is the perception that perpetrators are not punished. Of the disciplined officers interviewed, the majority were of the view that if identified, any punishment would be minimal. Whilst this is undoubtedly a

false perception in relation to internal misconduct proceedings, there is some evidence that criminal prosecutions are often seen against the backdrop of the principle of *'de-minimis'* and offences at the lower end tend not to be prosecuted. These decisions are rarely clear cut as the Crown Prosecution Service wrestles with the competing principle of the public interest in prosecuting offenders exploiting a position of trust, and each case is dealt with individually. It is notable however that of the seven disciplined officers who took part in this research, four were also charged with criminal offences. Finally the idea of the vulnerability of the victims can be seen as an analogy to the vulnerability of the systems and the ease in which computer misuse can be carried out. Ease was universally acknowledged by all interviewees as a constant feature.

'Corruption Controls' is a feature discussed with all interviewees in the form of their perception of the likelihood of being caught and how they believe this may be perceived by the officer on the street. This area in particular demonstrated significant differences of opinion, as well as highlighting an important misconception on the part of both the national ACPO lead and investigating officers. The first three research groups all held the view that the likelihood of being caught for computer misuse if one were not under investigation for any other reason was low, but that officers on the street thought it to be much higher. The view of disciplined officers however was that there was very little chance of being caught for such activity and even if they were, prior to their own discipline case they held the view that the sanctions for such misuse would be minor. The author is of the view that the perception of an absence of corruption controls in this area is as relevant as there being none in place, as without

knowledge of their existence, or belief in their effectiveness they cannot act as a deterrent.

The final two features identified by Sherman, those of the 'social organisation of police corruption' and 'moral cynicism' were not identified during this research. The author notes that no interviewees discussed computer misuse being a group activity or requiring any organisation, neither did it appear that morale played any part in the decision to undertake unauthorised checks, other than where it impacts on professional pride as discussed above. From the research undertaken it is evident that three of Sherman's variable features can be seen in the prevailing environment of computer misuse; 'organisational characteristics' (the absence of professional pride and the existence of boredom), legal opportunities (the temptation of readily available information) and corruption controls (the perception by officers on the street of a low likelihood of detection and low level sanctions).

Already in this chapter the author has advanced that there is scope to impact on organisational issues in order to reduce the incidences of computer misuse. This has been seen in impacting factors such as awareness, (against the backdrop to Stoddard's and Wilsons views that the matter is a criminal one); seriousness (against the ideas of Newburn's that it is recognisable when encountered); and perceived likelihood of, fear of, and sanction for being caught (against Sherman's variable features).

Whilst the issues of root causes of computer misuse have been explored, the matter of continued conduct or worsening behaviour has so far not been examined. In the literary review two models of recidivism were considered: Firstly that of 'Sherman's ladder', whereby as an officer moves from one deviant act to another and climbs a

ladder of seriousness each metaphoric rung requires a new re-evaluation of self, and one's personal moral position to decide whether it is a step one is prepared to take. This Sherman referred to as a police officer's moral career, and it is built on the hypothesis that one deviant act will not necessarily lead to another (*Sherman, 1985*).

The second idea considered was that of Kleinig's 'slippery slope', which suggested that once an officer had undertaken one deviant act, all moral objection to further acts was removed and therefore in the absence of an external intervention an officer would necessarily move to more serious forms of corruption (Kleinig, 1996). The research conducted here tends to indicate that lower level police corruption or deviance in the form of computer misuse is widespread within police forces. Whilst this maybe a relatively new phenomena and require longitudinal studies to fully evaluate, it does not appear to support Kleinig's view that further and more serious corruption will follow as a matter of course. If this were the case, it could be expected that in the 15 years that computer usage has been widespread throughout police services more serious corruption would be evident either in this research or in the findings of reviews by HMIC or the IPCC, both of whom reject the idea of endemic corruption.

Having now considered the relevant existing literature against the data obtained during this research the author has moved full circle, from examining differences, consistencies, and finally returning to significant differences with a view to reconciling them by suggesting an updated understanding of a traditional concept. The author now seeks to close the discussion and pull all aspects together to provide weight to impacting factors and provide a platform for the conclusion of this work.

In Closing the Discussion

In this discussion the author has examined the data gathered against three main backdrops; firstly the prevailing context for the research (along with the political climate at the time of data collection), secondly, the over-arching and political positions of organisations whose representatives took part in interviews, and thirdly, existing literature and previous research into police corruption. Having done so, the author is in a position to return for a final time to the identified impacting factors and place them into a hierarchy of 'impactive weight' and the ability of organisations to use this to counter computer misuse. In doing so, some factors have been joined and presented as a single entity reflecting the closeness of their relationship. Whilst this reduces the overall number of impacting factors identified it provides a clearer perspective on where efforts could be focussed to tackle this form of malpractice.

Awareness of wrongdoing

The author is firmly of the view that the awareness of wrongdoing rates highest as an impacting factor in the area of computer misuse. Whilst there may be further discussion as to whether a lack of awareness allows for the full criminal offence to be made out, it is clear that if success for policing generally is the reduction of unauthorised checks, irrespective of whether they are dealt with criminally, internally, or never discovered, then evidence from this research suggests awareness is the most significant factor. This position is made most vocally by the Police Federation and borne out by disciplined officers themselves, even allowing for some embarrassment factor, consensus is clear. Additionally whilst the national ACPO lead was of the view

that things are getting better, he also acknowledged that raising the awareness would be likely to reduce incidences of misuse.

The author is of the view that that the absence of a firm definition of '*Genuine Police Purpose*' a phrase that is used consistently to bench mark the legitimacy of computer use, is a significant contributing feature in the lack of clarity and awareness of officers. As previously discussed, any definition must at the very least be accepted by the organisation for it to be any value in preventing future misconduct. The author is of the view that even if such a definition is not agreed by the Police Federation, it at least gives a framework of expectation on the part of the organisation and something that can be used to educate officers. In this regard the author agrees with the perspective provided by Punch in that the role of policing the organisation includes 'checking the fruit' and 'applying insecticide'. In this context the firm definition may well represent 'an insecticide to assist in protecting the fruit'.

Perception of seriousness and possible sanctions.

Ranking next according to the interview responses, is the matter of the perception of seriousness of computer misuse by the officer on the street and the potential sanctions. Whilst at the higher level of the hierarchy discussed officers appear to be in no doubt as to the seriousness of obtaining information and passing it to third parties, this appears to be more related to the motivation and its intended purpose rather than the activity of computer misuse itself. At the lower level of the hierarchy it is apparent that officers feel that nosiness, curiosity or the obtaining of information to protect family and friends is a relatively minor disciplinary breach, even less so if the information is not passed to any third party at all. Significantly disciplined officers

were of the view that had they been aware of the seriousness of their actions, in particularly that the matter was job threatening, they would not have carried out the unauthorised checks.

Whilst this area may be linked with awareness the author is of the view that the two impacting factors are separate and distinct, in that the commission of an act due to a lack of awareness that it is prohibited is significantly different from the acceptance that something is unauthorised but continuing as the potential sanction is of little consequence. This 'running of the gauntlet' was alluded to by the ACPO national lead.

Perceived likelihood and fear of being caught

The third most significant area is that of the perception by officers on the street as to the likelihood of being caught and the resultant reduced fear of such an occurrence. This is an area of particular concern as whilst the first three research groups noted that the likelihood of detection was low, they held the view that officers on the street believed that technologically advanced methods were used to police internal systems, and therefore the risk of capture was high. Disciplined officers themselves held no such misconception and were clear in their views that they were unlucky in that they had either been the subject of a complaint or had been investigated for some other matter which led to the discovery of their activities. More significant is the fact that even following their own discipline cases officers retained this idea, indicating in the view of the author that the realisation is likely to be even more evident in officers who had never been caught. All research groups were of the view that if there existed a greater fear of being caught, officers would be less likely to undertake unauthorised activity.

Ease

Whilst it is clear from all research groups that police computer systems can be misused with relative ease the author believes that this particular impacting factor features fourth in his hierarchy. A number of the research groups also highlighted the distinction between the relative ease in misuse of local systems whilst the Police National Computer which was overtly audited was perceived as more difficult. Whilst all research groups suggested that making computer misuse harder would reduce this type of misconduct, the majority explained that they did not see a way in which this could be accomplished. The author notes the points raised and shares the view of Steve Evans from the Police Federation that making access to systems more difficult has the potential to defeat the purpose of the systems themselves, likewise it would in itself be difficult to establish, and ultimately lead to the truly determined corrupt officer finding another way to accomplish the unauthorised searches.

Stigma

Throughout the research the author identified very limited evidence of any stigma other than that which disciplined officers indicated was self-imposed. Whilst it was indicated by a number of interviewees that an increased stigma would reduce computer misuse, this is, in the view of the author likely to be a common sense response as opposed to evidence based. The author points out however that the experiences of officers who have been disciplined may well act as some form of deterrent if shared with other colleagues, particular those who indicate a difficulty in returning to work through their own perception of how colleagues saw them.

The discussions presented, along with the summary of the thesis arguments as to the weight each of the identified impacting factors carry, now provide a stable platform for the following concluding chapter. In this the author attempts to consider how the research conducted here can impact on the established corruption theories already advanced by academics but more importantly how it may be used in a real world application to influence professional policing practice.

Police corruption and computer misuse: an analysis of the contributing factors.

Chapter 7
Conclusion

Thesis Review

In this work the author has sought to open up the often closed world of police corruption and counter corruption as it relates to computer misuse. In the first chapter the author presented a history of police malpractice dating from the inception of the new police in 1829 through to modern day, showing how media exposés have shaped both public opinion and prompted action, either internally by the police themselves in the early years, and most recently at government level.

The literary review in chapters two and three examined existing theory, firstly in relation to police corruption and secondly into computer misuse. In both these areas the author looked firstly for a firm definition, secondly at types and typologies and thirdly at causes. Literature reviewed came from the academic world, internal reports/reviews and journalistic material. In the police corruption arena, the absence of a firm definition was highlighted[116] along with perhaps one of the most well-known typologies, that of Roebuck and Barker 1973 as amended by the work of Maurice Punch in 1985[117]. As to causes, significant was the work of Lawrence Sherman in 1974

[116] *P25 ante.*
[117] *P30-32 ante.*

outlining constant and variable features in police corruption[118]. In the area of computer misuse the author reviewed definitions from both previous academic works, (most notably from Martin Wasik in his 1991 article[119] and Stefan Fafinski in his 2008 work[120]) and also UK legislation, demonstrating the wide nature of activity than falls within its scope. Moving on to types and typologies the chapter explored Wall's three generations of computer crime, being traditional crimes assisted by computers, traditional crimes for which new opportunities have emerged through computers and finally 'true cybercrimes' which can only be committed by computer.[121] The author also drew out the distinctions in motivation in the three generations as they relate to police computer misuse.[122] In exploring the causes of computer misuse the chapter looked again at Stefan Fafinski's work and his comparison between the number of global internet users and the misuse reports received by CERT[123], showing a proportionate rise in the latter corresponding to a rise in the former. Additionally the three 'perceived features' as defined by David Wall were outlined.[124]

In the methodology the author provided an explanation as to the backdrop for this research as well as why this specific area of study was selected. He outlined his personal qualifications for undertaking the research along with his considerations as to preferred research methods of data capture, as well as subject identification. In closing, he noted the difficulties encountered in conducting the research and how these may be overcome by anyone wishing to repeat the exercise.

---

[118] *P37 ante..*
[119] *P46 ante.*
[120] *P47 ante.*
[121] *P50 ante.*
[122] *P50 ante.*
[123] *P52-53 ante.*
[124] *P54 ante.*

Chapter four firstly provided an overview of both the temporal and political context of the research[125] as it relates to different participants, before moving on to provide the findings themselves. In closing this section the author presented a table demonstrating the impacting factors as identified by the research participants, and their differing views on each one[126].

In chapter five the author discussed the conflicting ideas and responses of research participants. In the first instance these were examined purely against each other and secondly against the backdrop of existing academic theory already outlined. Key within this section is the demonstration of a lack of a firm definition of a *'Genuine Policing Purpose'*, a concept required for a check on a police computer system to be legitimate.[127] In closing the discussion the author revisited each of the impacting factors placing them in a hierarchy of 'impactive weight'[128], demonstrating the order as;

- Awareness of wrongdoing.
- Perception of seriousness and sanction.
- Perception of likelihood of capture.
- Ease.
- Stigma.

In this chapter the author seeks firstly to address the scale of computer misuse to provide some context for the observations to follow. Following this, original contributions are offered to both academic theory and professional practice. In the area of academic theory the author revisits the typologies of Roebuck and Barker

[125] *P72 ante.*
[126] *P118-119 ante.*
[127] *P124 ante.*
[128] *P157 ante.*

(1973), Punch (1985) and Sherman 1974) with a view to examining the impact on these works, of the results of this research. In relation to professional practice, the author seeks to provide a two stage test for determining the concept of a *'Genuine Police Purpose'* as well as making observations as to how the research may better inform counter-corruption activity with a view to controlling the identified impacting factors and thereby influencing officer's propensity to computer misuse.

In concluding the thesis, the author discusses whether this research may be applied more generically to other forms of police corruption or computer misuse generally, as well as addressing the limitations of this research and its potential weaknesses. Finally the author outlines the opportunities for further research in this area and how this may further contribute to both academic knowledge and professional practice.

The Perfect Storm

Throughout the research phase of this work one point in particular was made repeatedly by all four research groups, that of the high scale of computer misuse within the police service. In discussing scale the author is clear that he categorises computer misuse in accordance with the definitions outlined previously within this thesis, those of the UK government in legislation, and by Wasik (1991) and Fafinski (2008). These provide broad parameters but the author is of the view that this is appropriate based at least in part on the repeated confirmation of this by the English law courts[129].

[129] The Computer Misuse Act 1991 has been the subject of repeated appeals and interpretation (discussed ante) all of which has left the legislation intact with its wide definition of computer misuse.

During the research interviews all participants were provided with data from an organisation called 'Big Brother Watch' outlining a number of incidences of computer misuse by each police force.[130] The data itself was not overly significant but it provided a vehicle to discuss the perceived scale of the issue in terms of either the figures being under representative, about right, or over inflated. Of the responses provided it is apparent that the closer to the *'coalface of policing'*[131] interview subjects were placed, the greater and more firm their perception of prevalence

Table 8 –Observations on Prevalence of Computer Misuse by Research Group

Research Group	Coalface Proximity	Observations on prevalence
National Leads	Furthest	*"a serious problem but declining as people better understand and the organisation becomes better at detection"* *"With a quarter of a million people involved in law enforcement, it [the figures presented] strikes me as low"*
Investigating Officers	3rd	*[our in-house research on surnames searches] "shows that misuse has been as high as 25%"* *"I think it is under-reported, more widespread than we know"*
Police Federation	2nd	*"Every instinct tells me there must be more" [than the figures presented].* *"Very under-represented. [the figures] It's a huge issue. If you want to catch someone, you can always get them for that"*
Disciplined Officers	Nearest	*"I don't think any communicator can put their hand on their heart and say they have never looked at [something] they shouldn't have"* *"I would probably pitch it as high as 60%"* *"[The figures] are a huge underestimation. I would say 80-85% [of officers] misuse the system"* *"there must be thousands doing what I was doing"*

From the responses provided by research participants the author draws his first conclusion as a result of this work; *"that the scale of computer misuse by police officers in the UK is endemic"*[132] This conclusion is reached despite the lack of a

[130] Reproduced at Appendix B

[131] The author uses this expression as an analogy to operational policing as opposed to strategic leadership of the organisation.

[132] Endemic *Adjective* -(of a disease or condition) regularly found among particular people or in a certain area- Oxford English Dictionary online http://oxforddictionaries.com/definition/english/endemic?q=endemic accessed 10/11/12.

definition of a *'Genuine Policing Purpose'* and based on the premise that where there is doubt, the benefit of this is given to the officer. In some way mitigating the widespread nature of this type of malpractice, the author is confident that the research demonstrates that the vast majority of incidences relate to matters at the lower end of the seriousness hierarchy as previously outlined.

Given this first conclusion, the author seeks to examine what factors from this research and existing academic theory may have come together to create a 'Perfect Storm' ripening the environment for computer misuse. Of the external factors, significant is the view of Jane Furniss from the IPCC, that she was not at all confident that officers understood the limitations of acceptable police computer use. Moreover, she pointed to the cultural relationship young people now have with computers and their expectation of the right to data. She went on to explain that she did not believe officers even considered whether something was right or wrong, such was their familiarity with computers that they just accepted it as an ability without further consideration.

The observations of Jane Furniss are in keeping with some previous research. Firstly, and in relation to police corruption generically, Stoddard outlined his suggestion that breaking the rules is actually a social norm, but is only seen as deviant practice against the high standards expected in law enforcement. This would provide an explanation for the widespread nature of corruption across the board, but as a number or reviews have dismissed this argument,[133] it is necessary to look in more detail at computer misuse in particular. In doing so, notable is the previously summarised work of Stefan

[133] HMIC, 1999,2006,2012. IPCC 2012

Fafinski which points to the rise in society's internet usage as contributing to the rise of computer misuse. (Fafinski, 2008) This point is made even more clearly by David Wall in his assessment of the impact of the rise of internet usage *"... [the internet] made the information generation feel different ... it made them feel free to explore, to roam freely ..." (Wall, 2008. Pp 876).* It would therefore appear that whilst Stoddard's view of corruption as a social norm cannot be relied upon, the ideas relating specifically to computer misuse do provide a more convincing argument.

If this prevailing social construction can be seen as the first gusts of the 'Perfect Storm', other factors more specific to the police and computer misuse are now required to reinforce these. The first of these can be found in existing academic work, in particular that of Lawrence Sherman, Maurice Punch and David Wall.

Sherman in his 'variable features' (Sherman, 1974) highlights a number of issues, of these two in particular overlap the findings of this research and so take on added significance. Sherman's 'legal opportunities' relates to what he calls the 'invitational edge' (Sherman, 1974) of corruption, which is posed by the existence of something of interest albeit the method of obtaining it is prohibited. This neatly sums up the concept of police information as for many research participants, particularly disciplined officers, the information sought was either to assist in personal life events (such as divorce proceedings), to protect friends and family or boredom and nosiness.

This invitational edge is all the more inviting when one considers another of Sherman's variable features, that of 'corruption controls'. The organisational view here was that although corruption controls and computer audits were rare, officers on the street believed them to be frequent and powerful, a misperception that served to dissuade

them from malpractice. The findings of this research however, demonstrate that officers labour under no such misapprehension and for them therefore corruption controls are very limited. This is perhaps unsurprising given the reinforcing views of David Wall's 'perceived features'. *(Wall, 2008)* These suggest that far from being concerned about corruption controls, generally society holds a (false) perception as to the ease of computer misuse in the sense of its anonymity, the fact that perpetrators go unpunished and that victims are overly vulnerable. The idea of a lack of corruption controls or effective organisational work to tackle the issue is further reinforced by Maurice Punch's extension of the 'rotten apple' analogy; *"Whose duty was it to inspect the fruit and who neglected to apply the insecticide?" (Punch, 2009. p9)*

If these ideas now provide the impetus to create the gales, one more element is needed to complete the 'Perfect Storm', those impacting factors identified within this research. As has previously been discussed the most significant impacting factor identified by research subjects was that of awareness or wrongdoing, linked closely to the absence of a firm definition of a 'Genuine Policing Purpose' for searches on police computer systems. Whilst this may seem an easy and convenient (if not convincing defence), the author holds some sympathy for the position when the boundary lines between one's personal and professional life are often blurred. Examples include an officer living in a small village but working in a different area, regularly checking the crime systems to identify crimes of interest near his home, to enable him to warn neighbours of a spate of car thefts, or burglaries exploiting insecure rear patio doors etc. The officer would doubtless argue that he is always a police officer and his actions provide a better service to the public than they would otherwise receive.

At first sight this may seem acceptable to some. Others would point out the potential for the officer to gain personal information about his neighbours as collateral to his main objective and argue that this would be unacceptable. Even if this information were never shared the officer may have knowledge of personal information relating to friends or neighbours which he was not authorised to obtain; and gaining this type of information could reasonably have been foreseen as a consequence of his searches. From an organisational perspective the searches would be unauthorised. The position is made perhaps clearer if the officer worked for a different force and had to visit another police station and ask someone to carry out the checks for him and provide him with the information. In such circumstances the officer is unlikely to be successful. Where the position may become even more blurred is where the officer's geographic work area encompasses his home village. In this example it is the activity that is all important and it is that which falls one side or the other of the *'Genuine Policing Purpose'* debate.

An alternative method of classification would be by way of motivation. Whilst this is less tangible and requires greater effort in proving, it enables officers to act in good faith (albeit on occasion mistakenly) to serve communities, whilst maintaining organisational protection from those who seek to abuse police computer systems for their own benefit. In this way the idea of a *'Genuine Policing Purpose'* or lack of one, can be aligned to Wall's work on the three generations of cybercrime, where motivation is all important. Breaches at the higher end of the seriousness hierarchy where the objectives are to commit traditional crimes assisted by computers would fall within the 1st generation. Those breaches for which new opportunities have

emerged such as the protection of family and friends or assisting in personal life events would fall within the 2nd generation and those breaches which can only take place within 'cyberspace'[134] such as browsing through information systems out of boredom or nosiness would fall within the 3rd generation. *(Adapted from Wall, 2007).*

Whilst knowledge of wrongdoing featured prominently, there are those abuses which are immediately recognisable as unauthorised but are carried out against the backdrop of a perception of minor sanctions if caught. This is significant because whilst there may be an expectation upon officers to understand both the criminal law and the police conduct regulations, this is often lacking, with disciplined officers stating that had they known of the seriousness of the consequences they would not have undertaken the action. Linked to this area is the perceived risk of being caught misusing computer systems, which in this research was universally accepted to be very low if one were not being investigated for some other internal matter.

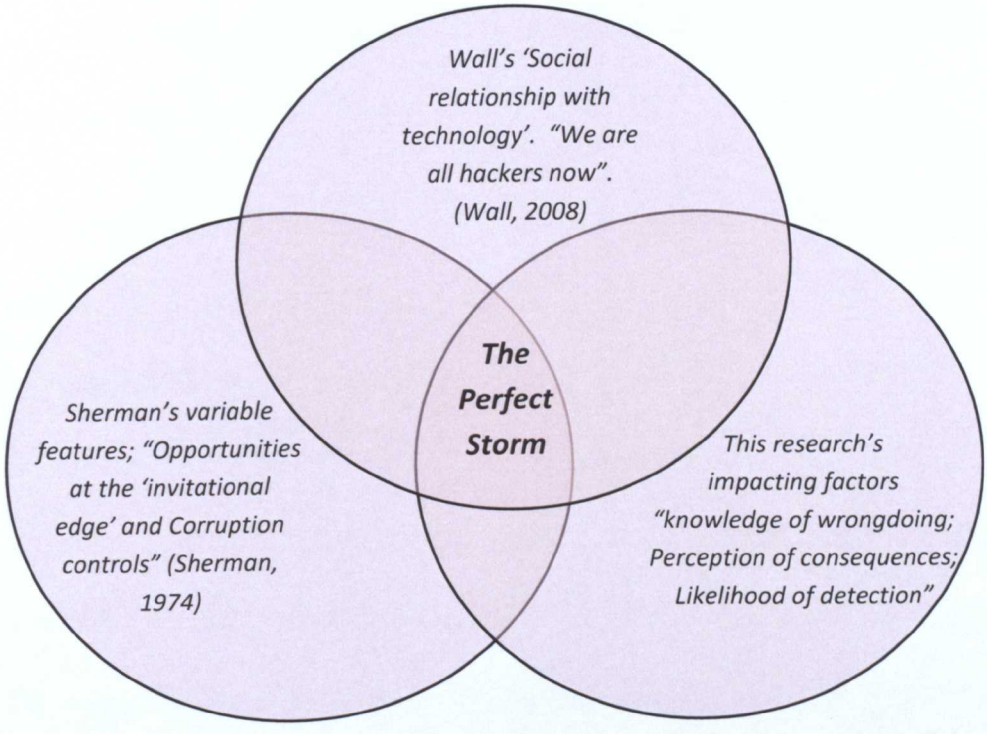
With the advent of new technology to allow greater computer monitoring by force's Professional Standards Departments[135] the likelihood is that more officers will be identified breaching the regulations as there currently endures a complacency around existing audit methods. Significantly other than the one disciplined officer at the higher end of the seriousness hierarchy all others were of the view that a greater likelihood of being caught would reduce the number of officers misusing the systems.

The three identified areas therefore; Wall's social relationship with computer technology, Sherman's variable features and the impacting factors from this research

[134] As used by Wall 2007.
[135] This comes from a recommendation of the 2011 HMIC Report 'Without Fear or Favour', which advised all forces to explore technological solutions to carry out speculative audits to identify computer misuse.

can be seen to come together to create the perfect storm of endemic computer misuse within the police service.

Figure 3. The Perfect Storm



Contemporary Challenges Versus Traditional Theory

In chapter two the author examined a number of typologies relating to police corruption as well as computer misuse. By their nature, those relating to computer misuse tend to have been developed over the last 10 years and appear to remain relevant to this research. Of those relating to police corruption however, two have emerged as holding repeated significance albeit requiring minor amendments to

remain relevant to computer misuse. This is perhaps unsurprising as the march of technology has created new ways to commit old offences or disciplinary breaches, as well as new breaches and offences themselves.

The typology of corrupt practice produced by Roebuck and Barker in their 1973 work outlined eight activities ranging from the receipt of free drinks to the undermining of criminal investigations. [136]

Whilst it is possible to demonstrate that some motivations for computer misuse fall within these existing categories, most notably those at the higher end of the seriousness hierarchy, there exists no easy fit for 2nd or 3rd generation offences such as protection of friends and family or nosiness searching. In 1985 Maurice Punch identified that as a result of the rise in drugs enforcement, new opportunities had arisen for the corrupt officer which were not catered for within the original typology. He subsequently added a ninth category of *'Flacking and Padding' (Punch, 1985)* to the existing typology to account for the adding to evidence to 'set someone up' to ensure a conviction. Through a similar process this work has identified a comparable gap in the original typology prompted by the exponential rise in computer usage within the police service, that of computer misuse.

This gap can be remedied by the addition of a tenth category to the existing nine. It therefore leads to the thesis' second conclusion; *"that the 1974 typology of Roebuck and Barker (as amended by Punch, 1985), requires the addition of a tenth category, that of 'Browsing' representing the unauthorised viewing and searching of police information systems"*.

---

[136] *P30 ante.*

Table 9- Amended typology of police corruption by Roebuck and Barker

Corruption of Authority	*The receipt of free drinks / meals without necessarily violating the law.*	Original Research Roebuck and Barker 1973
Kickbacks	*Gain for referring business to particular firms, such as the use of preferred boarding up companies, garages for vehicle removal etc.*	
Opportunistic theft	*Stealing from detained persons, dead bodies, scenes of crime.*	
Shakedowns	*Gain for not correctly applying the law, such as failing to arrest, issue a ticket.*	
Protection of illegal activities	*Enabling illegal enterprises to continue such a gambling dens by the provision of tactical / intelligence information. This also can apply to legitimate businesses that occasionally break the law.*	
The fix	*Undermining criminal investigations or the losing of evidence.*	
Direct criminal activities	*The commission of substantive crimes.*	
Internal pay-offs	*The paying of supervisors by officers for favourable adjustments to duties. The opportunity to earn overtime, promotion or easy assignments.*	
Flacking and Padding	*Planting or adding to evidence 'to set someone up' to ensure a conviction.*	Amendment Punch, 1985
Browsing	*The unauthorised searching and reviewing of police computer systems.*	Amendment This research

Whilst the typology of Roebuck and Barker provides a useful reference as to the types of deviant practice, it does not in itself provide any explanation as to its causes. For this it is necessary to look at the second recurring academic work in this thesis, that of Sherman's variable features.

Whilst only two of these hold particular relevance to this work, those of 'legal opportunities' and 'corruption controls', it can be seen that the primary impacting

factor identified in this research is lacking from Sherman's list; that of knowledge of wrongdoing. As with the previously discussed typology this can be ascribed to changing times with new transgression possibilities and the lines separating professional and private lives often being blurred in an environment where as David Wall puts it *"The internet's global reach, combined with easy access, made the information generation feel different..." (Wall 2008. Pp876),* and where information is available instantly in every other aspect of an individual's life.

To overcome this mismatch between Sherman's variable features and this research's impacting factors the author draws his third conclusion; *"that Sherman's list of variable features should be amended to add a seventh feature, that of knowledge of wrongdoing."*

Table 10- Amended typology of Sherman's variable features.

Sherman's Variable Features	
Community Structure	Original Research Sherman 1974
Organisational Characteristics	
Legal Opportunities	
Corruption Controls	
Social organisation of corruption	
Moral cynicism	
Knowledge of wrongdoing	Amendment - This research

(Adapted from Sherman 1974)

By making additions to the two existing academic theories the author hopes that these retain relevance to the modern phenomena of computer misuse within the police service, and may be used as a platform to examine the practical application of this work to the counter corruption effort.

Contemporary Challenges Versus Traditional Practice

During this research the author has identified his 'impacting factors' in relation to computer misuse which, when taken with existing theory create the 'Perfect Storm'. The three principal factors identified, those of awareness of wrongdoing, perception of consequences and likelihood of detection, as well as adding to existing theory, may also be applied to professional practice in order to prevent further offending. As has been previously demonstrated, first among these factors is the awareness of wrongdoing, fuelled by the lack of a definition of a *'Genuine Policing Purpose'*. The author is of the view that clarity in this area is essential as, even if it is argued that officers already fully understand that their actions are wrong, the removal of any doubt as to definition removes a potential pseudo-defence and in itself is likely to reduce breaches.

Having considered the responses of research subjects and in particular those of the Police Federation and disciplined officers, against the backdrop of academic work, such as Wall 2007 and Fafinksi 2008, the author arrives at his fourth conclusion; whether or not computer usage is for a *'Genuine Policing Purpose'* is not a matter of action but a matter of motivation. With this assertion it is possible to outline a two stage test to determine whether any activity breaches the disciplinary code; firstly, to consider whether the primary motivation for the computer usage is to prevent or detect crime and secondly, whether the likelihood of obtaining information of personal interest to the officer by way of collateral can be reasonably foreseen.

The test may be demonstrated on a four by four axis creating rebuttable and irrebuttable presumptions[137] depending on the responses to the two questions;

Figure 4. Two fold test for 'Genuine Policing purpose'

Primary test. *Is the primary motivation for this computer use the 'prevention or detection of crime' or 'apprehension of offenders' ?*		***Yes***	***No***
	Yes	***A rebuttable presumption that the computer usage is for a 'Genuine Policing Purpose' and therefore authorised***	***An irrebuttable presumption that the computer usage is for a 'Genuine Policing Purpose' and therefore authorised***
	No	***An irrebuttable presumption that the computer usage is not for a 'Genuine Policing Purpose' and therefore not authorised***	***A rebuttable presumption that the computer usage is not for a 'Genuine Policing Purpose and therefore not authorised***

Secondary test

As a result of this computer usage can the collateral intrusion of data be reasonably foreseen to include information of personal interest to the officer ?

The terminology used within the model is significant as the terms, rebuttable presumption, irrebuttable presumption and collateral intrusion are terms used in other areas of policing and are generally well understood. The model creates four possible responses as a result of the two tests; firstly an irrebuttable presumption that the proposed computer usage is for a *'Genuine Policing Purpose'* and therefore authorised where it relates to the prevention and detection of crime and there is no reasonably foreseeable collateral intrusion into matters of personal interest to the

[137] The concept of rebuttable and irrebuttable presumptions are familiar terms within policing. The former denotes that that the presumption is made until proven otherwise, the later creates a definitive position which must be taken to be true no matter what evidence exists to the contrary.

officer. In practice this will doubtless be the vast majority of an officer's everyday police work and computer usage. Secondly, where the primary purpose of a computer search is not to prevent or detect crime and holds a reasonable likelihood of collateral intrusion into matters of personal interest to the officer, the model creates an irrebuttable presumption that the computer usage is not for a *'Genuine Policing Purpose'* and is therefore unauthorised. Finally the model creates two rebuttable presumptions, one for and one against computer usage being authorised. In these cases officers should take care to guard against the suggestion that their computer usage is unauthorised by consulting with supervisors where appropriate.

Whilst the model provides a clear decision making process, the author is conscious of two principal drawbacks: Firstly the model relates to motivation and, whilst this is clearer than any existing model at this time, it can be difficult to demonstrate. This is overcome slightly by the creating of rebuttable and irrebuttable presumptions which relieve either the officer or the organisation of any burden of proof in clear cut cases whilst clearly outlining upon whom the burden rests in cases of rebuttable presumptions. Likewise the matter of motivation is a question of fact to be determined rather than an interpretation of concept such as *'Genuine Policing Purpose'*, which importantly does not have a definition.

Secondly the model can only be of any practical application if it is recognised and considered. For this to be the case the observations of David Wall (2008), supported by Jane Furniss of the IPCC in this work, that officers do not even consider their computer usage against a backdrop of authority, moreover they accept it as a right, need to be overcome so that officers do make conscious decisions in this area. For

this to happen awareness raising would be required, with officers and investigators both conscious of the model and using it to determine whether at first glance, a prima facie misconduct case exists.

Moving on from the idea of a *'Genuine Police Purpose'* to the other two main impacting factors, the author is of the view that both the awareness of sanctions and the likelihood of detection are areas that can be influenced relatively easily by campaigns within forces. As has already been discussed the Police Federation already accept in part a shared responsibility for the reduction in police corruption in two ways, firstly as police officers for the protection of the public generally, but more specifically as a representative body for their members, to reduce the likelihood of their members being vulnerable to internal investigations. The author however holds a view in keeping with that of Maurice Punch in that the organisation holds the most significant responsibility for corruption prevention. As such he is of the belief that forces have a greater role to play in both publicising the seriousness of computer misuse and actively demonstrating new technology enabling robust audits of computer systems.

Further application and limitations

Having considered a number of impacting factors as they relate to computer misuse, the question inevitably presents itself as to whether these factors may be applied to other areas of police mal-practice, to computer misuse outside the police service, or in the widest terms to other forms of deviant behaviour outside the police. The full list of impacting factors, (awareness, sanctions, likelihood of detection, ease and stigma) have in this research been considered against the very tight parameters set out in

chapter three in relation to computer misuse. Whilst the first three interview groups were selected for their role in either investigating offences or representing officers, the final group, that of disciplined officers were selected for the particular fact that they had been disciplined for computer misuse. As the views of these officers were generally seen as the nearest to the coalface of both policing and offending, and their responses allocated the corresponding weight, it is unlikely that a direct comparison to other forms of police corruption can be made.

In relation to further application outside the police service the author notes the special nature of policing which provides not only access to significant amounts of sensitive data at junior levels but also the implicit trust placed within holders of the office of Constable, as well as the blurring of the demarcation between personal and private lives. These characteristics result in the findings being applicable to a limited number of circles, however other agencies do exists with similar features, such as Her Majesty's Revenue and Customs (HMRC) and Local Authority fraud investigation units. Before directly applying the findings however each agency should be assessed against the characteristics of the research groups used in this study to ensure effective comparison.

In advancing the four primary conclusions the author is conscious of the limitations of this research and potential weaknesses which may have inadvertently created some distortion. Chief among these are the numbers of research participants particularly in the group of disciplined officers. Whilst the Police Federation were able to identify a significant number of officers who had been found guilty of computer misuse, gaining the trust and approval from these officers was often difficult and the number who

either did not reply or declined to take part far outweigh those who agreed to engage. This point is amplified when considering the motivations of those officers who did take part and where their offending would fall within the seriousness hierarchy.

The author is conscious that of the participants, only one can be categorised as using her position to disrupt the criminal justice process and this of course presents the possibility that if further such subjects were identified and interviewed a different pattern of impacting factors may become apparent at the higher end of the identified hierarchy. In mitigation of this point the author notes that the overwhelming evidence from all four research groups was that conduct at the higher end of the seriousness hierarchy is very rare, a position reinforced by a number of external reviews of policing.[138] This being the case the author is of the view that whilst being essential to providing a holistic view of police corruption, proportionately the 1 officer, making up 14% of the total research group, over represents the sub category of higher end offenders.

Additionally the author highlights the political context in which this research was undertaken during a period of high political and media interest in police corruption. It is possible that in times of lesser interest responses may differ particularly in the national leads group where individual's attention has been forcibly directed in the last two years.

Further Research

In concluding this research the author hopes that it may inspire others to examine in greater detail the issue of computer misuse within the police service. Whilst the data

[138] HMIC, 2006, 2011. IPCC 2011

collection for this work has been across a number of research groups, spanning a number of profiles, further work examining particular profiles such as gender, detectives, length of service and age may provide different and interesting results. Likewise, research focused at a particular area of the seriousness hierarchy could provide an insight into the impacting factors for specific groups rather than generically as presented in this work.

The author highlights at this point that any future research is unlikely to be possible without the assistance of both national leads and more significantly, the Police Federation. Whilst national leads provide a unique view of organisational perspectives, the Police Federation may justly be categorised as guardians of the chief source of data in this field, that of officers who have been disciplined. Even if one were able to overcome the issue of identifying such officers without the assistance of the Police Federation (which is unlikely given the non-public nature of such information), those officers would doubtless make contact with their Federation representative and discuss any interview request.

In Closing

In closing this work the author hopes that as well as contributing to existing academic theory in the area of police corruption, he has made a practical contribution to the counter-corruption effort in policing particularly as it relates to computer misuse. He hopes that his two fold 'presumption' test can be used to both protect the organisation and individuals by creating greater clarity and understanding in the area

of *'Genuine Policing Purpose'* and result in less abuses of police information systems be they inadvertent or deliberate.

References

ACPO. (n.d.). *About* . Retrieved September 20th, 2012, from ACPO: http://www.acpo.police.uk/About/AboutACPO.aspx

ACPO. (n.d.). *Media Center.* Retrieved September 20, 2012, from ACPO: http://www.acpo.presscentre.com/Press-Releases/ACPO-comment-on-HMIC-police-integrity-report-Without-Fear-of-Favour-133.aspx

Barker, T., & Roebuck, J. (1973). *Emprical Typology of Police Corruption - A study of Organizational Deviance.* Springfield, IL. USA: Charles Thomas.

Booth, W. C., Colomb, G. G., & Williams, J. M. (2008). *The Craft of Research (3rd Ed).* Chicago. USA: Chicago Press.

Brown, J. (1996). Policing Research: Some Critical Issues. In F. Leishman, B. Loveday, & S. Savage, *Core Issues in Policing* . Harlow: Longman.

Bryman, A. (2008). *Social Research Methods.* Oxford. UK: Oxford University Press.

Caldero, M. A., & Crank, J. P. (2011). *Police Ethics. The Corruption of Noble Cause.* Burlington. USA: Anderson.

Cohen, S. (1972). *Folk Devils and Moral Panics.* New York, USA.: Routledge.

Cox, B., Shirley, J., & Short, M. (1977). *The fall of Scotland Yard.* London. UK: Penguin Books.

Crown Prosecution Service of England and Wales. (2012). *The Code for Crown Prosecutors.* Bolton. UK: Blackburns.

Elliston, F. A., & Feldberg, M. (1985). *Moral Issues in Police Work.* Totowa. USA: Rowan and Allanhead.

European Council. (2001). *European Convention on Cybercrime.* Budapest: European Council .

Fafinski, S. F. (2008). *Computer Use and Misuse : The Constellation of Control.* Leeds; UK: University of Leeds: School of Law.

Gercke, M. (2011). *Understanding Cybercrime : A guide for developing countries.* Geneva, Switzerland: International Telecommunications Union.

Goffman, E. (1963 : 1986). *Stigma. Notes on the Managment of Spoiled Identity.* New York. USA: Simon and Schuster.

Goldstein, H. (1975). *Police Corruption: A perspective on its nature and control.* Washington. USA: Police Foundation.

Guardian News and Media Ltd. (2011, July 17th). Retrieved September 14th, 2011, from The Guardian: http://www.guardian.co.uk/uk/2011/jul/17/sir-paul-stephenson-resignation-statement

Hamilton, D. (2011 (Research 2007-2010)). *Police Databases: Over 900 staff abuse their access.* London. UK: Big Brother Watch.

Her Majesty's Inspectorate of Constabulary. (1999). *Police Integrity; Securing and Maintaining Public Confidence.* London: Swindon Press.

Her Majesty's Inspectorate of Constabulary. (2006). *Rasing the Standard.* London. UK: HMSO.

Her Majesty's Inspectorate of Constabulary. (2011). *Without Fear or Favour.* London: UK: HMSO.

Herath, H., & Wijayanayake, W. (2009). Computer misuse in the workplace. *Journal of Business Continuity & Emergency Planning* , 259-270.

Hobbes, T. (1996 (Hobbes 1588-1679)). *Leviathan.* (Ed. J.C.A Gaskin) Oxford. UK: Oxford University Press.

Hobbs, R. (1988). *Doing the Business.* Oxford: Oxford University Press.

Im, J., & Van Epps, P. (1992). Software Piracy and Software Security Measures in Business Schools. *Information and Managment*, 193-203.

IPCC. (2011). *Corruption in the Police Service of England and Wales Part 1.* London. UK: Independant Police Complaints Commission.

IPCC. (2012). *Corrpution in the Police Service of England and Wales (part 2).* London. UK: IPCC.

Kerr, O. (2003). Cybercrime's Scope: Interpreting 'Access' and 'Authorization'. *NYU Law Review,Vol. 78, No. 5*, 1596-1668.

Kesar, S., & Rogerson, S. (1998). Developing Ethical Practices to Minimize Computer Misuse. *Social Science Computer Review*, 240-251.

King, R. D., & Wincup, E. (2008). *Doing Research on Crime and Justice (2nd Edition).* Oxford, UK: Oxford University Press.

Kleinig, J. (1996). *The ethics of policing.* Cambridge. UK: Cambridge University press.

Klockars, C. B. (1977a). Invitational Edges. In P. K. Manning, & L. J. Redlinger, *Thinking About Police* (p. 334). New York. USA: McGraw Hill.

Klockars, C. B. (1977b). Invitational Edges. In T. Newburn, *Understanding and preventing police corruption: lessons from the literature, 1999* (pp. 5-6). London.UK: Home Office Research, Development and Statistics Directorate.

Knapp, W. (1973). *The Knapp Commission report on Police Corruption.* New York. USA: Brazillier.

Leveson LJ. (20012). *An Inquiry into the Culture, Practices and Ethics of the Press.* London. UK: The Stationary Office.

Levi, M., & Nelken, D. (1996). *The Corruption of Politics and the Politics of Corruption.* Oxford. UK: Blackwell.

Loader, I., & Mulcahy, A. (2001). The Power of Legitimate Naming. Making sense of the Elite Police Voice . *British Journal of Criminology*, 252-265.

Mangione, T. W. (1995). *Mail Surveys: Improving the Quality.* Thousand Oaks, California: Sage.

Manning, P. K., & Redlinger, L. J. (1977). *Thinking About Police.* New York. USA: McGraw Hill.

McLagan, G. (2003). *Bent Coppers.* London. UK : Orion Publishing Group.

McMullan, M. (1961). A Theory of Corruption based on a cosnderation of corruption in the Public Services and Governments of British Colonies and ex-Colonies in West Africa. *Sociological Review : July 1961 Vol 9, Issue 2*, 181-201.

Mollen Commission. (1994). *Report of the commission to investigate allegatons of police corruption and anti-corruption procedures of the police department of New York.* New York, USA: Mollen Commission.

Morton, J. (1993). *Bent Coppers.* London, Uk: Warner Books.

Murji, K. (2011). Working Together: Governing and Advising the Police. *The Police Journal (Vol 84)*, pp. 256 - 271.

National Police Improvement Agency. (2011). *Police Officer Recruitment: Eligibility criteria for the role of Police Constable.* London, UK: NPIA.

Newburn, T. (1999). *Understanding and preventing police corruption: lessons from the literature.* London, UK: Home Office Research, Development and Statistics Directorate.

Nolan LJ, M. P. (1995). *Standards in Public Life.* London. UK: HMSO.

Pattavina, A. (2005). *Information Technology and the Criminal Justice System.* California, USA: Sage.

Punch, M. (1985). *Conduct Unbecoming: The social construction of police deviance and control.* London. UK: Tavistock.

Punch, M. (1994). Rotten Barrels : Systemic origins of corruption. In E. W. Kolthoff, *Startegieen voor corruptie-beheering bij de politie* (p. 27). Arnhem , Netherlands: Goouda Quint.

Punch, M. (2009). *Police Corruption. Deviance, accountability and reform in policing.* Oxford, UK: Routledge.

Rawlings, P. (2002). *Policing; A short History.* Collumpton. UK: Willan.

Reiner, R. (2010). *The Politics of the Police (4th Ed.).* London, UK: Oxford University Press.

Reiner, Robert. (2000). *The Politics of the Police (3rd Ed.)* (3rd ed.). London, UK: Oxford University Press.

Sacco, V., & Zureik, E. (1990). Correlates of Computer Misuse: Data from a self-reporting sample. *Behaviour and Information Technology*, 353-369.

Salehnia, A. (2002). *Ethical Issues of Information Systems.* London. UK: IRM Press.

Sherman, L. (1974). *Police Corruption: A Socialogical Perpsective.* New York. USA: Doubleday.

Sherman, L. (1978). *Scandal and Reform: Controlling police corruption.* Berkley, USA: University of Californai Press.

Sherman, L. (1985). Becoming Bent: Moral careers of corrupt policemen. In F. A. Elliston, & M. Feldberg, *Moral Issues in Police Work.* Totowa. USA: Rowan and Allanhead.

Skolnick, J. (1966). *Justice Without Trial.* New York, USA: John Wiley and Sons.

Stoddard, E. R. (1968). The informal code of police deviancy: A group approach. *The Journal of Criminal Law, Criminology and Police Science. Vol 59. No 2*, 201-213.

Sudman, S., & Bradburn, M. N. (1982). *Asking Questions: A Practical Guide to Questionnaire Design.* San Francisco: Josey-Bass.

Sussman, V. (1995). Polcing Cyberspace. *Us News and World Report*, 54-61.

Sutherland, E. H. (1968). White Collar Criminality. *American Scoial Review, 1-12 (1940) in The informal Code of Police Deviancy: A group Approach, The journal of Criminal Law, Criminology and Polie Science. Vol 59 No 2*, 201.

Swinyard, W., Rinne, H., & Kau, A. (1990). The Morality of Software Piracy. *Journal of Business Ethics*, 655-664.

Sykes, G., & Matza, D. (1957). Techniques in Neutralisation: A Theory of Deliquency. *American Socialogical Review*, 664-670.

The Wood Commission. (1997). *Final report of the royal commission into the New Soyuth Wales Poicee Service: Volume 1 Corruption.* Sydney. Aus.: Royal Commission.

Wall, D. S. (2007). Policing Cybercrimes: Situating the public police in networks of security within Cyberspace (Revised Feb.2011). *Police Practice and Research:An International Journal. 8 (2)*, 183-205.

Wall, D. S. (2008/2011). Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knwoeldge about cybercrime (Revised Feb.2011). *Information, Communication and Society (11)*, 861-884.

Wasik, M. (1991). *Crime and the Computer.* Oxford: Clarendon Press.

Wasik, M. (2008). Computer Misusue and Misconduct in Public Office. *International Review of Law, Computers and Technology 22*, 135-140.

Weber, M. (1919). Politics as a Vocation. *Free Students Union - Munich University.* Munich - Germany.

Wilson , J. Q. (1963). Police and their problems - A theory. *Journal of Public Policy*, 1-19.

Appendix Ai

Appendices

Interview Question to National Leads
(Representing the Organisational Perspective)

The questions should be answered on the basis of organisational knowledge and experience.

In relation to the improper access of police information;

Can you tell me the organisation's belief on the principal motivations for misuse?
(Consider money, third party loyalty, protection of family friends, nosiness, blackmail.).

A Freedom of Information request in 2011 shows that some 904 members of police staff / officer were subjected to internal discipline for data misuse, between 2007 and 2010. An additional 98 individuals had their employment with a police force terminated. Do you believe this number is roughly the scale of the problem? If not how would you estimate the scale?
(Is everyone doing this to a greater or lesser extent?)

What do you believe is the greatest inhibitor to data misuse?
(Consider personal integrity, difficulty of access, fear of being caught, fear of consequences)

Is everyone aware of what is acceptable and what is not? Is it different for different motivations mentioned?

How clearly do you believe the organisation has raised the profile of the potential consequences of the risk of data misuse?
(Do people know what is acceptable and what is not?)

How easy or difficult do you believe it is to misuse police systems?

Do you think making it harder (within the limits of maintaining access legitimate access) would discourage misuse for any of the motivations you have mentioned?

What is the risk of being caught?
Do you think making being caught more likely would discourage misuse for any of the motivations you have mentioned?
Is the risk of being caught appropriately perceived by officers?

What are the consequences for information access?
(Presumably they are different depending on motivation?)
Do you think having tougher sanctions would discourage misuse for any of the motivations you have mentioned?
Are the consequences appropriately understood by officers?

Is there any stigma attached to computer misuse?

How serious is information misuse compared to other type of police deviance?
(Does the organisation take it seriously?)

Interview Question Head of Anti-Corruption Units
(Representing investigative perspective)

The questions should be answered on the basis of personal knowledge and experience.

In relation to the improper access of police information;

Can you tell me your belief on the principal motivations for misuse?
(Consider money, third party loyalty, protection of family friends, nosiness, blackmail.).

A Freedom of Information request in 2011 shows that some 904 members of police staff / officers were subjected to internal discipline for data misuse, between 2007 and 2010. An additional 98 individuals had their employment with a police force terminated. Do you believe this number is roughly the scale of the problem? If not how would you estimate the scale?
(Is everyone doing this to a greater or lesser extent?)

What do you believe is the greatest inhibitor to data misuse?
(Consider personal integrity, difficulty of access, fear of being caught, fear of consequences)

Is everyone aware of what is acceptable and what is not? Is it different for different motivations mentioned?

How clearly do you believe the organisation has raised the profile of the potential consequences of the risk of data misuse?
(Do people know what is acceptable and what is not?)

How easy or difficult do you believe it is to misuse police systems?

Do you think making it harder (within the limits of maintaining access legitimate access) would discourage misuse for any of the motivations you have mentioned?

What is the risk of being caught?
Do you think making being caught more likely would discourage misuse for any of the motivations you have mentioned?
Is the risk of being caught appropriately perceived by officers?

What are the consequences for information access?
(Presumably they are different depending on motivation?)
Do you think having tougher sanctions would discourage misuse for any of the motivations you have mentioned?
Are the consequences appropriately understood by officers?

Is there any stigma attached to computer misuse?

How serious is information misuse compared to other type of police deviance?
(Does the organisation take it seriously?)

Appendix Aiii

Interview Question Discipline Liaison Officers
(Representing the Staff Association's perspective)

The questions should be answered on the basis of personal knowledge and experience.

In relation to the improper access of police information;

How many of such cases have you personally dealt with ?

Can you tell me what in your experience are the principal motivations for misuse?
(Consider money, third party loyalty, protection of family friends, nosiness, blackmail.).

A Freedom of Information request in 2011 shows that some 904 members of police staff / officer were subjected to internal discipline for data misuse, between 2007 and 2010. An additional 98 individuals had their employment with a police force terminated. Do you believe this number is roughly the scale of the problem? If not how would you estimate the scale?
(Is everyone doing this to a greater or lesser extent?)

What do you believe is the greatest inhibitor to data misuse?
(Consider personal integrity, difficulty of access, fear of being caught, fear of consequences)

Do you believe everyone is aware of what is acceptable and what is not? Is it different for different motivations mentioned?

How clearly do you believe the organisation has raised the profile of the potential consequences of the risk of data misuse?
(Do people know what is acceptable and what is not?)

How easy or difficult do you believe it is to misuse police systems?

Do you think making it harder (within the limits of maintaining access legitimate access) would discourage misuse for any of the motivations you have mentioned?

What is the risk of being caught?
Do you think making being caught more likely would discourage misuse for any of the motivations you have mentioned?
Is the risk of being caught appropriately perceived by officers / staff?

What are the consequences for information access?
(Presumably they are different depending on motivation?)
Do you think having tougher sanctions would discourage misuse for any of the motivations you have mentioned?
Are the consequences appropriately understood by officers / staff?

Is there any stigma attached to computer misuse?

In your view how serious is information misuse compared to other type of police deviance?
(Does the staff association take it seriously?)

Interview Question Officers who have misuses IT Systems
(Officer's perspective)

Appendix Aiv

Can you please outline the nature of the system use which was deemed inappropriate?

What was your primary motivation for doing this
(Consider money, third party loyalty, protection of family friends, nosiness, blackmail.).

Were there any other motivations?

A Freedom of Information request in 2011 shows that some 904 members of police staff / officer were subjected to internal discipline for data misuse, between 2007 and 2010. An additional 98 individuals had their employment with a police force terminated. Do you believe this number is roughly the scale of the problem? If not how would you estimate the scale?
(Is everyone doing this to a greater or lesser extent?)

Did you know at the time that what you were doing was not allowed?
If you had known that it was wrong would you still have accessed the data?

How easy was access to the system for you?
If it were harder to do would you still have tried to access the data?

What did you think at the time was the risk of being caught?
If you thought it were more likely than not that you would be caught would you still have accessed the data?

What did you think at the time were the potential consequences?
If you had thought the consequences were more serious would you have still accessed the data?

Do you believe everyone is aware of what is acceptable and what is not? Is it different for different motivations mentioned?

How clearly do you believe the organisation has raised the profile of the potential consequences of the risk of data misuse?
(Do people know what is acceptable and what is not?)

Is the risk of being caught appropriately perceived by officers?

What are the consequences for information access?

Are the consequences appropriately understood by officers?

Is there any stigma attached to computer misuse?

In your view how serious is information misuse compared to other type of police deviance?
(Does the staff association take it seriously?)

Appendix B

Police databases:

Over 900 Police staff abuse their access[1]

To arrange broadcast interviews or discuss the research, please contact:
Daniel Hamilton, Director, Big Brother Watch

Mob (24 hrs): 07810 785 924 | Tel: 020 7340 6030

For the first time, Big Brother Watch has uncovered the true extent to which Police abuse their access to confidential databases.

- Between 2007 and 2010:
  - **243** Police officers and staff received **criminal convictions** for breaching the Data Protection Act (DPA).
  - **98** Police officers and staff had their **employment terminated** for breaching the DPA.
  - **904** Police officers and staff were subjected to **internal disciplinary procedures** for breaching the DPA.
- In Merseyside alone, 208 officers and Police staff received criminal convictions for breaching the DPA since 2007.
- The areas with the largest number of officers and Police staff who had their employment terminated for DPA breaches since 2007 were: Kent (10), Merseyside (7), West Midlands (7), Northumbria (6), Derbyshire (5) and Humberside (5).
- The areas with the largest number of officers and Police staff subjected to internal disciplinary procedures for DPA breaches since 2007 were: Merseyside (208), West Midlands (83), Humberside (62), South Yorkshire (42), and Northumbria (39).

A full breakdown of results by local police authority can be found from pages 4 and 5 of this document.

Commenting on the research findings Daniel Hamilton, Director of Big Brother Watch said:

"The allegations surrounding Andy Coulson are just the tip of the iceberg.

"It's astonishing to think that 904 Police officers and support staff across England have faced disciplinary action for abusing their access to confidential systems. 243 have received criminal convictions for their actions, while 98 have lost their jobs.

"Our investigation shows that not only have Police employees been found to have run background records checks on friends and possible partners, but some have been convicted for passing sensitive information to criminal gangs and drug dealers. This is at best hugely intrusive and, at worse, downright dangerous.

"Police forces must adopt a zero tolerance approach to this kind of behaviour. Those found guilty of abusing their position should be sacked on the spot."

[1] This report is by Daniel Hamilton, who received assistance with the research from Frank Manning. Previous Big Brother Watch reports can be found at http://www.bigbrotherwatch.org.uk.

55 Tufton Street, London SW1P 3QL
www.bigbrotherwatch.org.uk ▪ 020 7340 6030 (office hours) ▪ 07810 785 924 (24 hours)

Appendix B

Notable cases

- **In Merseyside, a combined total of 208 Police officers and staff received legal cautions for "viewing a computer record relating to a high profile arrest".**
- **In Dorset, a member of police staff resigned after disclosing information about the supply of class A drugs to a third party. They later received a Police caution for violating the DPA and were referred to the Crown Prosecution Service for misconduct in public office.**
- **In Nottinghamshire, a Police Sergeant was handed a twelve month jail sentence after being convicted of accessing police systems in order to obtain personal data for non policing purposes.**
- **In Humberside, action is still outstanding in the case of a member of staff who used Police systems to access information about a potential partner which they used to send harassing e-mails and letter.**
- **In Essex, a Police Sergeant was given "advice" by a disciplinary panel after accessing confidential records systems to obtain his ex-wife's details and passed them to his solicitors.**
- **In West Mercia, one police officer was handed disciplinary sanctions after using Police systems to access confidential information about their neighbour. Another was disciplined for conducting background checks on partner and a work colleague.**
- **In Norfolk, a Police Community Support officer received a caution and was dismissed from their job after being found guilty of accessing details of a call to the Police and passing details of it to a family member.**
- **In Lancashire, a member of police staff was dismissed after a disciplinary panel found her guilty of disclosing confidential policing information on Facebook. A Police officer in the same authority was given a final written warning for conducting 53 criminal records checks for "no obvious policing purpose".**

55 Tufton Street, London SW1P 3QL
www.bigbrotherwatch.org.uk • 020 7340 6030 (office hours) • 07510 785 834 (24 hours)

Appendix B

Methodology

Each Police force in England was sent a Freedom of Information request by Big Brother Watch on 1st June 2011. Statutorily, responses to this Freedom of Information request had to be provided to Big Brother Watch by 29th June 2011. In order to accommodate the responses of authorities who had failed in their obligations to reply in a timely manner, responses received up to 8th July 2011 are included in this research.

The following questions were asked of each authority:

1. *The number of a) police officers and b) civilian employees have been convicted for breaches of the data protection act in the past three years.*

2. *The number of a) police officers and b) civilian employees have had their employment terminated for breaches of the data protection act in the past three years.*

3. *The number of a) police officers and b) civilian employees have been disciplined internally but have not been prosecuted for breaches of the data protection act in the past three years.*

In each case, Police Authorities were asked to provide a clear, itemised list of the offences committed by the individual in question i.e. *"Abusing privileged access to the Police National Computer"* or *"Passing information to an unauthorised third party"*.

For the purposes of this research, the definition of the "past three years" is the period up from May 2008 to May 2011. Police Community Support Officers (PCSOs) have been included in our definition of a "Police officer".

55 Tufton Street, London SW1P 3QL
www.bigbrotherwatch.org.uk • 020 7340 8030 (office hours) • 07810 785 834 (24 hours)

Appendix B

- **Results by Police Authority**

	Data Protection Act			Employment Terminated			Internal Discipline		
Force	Police	Civilians	Total	Police	Civilians	Total	Police	Civilians	Total
Avon and Somerset Police	0	0	0	0	1	1	25	7	32
Bedfordshire Police	0	0	0	0	0	0	7	1	8
Cambridgeshire Constabulary	0	0	0	0	4	4	4	8	12
Cheshire Constabulary	1	0	1	3	0	3	23	7	30
City of London Police	0	0	0	0	0	0	0	0	0
Cleveland Police	0	0	0	1	3	4	7	3	10
Cumbria Constabulary	0	2	2	1	1	2	13	9	22
Derbyshire Constabulary	1	2	3	3	2	5	11	4	15
Devon and Cornwall Constabulary	1	0	1	1	0	1	24	14	38
Dorset Police	0	1	1	0	2	2	10	4	14
Durham Constabulary	0	0	0	0	1	1	0	3	3
Dyfed Powys Police	Refused to provide information								
Essex Police	0	1	1	3	0	3	7	4	11
Gloucestershire Constabulary	1	0	1	1	2	3	3	5	8
Greater Manchester Police	1	0	1	0	1	1	3	2	5
Gwent Constabulary	0	0	0	0	1	1	4	3	7
Hampshire Constabulary	2	2	4	3	1	4	22	11	33
Hertfordshire Constabulary	0	1	1	0	1	1	1	3	4
Humberside Police	0	0	0	1	4	5	34	28	62
Kent Police	2	0	2	5	5	10	7	21	28
Lancashire Constabulary	0	0	0	0	4	4	16	9	25
Leicestershire Constabulary	Refused to provide information								
Lincolnshire Police	Failed to respond								
Metropolitan Police	2	0	2	2	1	3	8	1	9
Merseyside Police	208			7			208		

55 Tufton Street, London SW1P 3QL
www.bigbrotherwatch.org.uk ■ 020 7340 6030 (office hours) ■ 07810 785 924 (24 hours)

Appendix B

	Data Protection Act			Employment Terminated			Internal Discipline		
Norfolk Constabulary	2	0	2	2	1	3	8	1	9
North Wales Police	2	0	2	2	0	2	18	2	20
North Yorkshire Police	Failed to respond								
Northamptonshire Police	0	0	0	5	0	5	3	10	13
Northumbria Police	0	0	0	2	4	6	20	19	39
Nottinghamshire Police	1	0	1	1	0	1	7	1	8
South Wales Constabulary	Refused to provide information								
South Yorkshire Police	0	1	1	0	1	1	26	16	42
Staffordshire Police	1	0	1	1	1	2	4	6	10
Suffolk Constabulary	0	0	0	0	0	0	5	3	8
Surrey Police	0	0	0	1	1	2	14	15	29
Sussex Police	0	0	0	1	0	1	17	2	19
Thames Valley Police	1	0	1	0	1	1	1	7	8
Warwickshire Police	0	0	0	0	0	0	0	0	0
West Mercia Constabulary	0	0	0	2	0	2	26	6	32
West Midlands Police	7	0	7	7	0	7	69	14	83
West Yorkshire Police	Refused to provide information								
Wiltshire Constabulary	Failed to respond								

55 Tufton Street, London SW1P 3QL
www.bigbrotherwatch.org.uk ■ 020 7340 6030 (office hours) ■ 07910 785 924 (24 hours)

Appendix B

▪ About Big Brother Watch

Big Brother Watch is a campaign from the founders of the TaxPayers' Alliance, fighting intrusions on privacy and protecting liberties.

Big Brother Watch produces regular investigative research papers on the erosion of civil liberties in the UK.

Whether it be by placing microchips in rubbish bins or snooping on your family using covert surveillance, we will name and shame the local authorities most prone to authoritarian abuse.

We champion individual cases. We want *to use the legal system to help the man in the* street fight injustice and regain his personal freedom; we are building up a legal fund to back such cases.

We will help you use the Freedom of Information Act to demand to see data held about yourself by the authorities, to extend our right to government information and to unearth the reality of the Big Brother state.

We want Big Brother Watch to become the central hub for the latest news and debates on personal freedom and civil liberty — a forum for information and discussion on something that directly affects British citizens in their everyday lives.

Big Brother Watch also aims to expose the extent to which the web has become the first line in state surveillance. The floodgates for the co-opting of internet activity into the state's control have opened, as companies are leant on to release online personal data. Safeguards are needed before it's too late.

We hope Big Brother Watch will become the gadfly of the ruling class, a champion for civil liberties and personal freedom — and a force to help a future government roll back a decade of state interference in our lives.

To arrange broadcast interviews or discuss the research, please contact:
Daniel Hamilton, Director, Big Brother Watch

Daniel.Hamilton@bigbrotherwatch.org.uk
Mob (24 hrs): **07810 785 924** | Tel: **020 7340 6030**

55 Tufton Street, London SW1P 3QL
www.bigbrotherwatch.org.uk ▪ 020 7340 6030 (office hours) ▪ 07810 785 924 (24 hours)

Appendix C

Table of Profiles of Disciplined Officers

	Gender	Age profile	Rank	Duties	Length of Service	Criminal prosecution	Current Status	Sanction
Officer 'A'	Male	40-45	Constable	Uniform	19 years	Yes – Fined at Magistrates court.	Remains employed	Final Written Warning
Officer 'B'	Male	30-35	Constable	Uniform	10 Years	No	Resigned prior to misconduct hearing	N/A
Officer 'C'	Female	35-40	Constable	Uniform	6 years	Arrested but not charged	Remains employed	Dismissed from force but on appeal sanction replaced with Final Written Warning
Officer 'D'	Female	35-40	Constable	Uniform	19 years	No	Remains employed	Final Written Warning
Officer 'E'	Male	30-35	Constable	Uniform	5 years	Yes – fined at Magistrates court	Remains employed	Final Written Warning
Officer 'F'	Male	35-40	Constable	Detective	11 years	Arrested but not charged	Remains employed	Final Written Warning
Officer 'G'	Female	25-30	Constable	Uniform	6 years	Yes – sentenced to 18 months imprisonment	Resigned prior to misconduct hearing	Currently imprisoned.

Appendix C

Detailed notes of interviews with disciplined officers

Officer 'A'

Officer 'A' continues to serve as a police officer. At the time of his computer misuse, he had 19 years service all at Constable rank. He is employed as a control room operator (communicator) within the force's control room. The nature of his misuse was the carrying out of a check on a vehicle registration number on the Police National Computer (PNC) for a former colleague who now works for a private detective agency. He classes his motivation as misguided loyalty to a friend. As a result of his computer misuse he pleaded guilty at court and was fined. Internally he was disciplined for gross misconduct and given a final written warning. On the previously discussed hierarchy this conduct is likely to fall around mid-table.

When asked about the scale of computer misuse the officer explained that the source data provided to him was very low compared to reality. He quotes *"I don't think any communicator can put their hand on their heart and say that they have never looked at an incident that they shouldn't have"*.

Throughout the interview the officer maintained that at the time of conducting the check he believed that as the person he was providing the information to was a former a police officer, his friend would still be covered by the Data Protection Act. The officer was clear that had he known that the check was unlawful he would not have done it, this he puts down to the fear of being caught, although at the time he was unaware of the possible sanctions for such activity.

When discussion moved on, the officer put forward the view that the majority of officers were unaware of what they could not look at on the systems, and certainly not how serious a matter it is. He stated that the figures shown to him in the 'Big Brother Watch' Source data, were totally unrepresentative for his own force and that as he did not believe his force to be any different to any other force, the likelihood was that all of the figures were under-representative of the truth. He did however acknowledge that in his view everyone knew they couldn't sell information or help criminals, this he believed to be very rare and he had no knowledge of such activity occurring. In relation to ease of access the officer was clear that in his case it was very easy, he was using a system that he was logged into all day and checks were not routinely carried out. Generally this created a perception for him that the chances of being caught were low. When asked about making computer misuse more difficult he was unable to see how this would be possible but even if it were, some officers would still find a way. He did state that if officers were more aware of the limitations of what they could and couldn't do, and that there were a high risk of being caught, fewer staff would breach the regulations out of ignorance, which in his view was what a high proportion of misuse could be ascribed to.

When asked about any stigma he may have experienced since the incident he was of the view that it was only self-imposed, and that none of his colleagues treat him any differently. He also stated that he had never witnessed any stigma attached to anyone for this type of misconduct. He was of the view that if it were stigmatised fewer people would be tempted to misuse the system.

Officer 'B'

At the time of his computer misuse Officer 'B' had 10 years service at Constable rank. He was employed within his force's crime bureau[139]. Having been discovered abusing the crime recording system and subjected to an investigation, the officer admitted his conduct and resigned from the force. The nature of his misuse was the searching for details on a young woman he had met and been out with a couple of times. He states that he searched the system to see if she had been the victim of any crimes, and to reassure himself that she was not making any allegations against him as he had not heard from her for a while. This particular type of computer misuse would fall towards the lower level of the described hierarchy.

This officer was clear that the scale of computer misuse is far higher than described in the figures given to him, although he does believe that the figures are falling. When asked if he were aware that his actions were wrong at the time he conceded that he did, but conversely that he did not fully understand the significance, and that he had some belief that provided he didn't give the information to anyone else or act upon it then it was not of a serious nature. He stated that in his view most people were unaware that they can't search for personal reasons, although knowledge on this is getting better. He stated that in his 11 years service he was only ever asked to sign one Data Protection Act reminder. He was clear that if more people were aware of the restrictions on use then less people would breach the regulations. The officer was asked about ease of access to police systems and replied that it was *"very easy and very simplistic, part of my daily routine"* He put forward his view that

[139] A force's Crime Bureau is the department responsible for the recording and administration of crime investigations.

one of the reasons so many people do so many unauthorised checks is that it is so easy. Making it harder would in his view dissuade most people.

When asked about his fear of being caught and the potential consequences the officer stated that at the time he did not believe there was a high likelihood of being caught and that he was not really aware of any audit capability on the system. He also stated although he was aware he may be disciplined, he certainly did not think it job threatening. He maintains the view that most serving officers hold the same belief as he had at that time. He does not believe that his force did enough to raise people's awareness of what is and is not allowed and what the consequences can be. Had he been more aware he would not have done what he did. He stated that the small efforts made by the force such as a 'pop up' when logging as a reminder of the Data Protection Act are useless as everyone just 'clicks past them'.

The officer was not aware of any internal stigma attached to computer misuse and at the end of the interview reaffirmed his view that generally the matter is not seen as serious by serving officers.

Officer 'C'

Officer 'C' is a serving officer working on an emergency response team. At the time of her computer misuse use she had six years service with the force. Both she and her husband were arrested as a result of computer misuse allegations, but no criminal charges brought. As a result of a gross misconduct hearing she was dismissed but later appealed and was reinstated with her sanction being reduced to final written warning. The nature of her misuse was checking intelligence systems for people her husband associated with at a local

pub, the information she obtained was passed to her husband who was not employed by the force. She maintains that she did this to make sure neither he nor she were vulnerable by mixing with criminals and to protect her position. She also states that her checks eventually widened to checking on family and friends of the associates. This would feature towards the lower end of the misuse hierarchy.

The officer was very clear that in her view the source data provided to her was a significant under-estimation of the scale of the problem. In her view 80-85% of people misuse the system. She stated that she started doing unauthorised checks just after she joined the force and continued throughout her career. She maintained that she did not fully understand that it was wrong, and that even during her training she was encouraged to look up family and friends in order to familiarise herself with the system. She states that had she known that it was forbidden she would not have continued with those searches.

When asked about ease of access the officer explained that not only was initial access easy, but that the system provided you with a series of links, making it very easy to look at associates of associates. The system was one she used every day for legitimate purposes and so there were no difficulties in gaining the data. She stated that she was unaware of any audits being conducted. The suggestion of making access harder was discussed but the officer did not feel that this would deter the majority of people. In the first instance she reinforced the point that most people do not know that they are not allowed to do personal checks and so making it harder would have no impact. Secondly she was of the view that those who did know what they were doing was wrong would probably find a way around it. She specifically mentioned that officers do not understand what is meant by the term *'Genuine Police Purpose'*.

The risk of being caught was discussed and the officer was of the view that generally it was next to zero. She explained that she herself was caught following an anonymous letter being sent to her force which led them to carry out an investigation. She stated that she never really gave any thought to the consequences of her actions, but when first confronted, thought that the misuse would probably warrant a telling off or at worst a written warning. The officer retains the view that most people still do not understand how serious it is, but added that following her experience her friends have stopped doing unauthorised checks.

'Officer C' was one of the very few interviewees who stated that she did feel that there was a stigma attached to computer misuse, and that for her returning to work was very difficult, in that she believed everyone thought she was corrupt and nobody trusted her.

Officer 'D'

Officer 'D' had 19 years service at the time of her computer misuse. She had worked in a variety of uniform roles at Constable rank. As a result of her actions she was originally dealt with for Gross Misconduct but following representations made on her behalf by the Police Federation this was reduced to misconduct. She received a final written warning. The nature of her computer misuse was the checking a variety of police system for details of her estranged husband and domestic incidents that they had both been involved in whilst undergoing a messy divorce. The officer maintains that she never misused the Police National Computer, but did use just about every system she had access to. She was however unable to gain any details as all records relating to police officers (in this case herself as she was also named on the reports) and their immediate family are routinely restricted allowing access by intelligence personnel and those officers specifically dealing with the case only.

The officer categorises her misuse as being for self-protection. She was discovered after her husband made a formal complaint to the force. The nature of this misuse would fall somewhere between lower level and mid-table on the hierarchy.

In discussing the scale of computer misuse the officer was of the view there is *"lots going on"* but not generally for malicious reasons. When questioned on this she stated that the majority of such checks are on neighbours and friends and that information is not passed on, but police officers are by their nature nosey.

The officer was asked if she knew at the time that what she was doing was wrong. She stated that had someone asked her at the time she would have replied "of course" but in some way she managed to reason to herself that it was ok and that she was entitled to the data anyway and had she gone through the appropriate channels it would have been provided to her. Conversely however she also stated that had she known categorically that she could not do those checks she would not have done so.

When asked about ease, the officer was clear that she was not actually able to view the records she was looking for as they had been restricted.

Officer 'D' raised the issue of consequences for what she had done. She stated that when served a with formal notice that she was under investigation it never occurred to her how serious the matter was until she was informed by the Police Federation. The officer believes that most officers have some awareness of what they can and cannot do on the systems but that there is *"some blurring of the lines"*. She is of the view that the organisation has gone some way to raising the profile of the issue but that more could be

done. She did not believe that there was any evidence of any stigma being attached to computer misuse.

When asked specifically about the risk of being caught she was of the view that unless a complaint was received or that the force was investigating you for some other reason the likelihood of being caught was very low. This she believed is also the perception of other officers. Whilst she is now clear on the seriousness of her actions she does not believe everyone else is aware of the significance of computer misuse.

Officer 'E'

Officer 'E' is a serving Constable with 5 years experience working as a response officer and on a local neighbourhood team. As a result of computer misuse he was suspended from work for four months and charged with a criminal offence for which he received a £1000 fine. He was subsequently disciplined internally and received a final written warning. The nature of his misconduct was the checking of police systems to assist his parents-in-law with a neighbour dispute and then passing this information on to his wife. He classes his motivation as being to help out his family but also maintains that he was not fully aware that what he was doing was wrong as it was information that his parents-in-law would have been entitled to had they made the appropriate requests through their local council. This would fall towards the lower to middle scale on the seriousness hierarchy.

The officer was asked about his view on the scale of computer misuse use, he stated *"there must be thousands more doing what I did."* He is of the view that most unauthorised checks are done out of nosiness or boredom.

When questioned further on his awareness of the fact that he was breaching regulations by carrying out the checks the officer responded that as far as he was concerned he was on duty 24 hours a day and that he did not believe he was doing anything untoward. He stated that as he looks back now he can see that he "*was a bit daft*" and that he wishes he had asked for help earlier. He stated that had he known categorically that he was not allowed to do the checks he would not have done so. He confirmed that he had had some Data Protection Act training in his probationary period but that he cannot remember much about it now and he does not recall seeing any refresher advice or training during his service. He is firmly of the view that generally people do not understand what they can and cannot do but that if people did understand and were aware of the potential consequences far fewer people would do it.

In discussing the ease of the computer misuse the officer confirmed that it was very easy as he only interrogated a system that he used every day. He was also of the view that the likelihood of being caught was very low, and that he had only been caught due to a complaint being made by a council official as she became aware that his family had information that they could only have obtained due to a leak from the police systems. The force then launched an investigation. Without some sort of complaint or information he remains of the view that being caught is extremely unlikely.

The officer was asked about any stigma he perceived as a result of being convicted and disciplined. He stated that he had not found any but that if he had thought that it were a possibility it would have influenced his decision making. He reiterated the view however that generally people were not aware that unauthorised checks was such a serious matter.

Officer 'F'

This interviewee remains a serving officer with 11 years experience, seven of which were as a uniformed officer and the last four as a detective. At the time of the computer misuse the officer was working within one of the most sensitive policing arenas, Special Branch, and was also a Police Federation representative. Following his computer misuse he was arrested and his home searched. The case was referred to the Crown Prosecution Service who discontinued the matter as *'not in the public interest'*. The officer was subsequently disciplined internally and received a final written warning. The nature of his computer misuse relates to searches on computer systems around his brother and his associates. Additionally having contacted police himself to report an incident involving his brother, on his return to work he accessed the system to view what had happened and to obtain linked details. The officer categorises his misconduct as to protect his brother. Again this type of computer misuse would feature towards the lower end of the seriousness hierarchy.

The officer was asked about his perception of the scale of computer misuse and was provided the source data. He was of the view that the data presented must be the tip of the iceberg. To back up his assertion he stated that having been through what he had experienced he was more alive to what other people were doing and he would notice on a daily basis people doing very similar things. He stated that in his view it did not stop at people just conducting checks, but also people passing information on, sometimes in good faith, but nonetheless breaching the regulations.

The issue of knowledge was discussed. 'Officer F' was firmly of the view that people do not fully understand what is acceptable and what is not. He stated that there is confusion particularly around family and friends. At the higher level seriousness of using police

information to assist criminals he was absolutely of the view that people knew this was criminal. In discussing the issue of the consequences of computer misuse the officer stated that he was aware at the time he was doing checks that computer misuse was serious and that one could be sacked for it. He did not however believe that what he was doing fell into that category. Generally he was of the view that officers do understand that computer misuse is serious, but that often they do not understand what is meant by 'computer misuse'. Greater understanding in his view would undoubtedly lead to less people breaching the regulations.

When asked about the general risk of being caught the officer was of the view that if an officer were being investigated for any matter or a complaint came in against them, PSD would carry out an audit on their computer usage, so the likelihood of being caught was reasonably high. He did not believe all officers were aware of this however and advanced that the majority of officers probably believe that the risk is quite low.

In discussing any potential stigma the officer stated that he had not personally experienced any and that his view was that for lower level breaches this was unlikely. He did however state that for more serious breaches involving helping criminals or selling information there would be a strong stigma and it would be difficult for an officer to hold any trust with his colleagues.

Generally the officer is of the view that at the lower level of computer misuse the biggest issue is awareness of the limitations of legitimate access and the confusion surrounding the term 'Genuine Police Purpose'.

Officer 'G'

Officer 'G' was a constable of 8 years working as a uniformed officer on a response team. The officer was subject of a proactive operation by her force for suspected computer misuse and resigned shortly after being arrested and charged. At court she was sentenced to 18 months imprisonment. At the time of the interview the former officer was halfway through this sentence. The nature of the computer misuse was assisting her boyfriend and his friend in the supply of cocaine. Information provided included the fact that one of them was currently being sought by police. The former officer also received cocaine in exchange for the information she provided. This former officer's conduct is at the higher end of the seriousness hierarchy.

On being asked if she was aware that what she was doing was illegal this subject was very clear that she did. She also confirmed that although the actual access to the information was very easy, as she only used systems that she would be expected to as part of her normal working day, she always held the view in the back of her mind that she would one day be caught, and that in her words, she was "*on borrowed time*". She stated that she was aware that a number of audits could be done on her computer usage and accepted this risk. Generally however for computer misuse at the lower level of just nosiness she was of the view that officers were unlikely to be caught and that most people shared this perception. Significantly the former officer stated that on no occasion did she misuse the Police National Computer as she would be required to come up with some reason for any checks on this system, whereas on other computers no such reason needed to be provided.

When asked about her perception of the scale of computer misuse she was of the view that it was very widespread within her force, she acknowledged that rarely was it at her level,

and in fact that she did not know of anyone else doing exactly what she did, as by the nature of criminal activity at that level, people keep things very well hidden, but unauthorised checks out of nosiness or boredom were commonplace.

When asked whether everyone is aware of what is and is not acceptable the officer was of the view that most people are, and that generally people do understand what is and what is not a *'Genuine Policing Purpose'*. She pointed out that her force had put warnings on computer systems that pop up when you log in and that she had received training on the Data Protection Act.

The former officer was asked whether in her opinion there was any stigma attached to computer misuse, she was unable to provide any definitive response but suggested that it varied. She did not feel that even if it had been an option, she could have continued as a police officer.

Generally this interviewee was of the view that the matter of computer misuse was very serious and that generally people understand what they can and cannot do. For the greater part however she believed that most people felt that unless computer misuse is at the higher end and involved with criminality the likelihood of being caught was low.