Contemporary organisational pathologies in police information sharing: new contributions to Sheptycki's lexicon of intelligence led policing

Author: Ian Phillip Stanier

Professional Doctorate awarded by London Metropolitan University

Submitted: February 2013

Declaration

I certify that the thesis I have presented for examination for the Professional Doctorate degree of the London Metropolitan University is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of a work carried out jointly by me and any other person is clearly identified in it).

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

....

Ian Stanier

Contents

Appendices

Abstract

Inadequate information sharing practices remain a significant contributory factor in police intelligence and investigative failure. The consequences are serious, as ineffective and inefficient policing present direct threats to the very community police seek to protect. The modern digital environment, enabling legislation, high level commitments to information sharing, and, depressingly, recurring criticism arising out of high profile information management failures, appear not to have made any discernible positive difference. This thesis seeks to understand why information sharing failures still stubbornly remain, using as its starting point Sheptycki's (Sheptycki, 2004) eleven organisational pathologies in information sharing in police intelligence systems. This thesis's research reveals a complex inter-connected array of factors actively undermining effective information sharing within policing and wider law enforcement but holds that three are central to any attempt to improve processes. It contends that a combination of codified and simplified legislation and regulation, a professionalization of the role of the intelligence operative and the criticality and smarter use of available data management technologies, can significantly reduce information sharing pathologies. Accordingly, the thesis offers suggestions for essential next steps to tackle these three key challenges to enhanced police information sharing.

Acknowledgements

I would like to thank my family who made many sacrifices over the years, allowing me the time to research and prepare this thesis. I also would like to thank my friends and colleagues for their support in securing the funding, time given to debate the hypothesis and the subsequent friendly arguments that ensued.

Table of Legislation and Cases

United Kingdom

Audit Commission Act 1998 (c.18) London, HMSO.
Children Act 1989 (c.41) London, HMSO.
Civil Contingencies Act 2004 (c.36) London, HMSO.
Criminal Justice and Public Order Act 1994 (c.33) London, HMSO.
Criminal Procedures and Investigations Act 1996. (c.25) London, HMSO.
Crime and Disorder Act 1998 (c.37) London, HMSO.
Criminal Appeals Act 1995 (c.35) London, HMSO.
Criminal Justice Act 2003 (c.44) London, HMSO.
Data Protection Act 1984 (c.35) London, HMSO.(Repealed:1/03/2000)
Data Protection Act 1998 (c.29) London, HMSO.
Freedom of Information Act 2000 (c.36) London, HMSO.
Health and Safety at Work Act 1974 (c.29) London, HMSO.
Human Rights Act 1998 (c.42) London, HMSO.
Immigration Act 1971 (c.77) London, HMSO.
Immigration and Asylum Act 1999 (c.33) London, HMSO.
Intelligence Service Act 1994 (c.13) London, HMSO.
Interception of Communication Act 1985 (c.56) London, HMSO.
Misuse of Drugs Act 1971 (c.38) London, HMSO.
Offender Management Act 2007 (c.21) London, HMSO.
Official Secrets Act 1911 (c.28) London, HMSO.
Official Secrets Act 1920 (c.75) London, HMSO.
Official Secrets Act 1989 (c.6) London, HMSO.
Police Act 1997 (c.50) London, HMSO.
Police and Criminal Evidence Act 1984 (c.60) London, HMSO.
Police Pension Regulations 1987 (No.257) London, HMSO.
Proceeds of Crime Act 2002 (c.29) London, HMSO.
Prison Act 1952 (c.52) London, HMSO.
Prison and Young Offender Rules (1999) (No. 728) London, HMSO.
Regulation of Investigatory Powers Act 2000 (c.23) London, HMSO.
Security Service Act 1989 (c.5) London, HMSO.
Serious Organised Crime and Police Act 2005 (c.15) London, HMSO.
Terrorism Act 2000 (c.11) London, HMSO.
Wireless Telegraphy Act 1949 (c.54) London, HMSO.

Foreign

US Congress (2010) *Reducing Over-classification Act 2010.* Public Law. 111-258 Oct.7,2010

Convention, Treaties and Directives

European Convention on Human Rights and Fundamental Freedoms
EC Data Protection Directive 1995 (Council Directive 95/46/EC on the protection of individuals with regard the processing of personal data and on the free movement of such data)

Cases

Chappell v UK (1989) 12 EHRR 1)
Chief Constable of Humberside and Anors v The Information Commissioner [2009] *EWCA Civ 1079.*)
Guerra v Italy App no. 307-B, para.92).
Khan v UK (2001) 31 EHRR 45
Leander v Sweden (1987) 9 EHRR 433).
Malone v United Kingdom (Application 8691/79) (1984) 7 EHRR 14, ECtHR, (Application3 5394/97) (2000) 31 EHRR 45, 8 BHRC 310, ECtHR).
McCann v UK The ECrtHR (application 18984/1991)
McCann and others v United Kingdom [21 ECHR 97 GC]
Osman v UK (1998) 29 EHRR 245
X *(South Yorkshire) v Secretary of State for the Home Department and Another [2012] EWHC 2954 (Admin)*

List of acronyms and abbreviations

ACC	Assistant Chief Constable
ACPO	Association of Chief Police Officers
ACPO TAM	Association of Chief Police Officers Terrorism and Allied Matters
ANPR	Automatic Number Plate Recognition
AO	Authorising Officer
APA	Association of Police Authorities
ASB	Anti Social-Behaviour
ASIS	Australian Secret Intelligence Service
BC	Benefits and Credits Directorate
BCU	Basic Command Unit
BoF	Back Office Function
CDA1998	Crime and Disorder Act 1998
CDRP	Crime and Disorder Reduction Partnership
CI	Chief Inspector
CIA	Central Intelligence Agency
CID	Criminal Investigation Department
COMPSTAT	Computerised Statistics
CPA	Crime Pattern Analysis
CPT	Child Protection Teams
CSP	Community Safety Partnership
CT	Counter-Terrorism
CTU	Counter-Terrorism Unit
DC	Detective Constable
DCC	Deputy Chief Constable
DCI	Detective Chief Inspector
DI	Detective Inspector
DIM	Daily Intelligence Meeting
DMM	Daily Management Meeting
DOI	Director of Intelligence
DPA1998	Data Protection Act 1998
DS	Detective Sergeant
DSU	Dedicated Source Unit
ECHR	European Convention of Human Rights and Fundamental Freedoms
FIB	Force Intelligence Bureau
FIO	Field Intelligence Officer
GCHQ	Government Communications Headquarters
GPMS	Government Protective Marking Scheme
HMIC	Her Majesty's Inspector of Constabulary
HMICP	Her Majesty's Crown Prosecution Inspectorate
HMPS	Her Majesty's Prison Service
HMRC	Her Majesty's Revenue and Customs
HO	Home Office
HRA1998	Human Rights Act 1998
ILP	Intelligence-led policing
IOCA1985	Interception of Communication Act 1985
IOCCO	Interception of Communication Commissioners Office
IM	Intelligence Manager
IMS	Information Management Strategy
IPCC	Independent Police Complaints Commission
IR	Intelligence Requirement

IOMU	Integrated Offender Management Units
ISA	Information Sharing Agreements
LEA	Law Enforcement Agencies
LIM	Laminated Intelligence Methodologies
MAPPA	Multi Agency Public Protection Arrangements
MOD	Ministry of Defence
MoJ	Ministry of Justice
MOPI	Management of Police Information
MPS	Metropolitan Police Service
NCPE	National Centre for Policing Excellence
NCA	National Crime Agency
NCIS	National Criminal Intelligence Service
NCS	National Crime Squad
NFIB	National Fraud Intelligence Bureau
NFIU	National Football Intelligence Unit
NIM	National Intelligence Model
NPIA	National Policing Improvement Agency
NPM	New Public Management
NPP	National Policing Plan
NPT	Neighbourhood Policing Team
OPT	Operational Partnership Team (Formerly PAS)
OSC	Office of Surveillance Commissioners
PACE1984	Police and Criminal Evidence Act 1984
PAS	Police Advisors Section (now OPT)
PCSO	Police Community Support Officers
PIO	Police Intelligence Officer (Prison)
PITO	Police Information Technology Organisation
PNC	Police National Computer
PND	Police National Database
RIPA2000	Regulation of Investigatory Powers Act 2000
RCS	Regional Crime Squad
RIU	Regional Intelligence Unit
SFO	Serious Fraud Office
SMT	Senior Management Team
SOCA	Serious Organised Crime Agency
STCG	Strategic Tasking and Coordination Group
SIS	Secret Intelligence Service
SISII	Schengen Information System II
SyS	Security Service
T&C	Tasking and Coordination Process
TSU	Technical Support Units
TTCG	Tactical Tasking and Coordination Group
UKBA	United Kingdom Border Agency
YOTS	Youth Offending Teams

Chapter One

Introduction

Sheptycki's[1] work, *'Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-led Policing'* (Sheptycki, 2004, pp.307-332) categorised eleven United Kingdom (UK) police information sharing pathologies, and these provide the benchmark for assessing contemporary pathologies in this thesis. Since its 2004 publication, aspects of information management have been subject to close scrutiny from Government Inquiries, judicial review and *Independent Police Complaints Commission* (IPCC investigations. His information sharing pathologies have been exposed to advances in data handling technology, new legislative provisions, the introduction of detailed regulatory administrative frameworks, learning from critical inquiry and imperatives from continuing and new national and international security threats. Set against this backdrop, it might well be assumed that Sheptycki's pathologies would now be outdated, no longer relevant and consigned to annals of police intelligence history. This thesis holds that the pathologies still exist, and new ones have emerged. It will highlight that this dismal situation has arisen as a consequence of three challenges; legislative provision, the role and status of the intelligence professional within policing and the use of technology. It will argue that legislation needs to be codified, simplified and utilised, to introduce a duty to share default. It will stress the importance of a valued and organisationally embedded culture of intelligence professionals, and finally it will emphasise the requirement to work more efficiently to maximise the potential of technology in support of information sharing.

The Research

The thesis tests this perspective, drawing on appraisals of IPCC investigations, Government initiated inquiries and findings from primary research involving intelligence practitioner interviews and focus groups. All of this material is used to examine contemporary information sharing shortcomings within policing, particularly the three areas identified above. The research provides an evaluation of extant information sharing challenges, an identification of new pathologies and the factors by which they are sustained, augmented or moderated. From this assessment, proposals are submitted to address critical and persistent pathologies with a

[1] Sheptycki,J. (2004) Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-led Policing. *European Journal of Criminology Volume 1 (3),* pp. 307–332.

view to enhancing information flow between collectors, holders and users across the criminal justice and security sector.

Background

On joining the *Metropolitan Police Service* (MPS) in 1985, I very quickly understood that to deliver effective operational responses to community problems, high quality, corroborated and timely intelligence is required. Intelligence is a prerequisite. It was as important then, as it is now, in driving police enforcement activity by determining operational priorities and informing decision making. It is key to appropriate resource allocation in response to a given problem. It is central to the design and selection of bespoke operational tactics and subsequent justification of the use of proportionate risk control measures. In the mid 1980s, intelligence's importance was neither structurally nor even informally recognised, whereas now, the corollary of intelligence with operational policing is acknowledged, if not always necessarily resourced accordingly.

My six month initial training at the MPS Hendon Police College included forty-five minutes on intelligence, limited to an explanation of the existence of the 'collator's card' system and basic guidance on where information I had collected during my tour of duty should be recorded on my return to the police station. During the remaining eighteen months of the probationary period I received no further inputs on intelligence. My evaluated record of work, key to passing my probationary period, was primarily based on evidencing the number of traffic prosecutions and arrests made. There was no requirement to evidence any contribution to a police model which produced a formal intelligence picture of threat and harm to the community.[2] Perhaps unsurprisingly, recorded crime was spiralling at that time.

Mobilised by the new thinking introduced through the MPS '*Systems For Detection*' (SID) Project which adopted an offender focused and intelligence based ethos, I embarked on a career that undertook a series of intelligence based roles including crime analyst, football intelligence officer, public order intelligence officer, surveillance and intelligence policy officer, informant handler and controller, prison intelligence officer, automatic number plate recognition intelligence unit, various intelligence supervisor positions and covert policing trainer.

[2] Metropolitan Police Service (1985) *Probationers Record* The Yellow Book. London:MPS.

As a consequence of this chosen career pathway, I gained exposure to, and insight of, various categories of intelligence failure associated with policing, many of which were neither exceptional nor unique.

Research Aim and Research Question

The aim of this doctorate is to identify contemporary obstacles to effective sharing of police information and intelligence, to assess which poses the greatest challenge and threat, and eventually to provide recommendations for changes to reduce the likelihood and impact of information sharing failures. It takes an interpretive approach in attempting to answer the research objective to find the contemporary organisational pathologies in police information sharing. By doing so it allows the research greater scope to address the extent of influence and impact of each of the identified pathologies.

By using Sheptycki's eleven information sharing pathologies as a benchmark, there is a credible starting point to track how the pathologies may have altered with current policing methods. The thesis assesses these in the context of organisational processes, practices and structures. It considers the current position on information sharing by drawing on stakeholder interviews, intelligence officer focus groups, legislative provisions, and academic literature. The thesis analyses primary and secondary data including official documents, inquiries and publications, and includes a review of protected and restricted material, internal policing policies and doctrine and archived material.

The importance of identifying and implementing solutions to apparent perennial information sharing pathologies is based on the need to effectively serve and protect different communities. The pathologies and subsequent failures do not simply generate material of theoretical interest. They lead to reputational damage, inefficient use of taxpayer's resources, undermined community trust and confidence in policing, increased crime/disorder and serious harm to life and property.

The thesis will also explore the emergence of various policing models, including problem orientated policing, intelligence led policing and community policing in the context of intelligence development. It adopts a developmental approach in assessing the emergence of formal, structured, multi-tiered intelligence organisation. It analyses the various definitions put forward to explain what is meant by 'intelligence' and 'information' in a policing context, and how these definitions shape information sharing decisions.

Information sharing failure associated with organisational subcultures is considered, revealing two areas not explicitly mentioned in Sheptycki's eleven pathologies: technology, its use, functionality and reach; and the interpretation, clarity and impact of existing legislative powers.

These factors can be both the most powerful enablers for information sharing, and the main obstacle. The police service is bound by legislation and common law. It interprets these in an increasingly risk averse organisational culture and critical society. One of the consequences is that information holders then avoid decisions that may attract closer scrutiny and criticism. The existing legal ambiguity associated with information management and sharing attracts inaction or deferred decision making, impacting on decisions whether to share information to customers and partners.

In an information-rich age, effective management of vast volumes of data requires the use of technology that can securely hold, filter, evaluate and disseminate data. Technical solutions to information sharing are available, but implementation is hampered as a consequence of organisational structures within UK law enforcement agencies. Legacy systems, procurement approaches, connectivity and different operating requirements and standards all pose difficulties for effective information sharing. Most are simply not able to pull or push timely and relevant information to the people who can use it, at the time and place they need it, and in a convenient format for them to be able to absorb it quickly to inform decision making.

Key Concepts

The key concepts explored in this thesis are: information sharing pathologies, police intelligence, and intelligence models.

Information sharing pathologies: These describe the organisational problems that impact on the effective and efficient collection and sharing of police information. The thesis takes as it's starting point Sheptycki's (Sheptycki, 2004) eleven information sharing pathologies[i] in police intelligence systems, and reviews these in the context of information sharing problems identified since publication of his 2004 Article.

Police intelligence: To some (Grieve, 2004, p.35), police intelligence *'is about making sense of ambiguities or contradictions and recognising the relative importance of different elements.'* Various definitions of intelligence exist, not just within a policing setting, but also within a wider national security and military context, where the lines are increasingly blurred between state security operating arenas. The thesis considers whether the actual difference between intelligence and information is simply based on semantic sparring. It considers whether distinction between national security intelligence and criminal intelligence is in practice a false dichotomy. It looks at whether these different definitions shape information sharing pathologies.

Intelligence based models discussed in this thesis, i.e. *Intelligence Led Policing* (ILP), *Problem Orientated Policing* (POP) and the *National Intelligence Model* (NIM), represent attempts by the police to impose order on chaos. The ILP, POP and the NIM were all developed with the aim of enabling law enforcement to manage the increasing demand for their services. This would allow them the space to create an operational reserve, not committed to reactive policing, which therefore could be used to resource longer-term problem-solving measures.

Sheptycki's eleven Information sharing pathologies

The process of intelligence production in a police operating environment is primarily about the way in which information moves within and between units, departments, forces, partners and national and international policing agencies. To assist, it may be useful to provide a short introduction to each of Sheptycki's pathologies.

Digital divide

Unlike many European countries, the UK police service is fragmented. England and Wales have forty-three different police forces, all developing and evolving their own practices and systems, and offering different interpretations to published national policing guidance and doctrine. A consequence of this is an array of different ICT 'legacy systems'. Even within forces, different ICT systems, including intelligence databases, record, store and manage data in different ways. Few systems store all the force intelligence and information centrally, and accordingly 'all source assessment' is very difficult. To a large extent, the *'continuous and uncoordinated upgrading of ICT systems.'* (Sheptycki, 2004, p.314) is still an on-going issue.

Within this information pathology, Sheptycki highlights the difficulties of management of information where there is a cross border event (he uses the example of missing persons where the search took place over two force areas), introducing the *'communications divide'* (where crucial information is not effectively communicated between two different forces). The 'digital divide' can delay effective analysis of information that is time critical, thus undermining 'real time' opportunities. The extent of the digital divide can be significant. The *Serious Organised Crime Agency* (SOCA) inherited over 138 different ICT systems during its merger with different law enforcement agencies, including *HM Revenue and Customs*, the *National Criminal Intelligence Service* and the *National Crime Squad (*Harfield and Harfield, 2008, p.107).

Linkage Blindness

Sheptycki's concept of 'linkage blindness' describes how an analyst's ability to spot a series of crimes that would have otherwise been linked through a link of commonality can be undermined. The failure to share information means that the analyst is left with inadequate or insufficient data to make an accurate and complete assessment. He holds that when a *'crime series transgresses force boundaries, and the horizontal connections for sharing relevant intelligence are inadequate or non-existent, linkage blindness occurs'*. (2004:315) Sheptycki stresses that this is a system problem rather than an ICT based one, and as such is a separate issue. Sheptycki's field observations indicated that, even where internal procedures permit, the horizontal flow in information hierarchies is often poor because police organisations focus most effort at ensuring information sharing moves in a vertical flow rather than the more pragmatic and practical horizontal flow.

Noise

Often information is collected by different people than those processing the intelligence. This distance means that, on occasions, the circumstances of the collection, the rationale for the initial recording decisions and the provenance of the information itself, is not known or fully understood. As a consequence, relevant intelligence in relation to an emerging problem may be discarded, not shared or overlooked. Sheptycki describes *noise* as that which *'pertains to the value of processed information circulating in the intelligence system. Information may be graded along a spectrum of usefulness, but this intrinsic quality is further shaped by decisions* *made about recording and dissemination'* (2004:315). The consequence is that there may be a significant amount of low quality, over-sanitized' or *'overly complicated'* intelligence in the system, impacting on subsequent intelligence products. The distance between the reporting, recording and interpretation of data will impact on the volume of 'noise'. This is because police personnel who turn information into intelligence often know little about recording decisions. Analysts who operate at a degree removed from such decisions are less able to qualify their interpretation of specific intelligence properly. This aspect of the pathology has also been noted by the military during intelligence collection during the Afghanistan conflict (Flynn, Pottinger and Batchelor, 2010).

Intelligence overload

Sheptycki reports that across policing, the lack of analytical capacity and associated administrative support means that the information becomes, on occasion, overwhelming. One of the consequences is that the information may be misinterpreted. His study found the problem exacerbated by forces having insufficient analysts, or redeploying them to other duties. The bureaucratic delays in processing the information meant that it became out-of-date, undermining effective action and created a backlog, cluttering the system further. If housekeeping is poor, data is not assessed and managed appropriately. Sheptycki highlights that *'Multiple recording of data on multiple systems and at multiple levels is a contributing factor'* (2004:316). A *compulsive data demand* also leads to overload of an intelligence system. This problem, ironically, can be fuelled by policing models that embrace ILP or POP. By not focusing on the collection of better quality data to assist analysts in determining the nature of an emerging crime problem, the emphasis, in practice, can be on the collection of more data, and as a consequence, the *'analytical capacity became more or less completely absorbed with the task of inputting the volume of reports received and contributing to an unspecified number of active operational investigations.'* (Sheptycki, 2004, p.316).

Non-reporting and Non recording

Poorly designed ICT systems may mean that intelligence recording is unnecessarily time consuming and onerous, especially when double keying of information is required. Regulations demanding input in a standard format may add to this administrative burden.

Moreover, each of these types of information could be of interest to other agencies and this might generate yet more reporting requirements. When pressed for time, especially in the context of a political commitment to reduce paperwork and the increasing demands on police during their tour of duty, it is likely that officers will either unwittingly or deliberately fail to record collected information on to force systems. Non-reporting by officers of information collected during their tours of duty may mean that *intelligence gaps* are not closed. It also has a knock on effect of contributing to *linkage blindness*, as links of commonality are not discovered. The non-recording of information has been identified as a constant problem, with the loss of experiential knowledge (Cope, 2008, p.405), biographical information on criminals (Van Duyne, 1999; Braga, Piehl, and Kennedy, 1999, p.294; and Higgins, 2004, p.80).

Intelligence gaps

Most of Sheptycki's organisational information sharing pathologies ensure that there is a gap in the police's knowledge of a specific problem such as a crime, an individual or an organised crime group. Sheptycki believes that an *intelligence gap* most obviously manifests itself in the so-called *'Level 2 gap'*[ii]. He holds that the *intelligence gap*s are also the consequence of the hierarchical nature of the intelligence system (local to force intelligence units, often responsible for cross border criminality to a national unit dealing with serious organised crime).

Duplication

Criminals do not dutifully adhere to expected operating levels, Basic Command Unit boundaries or even crime types. They may be of interest to a host of different law enforcement agencies across a force, a region or nationally. Duplication of effort can easily result, leading to the waste of financial and specialist resources and contributing to *linkage blindness* through institutionalised *information silos*. At the time of Sheptycki's report, the duplication was evident in the UK in the separate intelligence systems maintained by *HM Customs and Excise* (HMCE), the *National Crime Squad* (NCS) and *National Criminal Intelligence Service* (NCIS).

Institutional friction

Partnership working involving different law enforcement agencies is at its most effective when there is a seamless sharing of intelligence. This successful relationship is characterised by a collaborative working relationship rather than a hierarchical command. In reality, performance cultures can undermine collaborative working. *Institutional friction* is not limited to different agencies, but exists within the same body. Sheptycki (2004:320) holds that institutional friction is *'structural in origin and is not restricted to the inter-agency context, nor is this problem limited to the UK insofar as intelligence-sharing is concerned'.* Information sharing across bureaucratic boundaries can be negatively affected by this *'institutional friction'*. Sheptycki believed that a solution, or at least a partial solution, may come from the establishment of 'multidisciplinary integrated teams'.

Intelligence-hoarding and information silos

ILP is dependent upon information being shared with all the parties attempting to tackle an identified crime or disorder problem. Institutional friction may lead to two particular information sharing pathologies, 'information-hoarding' and 'information silos'. Information hoarding is symptomatic of the competitive performance culture in law enforcement and its sub-cultures. A 'good arrest' attracts status and praise, which may assist in career advancement. Sheptycki holds that this is an obvious motive to control information and limit dissemination to individuals or units that compete. The intelligence holders may attempt to justify non-sharing by arguing operational security, so the product is only released on a *'need to know'* basis. This rationale may be somewhat disingenuous, but need not be calculated - Sheptycki proposes that *'it may be a post hoc rationalization for not communicating relevant information that stems, in the first instance, from institutional friction. It may also be an expression of non-reporting or non-recording – such information, in effect, being 'hoarded' inside the head of the individual officer who finds the task of double-keying information too time consuming'* (2004:321). According to Sheptycki, *information silos* are *'the structural expression of hierarchical information systems'* (2004:321). During his research he found that intelligence relating to a crime type (he uses the example of vehicle theft) is expected to flow vertically upwards from the local, through a force intelligence unit and onto a national agency (in this case NCIS/SOCA). To Sheptycki, this vertical flow of information contributes to the loss of identification of linkages through horizontal information exchange.

Defensive data concentration

Pathologies result in a tendency to concentrate data collection on known problems, or a particular crime type, to the detriment of embarking on analytical work to identify any new or emerging crime trends. This can occur as a consequence of public concern over an issue such as gun crime or gangs, resulting in the establishment of a specific database for that task. To populate this database, intelligence tasking requests are sent out to police units to ensure that the relevant facts be concentrated in one place and analysed. This is another form of duplication of data, adding to the pressure on information management.

Differences of occupational subculture

The growth of the dedicated crime analyst has created tensions with the traditional role of investigators. The friction occurs when they appear to be working with competing interests. Sheptycki conceptualises this organisational pathology under single organization and intra-agency subcultures. At a simple level, the differences in terminology used to describe varieties of intelligence can impact greatly on future dissemination.

Thesis Structure

Chapter 2 establishes the rationale, scope and purpose of the study, and describes the methodology used. Case studies prove helpful in this research. It is acknowledged that there are some difficulties in validating case studies as a reliable research tool, but they do provide, if approached with rigour and objectivity, an opportunity to explore and understand phenomena affecting information sharing. It highlights some of the research challenges that police intelligence presents, and what strategies are employed to overcome them.

Chapter 3 explores the legislative framework in which information is collected, managed and shared. It introduces the oversight bodies that regulate implementation, application and use of the powers. The disparate provisions are highlighted, including case law, found at common law, primary and secondary legislation including the *Data Protection Act 1998*, the *Human Rights Act 1998*, the *Crime and Disorder Act 1998*, and the *Regulation of Investigatory Powers Act 2000*. The Chapter also examines how subsequent Government Doctrine (including the *Government Protective Marking Scheme* (GPMS) and ACPO doctrine (including the guidance on *Management of Police Information* (MOPI)) attempted to interpret legal provisions and provide more accessible guidance through bespoke national practice. It is argued that the police interpretation is causing (at best) hesitation that contributes to information sharing failures.

Chapter 4 analyses the development of policing in the context of intelligence. It adopts a developmental approach in assessing the emergence of formal, structured, multi-tiered intelligence organisations. It analyses the various definitions put forward to explain what is meant by intelligence and information in a policing context. It examines the various policing models that shaped and influenced intelligence use within policing, joint agency working and the accompanying prerequisite of information sharing. It explores how the various policing models that were supported by the introduction of the National Intelligence Model (NIM). It will examine to what extent the NIM was adopted by the police service, how it affected information sharing practice and organisational culture. It will assess how the absence of the intelligence professional has undermined effective information management and contributed to continuing information sharing pathologies.

Chapter 5 provides an overview of the key findings in relation to information sharing failures associated with policing since Sheptycki's identification of eleven pathologies. It will draw on the methodology used, the literature reviews, the interviews, and the focus group findings. It will look at aspects of *Independent Police Complaint* Commission (IPCC) investigations and other associated inquires where information management and sharing have been a contributory factor to negative outcomes.

Chapter 6 concludes the thesis by summarising the general findings and arguments. It will explain how the key obstacles to effective and efficient information sharing, (under-utilised technology, an absence of adequately professional culture, and flawed legislative provisions) can be addressed. It touches on areas worthy of further research, and contributes to the established lexicon of information sharing and intelligence led policing. Crucially, it will offer recommendations for improvements to information sharing.

Chapter Two: Research Methodology

Introduction

Information sharing failures pose a threat to life and property; they have the potential to undermine public confidence in the criminal justice system's ability to protect the public from harm and, in an increasingly difficult financial landscape, they equate to an inefficient and ineffective use of resources. This assessment of contemporary information sharing failures in policing offers a valuable opportunity to identify reasons, and make proposals, that tackle this recurring theme. This thesis is based on an analysis of official records, interviews from those responsible for the strategic and tactical management of police information, personal observations, accessible archival records, Government sponsored inquiries, documentary material and the collected views of other contributors to this study. The research methodology balances operational sensitivities with insight into relevant police practices.

Rationale

The thesis seeks to test whether police information sharing pathologies, first identified in Sheptycki's study (2004), still hold true in contemporary policing. It will test the claims of police advances in both technology and organisational culture associated with more effective information management.

The question this thesis will pose is whether the police are learning how to share information more effectively to ensure successful enforcement, crime prevention and public reassurance. It will examine whether the nature and form of information sharing pathologies has stubbornly persisted despite technological advances and revised doctrine falling out of previous information management and sharing failures, encapsulated through public inquiries (including The Bichard Inquiry, 2004) and *Independent Police Complaint Commission* (IPCC) investigations.

Background

Attention on intelligence failure and associated information sharing management issues have been dominated by events associated with terrorist attacks. The subsequent inquiry's and investigations into alleged failures have centred on what was known at the time, how was this interpreted by the receivers, and how was it managed and shared. Existing studies tend to focus on intelligence processes, structures, governance and failures associated with these national security matters[iii]. The missing dimension in UK intelligence studies is that of general police intelligence. Police information sharing has received relatively little attention, whereas numerous academic studies have produced articles on investigations, community policing, interviewing and covert policing. An evaluation of police intelligence practice and failure has been generally limited to issues raised in Government Inquiry, and event driven IPCC investigations.

The absence of any dedicated updated theoretical framework which seeks to explain police information sharing pathologies within the United Kingdom has probably contributed to an absence of strategies that effectively address the recurring themes.

Research design

When setting out to design the research methodology to support this thesis it appeared this would entail delving into a world that has been shrouded in some secrecy, out of a duty of care to the original source of information, and the need to protect operational collection methodology. Information is protected through the adoption of the principles and conditions laid out in the *Government Protective Marking Scheme*, articles within the *Human Rights Act 1998*, data management requirements under the *Data Protection Act 1998* and specific statutory provisions under the *Regulation of Investigatory Powers Act 2000*. These legislative provisions are covered in Chapter 3. Access to intelligence based information has to be undertaken with caution, and each use reviewed in light of the statutory provisions and the duty of care obligation. In practice this has limited its dissemination and use in support of police investigations or operations, and also in relation to this research.

The research design also considered how the research material was protected. It ensured that subsequent product was held securely either on password protected laptops or, where particularly sensitive, on Government approved encrypted memory sticks.

Government commitments to increased transparency and accountability have meant greater access to material that may have previously been difficult to obtain. Allegations concerning police mismanagement of information are now made available for public scrutiny. Many of these incidents and the circumstances around them would have previously been left unreported or remained undiscovered without data related legislation and new independent oversight arrangements associated with alleged disciplinary breaches or criminality by police.

These are now regularly investigated by the IPCC and the findings published albeit, on occasions, in redacted forms.

The research design took advantage of this greater openness associated with IPCC investigations. Access to information sharing failures has been possible due to legal requirements to publically publish findings. The IPCC has chosen to use its own web-pages to deliver this access and this thesis uses the findings to identify information sharing pathologies. I have been involved in the management of intelligence for over 25 years and accordingly I have used this insight into the application of policy and practices to guide my research design ideas. The police experience has undoubtedly shaped my attitudes, perceptions and interpretation of the subject area. My background includes the design and delivery of a Home office sponsored Prison Debriefing course, the delivery of advanced *Source Handlers* and *Source Controller's* courses, project lead in delivering the Metropolitan Police Service's covert policing strategy and membership of a number of covert and specialist intelligence working groups. I have exploited this experience to secure access to strategic and tactical leads currently operating in the intelligence world and to review policies in light of the thesis objectives.

This familiarity with the subject matter clearly has a bearing on the design, analysis and subsequent conclusions. It is, however, a double edged sword. It offers me an opportunity to appreciate the culture of the policing organisation and the intelligence community, and therefore relevant cultural sensitivities. Policing has its own jargon but it varies how this language is used. Non verbal communication is also easier for an insider to unpick. This shared understanding enables police officers to 'interpret words and gestures as they do' (Wax,1971). There is though, a potentially negative consequence. Accordingly, I also considered the concept of reflexivity at the research design stage and during the collection and subsequent analysis of data. Reflexivity has been described as *'an attitude of attending systematically to the context of knowledge construction, especially to the effect of the research, at every step of the research process'* (Cohen and Crabtree, 2006).

The role of the researcher is significant. Malterud (2001:484) stated that *'a researcher's background and position will affect what they choose to investigate, the angle of investigation, the methods judged most adequate for this purpose, the findings considered most appropriate, and the framing and communication of conclusions'*. Malterud's observations are important.

The police are a disciplined organisation, operating, at times, under quasi-military processes and conditions. Clearly, serving officers involved in this study are unlikely to be able to deliver 'value free data' collection. I acknowledge that my position and perspective will influence my collection and subsequent interpretation of both quantitative and qualitative data, but as Malterud states *' Pre-conceptions are not the same as bias, unless the researcher fails to mention them'* (2001:484).

The tools I selected to foster reflexivity include the use of research that included multiple investigators. This included the facilitation of focus groups with intelligence practitioners using an independent moderator. This sought to generate debate and dialogue in relation to information sharing, encouraging divergent positions and perspectives. The advantage of this was its ability to tease out hidden context and positions concerning values, assumptions and beliefs. Reinforcing this, I ensured police ranks were not part of the introductions, the focus group was away from police buildings and uniforms were not worn. I also developed a journal (a decision log), where I recorded my decisions as to why I used certain methodological positions, the logistics or the study, and personal reflections on the on-going findings. I acknowledged criticisms of research in this area and I sought to factor in these challenges in the design. I utilised open source information to corroborate sensitive information I had access to, and sought to use publically available official documents to evidence information sharing pathologies. During interviews with police officers the issue of rank needs to be factored in when interpreting the collection of information. Strategic lead respondents focused on corporate level organisational issues impacting on police information management practices. Lower ranks tended to focus on issues associated with day to day problems that impact on operational planning and specific investigations.

Methods

The methods adopted in the research sought to identify the nature and scope of information sharing within policing. It adopted primarily a qualitative approach to research and, as a consequence, required a proactive role in the collection of data (Wimmer and Dominick, 1997, p.84). The policing environment is at times fast moving, where decisions are made in response to immediate problems. The research design has not included 'artificial' studies. It explores the circumstances that led up to an apparent information sharing failure. Authentic examples provide an opportunity to see how information sharing differs between people, departments and locations, depending on available resources. The reality is complex and has many different layers of meaning (Berger, 1966).

Different perspectives or understanding of information sharing are further influenced by the owners' propensity to take risks. How people interpret information sharing situations, and their perspectives on what processes should be adopted, is relevant to information sharing pathologies. The research methods used are sensitive to all perspectives and as consequence different approaches are used to elicit as much information as possible from an array of perspectives. This will identify levels of compliance to information sharing procedures, the inconsistencies, the *'what should happen'* against the *'what does happen'*.

The qualitative approach explores how intelligence roles are perceived, how the professional community culture is formed and develops, and how policy was formulated, received and implemented within police organisations and partner agencies. The Sheptycki information sharing model is used as a basis for the thesis, which tests his model and builds on his work in a theoretically productive way.

Observation is used in the research methodology in a limited sense. As an active participant in intelligence based operations and investigations I am provided with access to the same operating circumstances as the police staff and officers. The research will introduce findings from an operation which was based, in part, on the development of intelligence, including the dissemination to operational teams and patrols. Involvement in this operation gave me access to sensitive documents, discussions and behaviour. I did not use audio or visual devices, nor were minutes taken from the regular meetings.

The disadvantage of participant observation methodology is that it is possible that my presence shaped or influenced subsequent management of information and linked activity. I acknowledge there may be a potential conflict of interest between my role as a participant in the actual operation and related academic interest.

An interpretive approach to the research was adopted. Some researchers hold that this approach is 'scientific' (Stevenson and Cooper, 1997, p.159) The approach assumes *'people create and associate their own subjective and inter-subjective meanings as they interact with the world around them. Interpretive researchers thus attempt to understand phenomena* *through accessing the meanings participants assign to them'* (Orlikowski and Baroudi, 1991) Due to the subject area, the choice of method is, in part, determined by the sensitivities of the data.

Interviews were used to secure an insight into the contexts, experiences and narrative of practitioners at both a strategic and tactical level. An interview has been defined as *'a purposeful conversation in which one person asked prepared questions (interviewer) and another answers them (respondent)'* (Frey and Oishi, 1995, p.1). Interviews can be of three main types; the first structured (closed interview style), secondly an unstructured interview (open interview style) or a combination of the two (Semi-structured style). Structured interview allows for consistency of questioning and delivery. It permits the interviewer to measure the depth of understanding the interviewee has about a subject area. The inexperienced researcher can be supported with pre interview planning and the drafting of specific list of questions. It can assist with the collation of standardised information providing a reliable source of quantitative data. However, the approach, with its scripted nature and formality, may discourage naturally flowing conversational exchanges, limiting incidental comments that can be revealing. The interview design is also crucial to its success. Poorly designed questions prevent the interviewee examining and exploring issues outside of the question script, and unexpected or rich answers may not be explored further. Consequently, information may be lost.

The thesis primarily used semi-structured interviews. They can provide an insight by securing evidence from key stakeholders involved directly within intelligence management. I believed that the less formal interview framework encourages openness and a dynamic exchange between interviewer and respondent. This contrasts with structured interview, which can prejudge the issues. The flexibility of the semi-structured interview interaction may allow areas, previously overlooked or discounted, to be probed further. It may start with general questions and then move to more specific probes. The weakness of this technique is that it is subject to both interview and respondent bias, can be costly and time consuming. To address this, the researcher can attempt to identify persons who provide perspectives from either end of the spectrum. Where possible, the content can be triangulated in an effort to corroborate comments and views. The benefit of this methodology is that product can be detailed and provide an excellent insight into the actual day-to-day workings of the intelligence management.

Unstructured or informal conversational interviews are another method of qualitative research. They rely on a spontaneous generation of questions, often in an interview setting. The weakness of this methodology is the systematic data collection is less disciplined, and the subsequent analysis more time consuming and difficult. Some interviews were undertaken using this method of interview. Unstructured interviews permit a free flow of information from the respondent. They have been defined (Nichols, 1991, p.131) as '*an informal interview, not structured by a standard list of questions. Field workers are free to deal with the topics of interest in any order and to phase their questions as they think best*'. They can be difficult to control, and the risk is that the respondent will provide material that is not relevant to the matter at hand. The advantage though is the respondent may cover issues not considered in the pre-interview planning, opening up new areas of study.

Social factors also impact on the interview process. All interviews are dependent on the interviewer ability to establish rapport. If achieved then the likelihood is that the information gleaned will be richer. A disadvantage of the general interview process, especially in covert policing, is that the researcher is likely to have to travel across the UK to secure a representative sample. The current legislation is geared towards legal authorities being issued by individual forces rather than a single national centralised authority's database. This brings with it logistical challenges, increased costs and travel. The assumption here is that once both parties have agreed, the interviews can be arranged with relative ease.

I employed methodological triangulation, using different methods to collect data including interviews, personal observations, published reports and open source research, to test the reliability of the results. This provided additional confidence and credibility that information obtained, either through quantitative or qualitative methods could be validated. As Cohen and Manion (2000, p.254) stated it offers 'an *attempt to map out, or explain more fully, the richness and complexity of human behaviour by studying it from more than one standpoint*'. Others have held it provides more meaningful data in that it '*gives a more detailed and balanced picture of the situation*' (Altrichter, Feldman, Posch and Somekh 2008, p.147).

Data Collection

Interviews were undertaken with strategic and tactical practitioners between April and December 2011. 15 interviews were undertaken on a one to one basis and 13 were engaged as part of a Focus Group. Respondents were chosen based on their daily experience of information management. All had extensive experience of operating within the police intelligence community. Structured and semi-structured interview styles offer the most opportunity for success in terms of accessing information on covert policing. However, with all interviews, it is difficult to verify whether the interviewee is lying or withholding information, hence the importance of using other methods to corroborate or dismiss what has been said. This is not straightforward, as some documentation that would help corroborate or dismiss information gathered is restricted due to operational security, source protection and duty of care obligations.

Another method of qualitative research has been conversational interviews, using spontaneous generation of questions, often in a workplace context, and occasionally during real time operational activity. The weakness of this methodology is that it is often unplanned and in response to ongoing events. The data collection was less disciplined and the analysis more time consuming.

Semi-structured interviews were also used with key stakeholders, including implementers, members of inspection units, analysts, intelligence officers and their 'customers'. The weakness of this technique is that it is subject to both interview and interviewee bias. To address this, I attempted to identify persons who could offer perspectives across the information management spectrum. Again, triangulation of methodology was adopted to corroborate and validate findings. The benefit of this approach was that the data was rich in detail and provided an excellent insight into the actual processes.

Documentary research was utilised during the thesis. The documents were primarily open source published material, although some GPMS restricted material was also reviewed. These documents included HM Government strategy documents, Ministerial speeches, legislative documents (including primary and secondary legislation) and ACPO addresses. This provided insights into matters associated with compliance, existing information sharing practices and emerging concerns. While the IPCC documents are central to this thesis research, other oversight bodies' reports are also considered, including the *Office of Surveillance Commissioners,* the *Interception of Communication Commissioners* and the *Intelligence and Surveillance Committee*.

While secondary sources are used, they have limited value. The documents are often produced and crafted in such a way that they meet the customer's requirements rather than for research goals. They may only offer a synopsis of original information from multiple sources with key original detail missing. Secondary source document trails are fragmentary as their content reflects what persons want/need in the data, or contain only the information that time and space permitted to allow for its content. Nonetheless, they may offer extensive literature lists allowing for further signposts into other research, thus reducing the time the researcher may spend exploring what else is already known about a subject area.

The qualitative methodology also involves research through open sources, primarily the internet. This provides wide access to academic research articles, media reporting and police 'blogs'[iv]. The advantage of unlimited and immediate access to internet based opportunities is always balanced with the credibility and integrity of the author and information cannot always be clarified and provenanced.

An extensive literature search also can be undertaken to secure a detailed and thorough understanding of the myriad of primary and secondary legislation, common law, reported cases, OSC guidance and prosecution policy associated with the subject matter. The literature search will entail the identification of relevant law reports using both a manual searches of libraries and academic institutions and Internet searches of web-based legal resource sites (*Lawtel* and *the European Court of Human Rights*).

A focus group was established to secure a broader collection of views about information sharing issues within policing. This methodology was chosen as it is particularly suited to securing different views and perspectives from participants. There was also a financial consideration, as the cost of arranging the focus group was considerably cheaper to run and quicker to organise than a series of individual meetings with strategic and tactical leads. The definition of the focus group in this context mirrors that proposed by Powell and Single (1996:449) in that it is a '*group of individuals selected and assembled by researchers to discuss and comment on, from personal experience, the topic that is the subject of the research*'. The attendees experience and knowledge encompassed the handling and dissemination of information across all three levels of criminality (local crime, cross border and national / international). To strengthen the impact of the focus group they were encouraged to debate with each other and reflect on their previously held assumptions. An advantage of the methodology is that it can identify solutions to information sharing pathologies and the focus group can act as a bonding process (Kitzinger, 1995). While the 'bonding' aspect is important, it can be undermined by dominant participants within the group (Wilmer and Dominick, 1997, p.107). To address this I used an experienced moderator to ensure that the exchanges remained relevant and to encourage all participants to share their views.

Nonetheless it is not certain that participants in the focus group or the interviews will provide candid answers. The ethnographer would argue that the artificial environment generates responses that are not found in the 'real world'. Behavioural research has suggested that what is told can often be at odds from what is actually done from both organisational and individual perspectives. The issue of openness, completeness and truthfulness of the answers is also another consideration, as failures to share information may leave officers and staff open to criticism, career threatening allegations or perceptions and in some rare cases, criminal proceedings. This means that many observations and experiences may be withheld, sanitised or reframed. Another limitation to focus groups is the potential skewing of data based on the selection and filtration of participants, and the nature of the questions posed to elicit responses. To address this, I chose police staff from different departments and forces, with whom I had no direct supervisory responsibility or previous connection. The focus group was operated under 'Chatham House rules' to reduce the group's apprehension over their disclosures.

The literature search including the reviews of *Independent Police Complaints Commission* (IPCC) published investigations and Government Inquiries, both of which reveal a rich seam of data on information sharing issues and recurring problems. The academic literature search for this area was examined in detail. There has been limited, if any, published research in the area of police information sharing failures, either before Sheptycki's work or since.

Central to the research design was a literature search and review of IPCC investigation reports. The IPCC is a non-departmental public body with overall responsibility for overseeing complaints made against police, including ACPO police forces, serious complaints against *HM*

Revenue and Customs, UK Border Agency staff exercising police-like powers and the SOCA in England and Wales.

The IPCC is responsible for ensuring the public have confidence in the regulation and investigation of complaints against police and other law enforcement agencies. The Chair, who is accountable to the Home Secretary, and Commissioners, oversee and take responsibility for IPCC investigations and associated casework. To maintain its independence, there is a statutory requirement that a Commissioner cannot have served as a police officer. The Commissioner's each have a geographical responsibility and most have lead responsibility for themed areas i.e. public order. The IPCC investigate the most serious allegations of misconduct or criminal behaviour including death or serious injury, serious or organised corruption and racism. It uses varied modes of investigation including *'Independent investigations'* carried out by their own investigators with all the powers of a police officer, *'managed investigations'* carried out by Professional Standard Units (PSDs) but overseen by the IPCC and PSD *'Supervised'* and *'local'* investigations.

A Commissioner's report differs from IPCC investigations. The purpose of a Commissioner's report is to share with the public the key findings and summary of the IPCC investigation, including the Commissioner's own decision making, the outcome of any legal processes that followed from the investigation, and the learning recommendations. The report belongs to the IPCC Commissioner who retains oversight of the investigation. The Investigation report is provided to the family or complainant, the police force, individual officers, and with a Coroner ahead of any Inquest. The Investigation report and related evidence is also provided to the *Crown Prosecution Service* when the IPCC considers that serious consideration should be given to whether or not a person should be prosecuted for a criminal offence. Investigation reports are published only in exceptional circumstances, because of data protection or other legal restrictions.

Data Analysis

The focus group was recorded contemporaneously rather than through the use of tape recording. This ensured the participants could speak more freely and honestly. Notes were made of each of the one to one interviews by myself. The notes were not a verbatim description of all that was said although some key statements were recorded in full. I ignored recording non verbal responses or interruptions from non-participants (ACPO level respondents has to periodically break off to respond to authority requests)

I collected copies both hardcopy and electronic of IPCC investigations and Government Inquiries, written responses and focus group notes.

Ethical considerations

Participants in the focus groups and the interviews were made aware of the purpose and use of the material gleaned. They were informed that comments made would not be directly attributable to any named individuals. Each participant was made aware that their contributions would be known to other members of the focus group. The focus group was not subject to audio recording to reduce the chance of compromise of any discussion. Warnings concerning the confidential nature of the group discussions were reiterated to participants and all were encouraged to maintain the group confidentiality. No participants raised any concerns or issues with the process.

All respondents were guaranteed anonymity although a number were content for their names to be attributed to some quotes. However I have taken the position that all will remain anonymous. The reason being is that identification of their association with specialist intelligence and covert policing techniques may, at a later date, be unhelpful.

All participants' involvement in the research was on a voluntary basis. No deception was practiced and I personally spoke to each participant explaining that they could withdraw from the focus group or interviews at any time. No concerns were raised, nor did any participant withdraw their support for the research.

Participants chose to be interviewed, in the majority of occasions, in their workplace. All meetings were in secure locations with no or limited access to non participants. Participants provided information during their tours of duty. No participant was instructed by their supervisors to participate.

Participants were selected based on a broad range of factors but primarily their involvement in intelligence management and use. Ranks ranged from Constable to Chief Constable, and included police staff analysts and researchers. Their intelligence fields varied from covert to discrete to overt policing. Participants were also drawn from partners, including members of prison service intelligence units where they undertook joint intelligence work with police. The majority of participants were male, although this reflected the profile of police intelligence units and the police service in general.

No participants, to the best of my knowledge, were excluded from interviews or focus group and no apparent problems have arisen since their involvement in the thesis research. All participants have been acknowledged.

The research was carried out in accordance with the London Metropolitan University's research ethics policy. I also gave proper regard to the six core principles for ethical research as laid down in the ESRC revised framework. This included the research ensuring integrity, quality and transparency, participants fully informed about the purpose, methods and use, and respect for confidentiality of all participants.

Research challenges

The nature of police operations and investigations understandably means that certain aspects remain sensitive and confidential. This is primarily to protect sources and methodologies, adhere to legal requirements and to avoid litigation. As a consequence some IPCC investigations were not published publically and some of those were published in a redacted form, so inference had to be drawn from the content.

There residual mistrust between academics and police could undermine the research design:

> *'there is sometimes a lingering cultural mistrust between police and academia that can hinder research partnerships. Some of this may be due to anecdote and some to actual bad experiences. On occasion, it is a clash of cultures and personalities—policing and academia are very different professional worlds. Police may fear, rightly or wrongly, that research will be politically biased, of poor quality, or misrepresent their own perceived position'* (Wilkinson, 2010, p.147).

Interviews were undertaken nationally and, therefore, at considerable financial cost. Some of the expense involved was reduced through the use of telephone interviews. This alternative allowed for more interviews to be undertaken in a shorter time frame. Some respondents were prepared to disclose more over a phone than a face to face interview, although the method undoubtedly reduced rapport building (important non verbal communication cues may have been missed), inter-personal dynamics were not engaged and the information flow potentially hindered. The telephone interview also meant that the interviewer can lose control as the interviewee can terminate the call without warning.

The access to ACPO was challenging in that diaries are often full many months in advance. I was grateful to all of those who rearranged diaries to permit me time. Longer interviews would have enabled more exploration of the issues raised outside of the specific line of questioning around Sheptycki's pathologies.

While every effort was made to ensure participants were confident that they could say what they felt and share their experience as openly as possible, I do acknowledge that some may have been aware of my rank and position (and that of other participants) and this may have influenced what they said and how they said it. I'm confident that the majority felt relaxed enough to be as frank as possible.

The interviews were secured on the basis of confidentiality to protect both organisational reputation and its staff. Certain aspects of the intelligence content process will not be commented on in detail due its assigned classification under the Government Protective Marking Scheme (GPMS) (Appendix A), and prohibitive statutory provisions. For the purpose of clarity, the GPMS is the national standard for classifying documents and information based on the likely impact if it were to be disclosed to hostile third parties. The scheme assists with the management of information sharing, storage, destruction and analysis, as adopted by UK law enforcement. (Note: The current GPMS is likely to be replaced with the Cabinet Office new categories of *Operational*, *Protected* and *Top Secret* which ascend in order of sensitivity)

Summary

I used both quantitative and qualitative methods to examine the information sharing pathologies identified in policing since 2004. This allowed me to assess whether the pre 2004 pathologies still remain valid or whether new pathologies have emerged.

Data was collected through focus groups, one to one interviews with tactical and strategic intelligence managers and users, open source Government publications/Inquiries and restricted police internal documents. Additional information was secured through an extensive literature review.

An assessment of the data was informed by both my previous knowledge of the area, previous research into information sharing inquiry findings and internal investigations. While every effort was made to remain objective and impartial, it is inevitable that my findings were shaped and influenced by my own experience of intelligence management, intelligence staff supervisory responsibilities and my organisational career path.

Chapter 3: Overview of legislation and police information sharing policy

Introduction

'There are symmetrical risks associated with data sharing – in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data.' (Thomas and Walport, 2008, p.i)

The chapter explores the scope and nature of the information sharing legislation, primarily focusing on statutes and provisions providing both explicit and implied powers which enable UK law enforcement and their partners to collect, store and share information. It examines the relationship between information pathologies and associated legislation, whose primary function is to protect confidentiality and sensitive methodology, rather than encourage further dissemination. It will also look at law enforcement information sharing doctrine, policy and issues affecting organisational risk assessment, all variables influencing organisational thinking and interpretation. The consequences of information management failure are discussed further in Chapter 5 during an examination of inquiries and reviews undertaken by the IPCC, HM Inspectorates, Government and the Judiciary.

The legislative landscape relating to information is complex. Harfield and Harfield (2008:125) view the legislative framework from a functional angle (statutory duty to disclose, to protect and discretionary disclosure powers), while Bessant (2009:94) characterised information sharing legislation as provisions which *'restrict, require or enable'*. The provisions can be distinguished as those enabling collection methodology (both overt and covert), and those determining the use of the information collected.

Statutory oversight and accountability arrangements

The perceived lack of accountability of law enforcement in its information and intelligence management activity poses a dilemma to its democratic legitimacy. According to Lowenthal (2009:199), efforts to reassure are *'a responsibility to be shared by the executive and legislative powers'*. Failure to do so undermines community engagement in crime reduction strategies and hinders the flow of valuable information used to inform decision making. The required oversight is delivered on different levels, including internal managerial control and accountability to parliamentary, judicial and 'independent' non-governmental bodies.

Oversight arrangements need not just focus on failures, but should also identify and promote best practice, monitor lessons learned and ensure momentum for implementation of recommendations. There is no single oversight arrangement, with different statutory provisions providing its own Commissioner, but the main bodies are briefly discussed here.

The Information Commissioner's Office (ICO) was established to *'uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals'*[3]. It oversees the *Data Protection Act 1998*, the *Freedom of Information Act 2000*, the *Privacy and Electronic Communications Regulations 2003*, the *Environmental Information Regulations 2004* and the *INSPIRE Regulations 2009* (the latter three involve *non-criminal* enforcement). The Information Commissioner responds to allegations of personal data mismanagement and acts as arbiter in information-related disputes. The ICO attempts to balance access to information and protection of privacy, while acknowledging the public interest in both. The ICO acknowledges that the *DPA 1998* and regulatory practice is broader than the individual right to privacy: *'10. the public confidence in information rights law as necessary, serving the public interest, effective in practice and properly enforced.* (ICO,2011, p.5).

To effectively regulate, any oversight body needs enforcement powers. The ICO powers include an ability to secure warrants for entry and inspection of premises where there are reasonable grounds for suspecting that the data controller is not complying with one or more of the eight *DPA 1998* principles listed in the table below:

	The '8' Data Protection Act 1998 principles
1.	Data should be processed **fairly** and **lawfully**
2.	Data should be obtained for a limited **specified lawful purposes** and not used in a manner incompatible with that purpose
3.	Data should be **adequate, relevant** and **not excessive**
4.	Data should be **accurate** and, where necessary, kept up to date

[3] Information Commissioner's Office (2012) *Homepage* [Internet] <http://www.ico.gov.uk/> [Accessed 30/06/2012].

5.	Data should be kept no **longer** than is necessary
6.	Data is processed in accordance with the Act and individual rights
7.	Data is held securely
8.	Data is not transferred outside of the EEA unless adequate data protection measures are in place.

The ICO two main tools, in terms of the *DPA 1998,* are the *Information Notice* (requiring production of information requested) and the *Enforcement Notice* (requiring specific steps to be taken in relation to data). A breach of the Enforcement Notice is a criminal offence, although, in practice, the use of both of these powers is rare, as the ICO seeks agreement through undertakings given by the data controller or by way of informal resolutions.

The *Regulation of Investigatory Powers Act 2000* (RIPA 2000) concerns covert policing practices used by public authorities. The Act provides oversight via four Commissioners, an Interception Commissioner, an Intelligence Service's Commissioner, an Investigatory Powers Commissioner for Northern Ireland and a Chief Surveillance Commissioner, responsible for both functions under the *Police Act 1997 Part III* and *RIPA 2000* provisions relating to Covert Human Intelligence Sources (informants, undercover officers and agents), and a number of forms of surveillance. They undertake inspections of covert activities, where necessary approve authorities, and hold public authorities to account for their activities, including the collection, storage and use of information and intelligence. All the activity of public authorities including the Intelligence Services and Law Enforcement are subject to an *Investigatory Powers Tribunal* that can receive, investigate and determine complaints from the public.

Additional oversight comes from the parliamentary *Intelligence and Security Committee (ISC),* established under the *Intelligence Services Act 1994, 'to examine the policy, administration and expenditure of the Security service, Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ)'*[4]. While not established specifically to deal with information issues, its remit has included an examination of the collection, storage and

[4] Intelligence and Security Committee (2012) *Introduction: About the Committee.* [Internet] 29/06/2012 <http://isc.independent.gov.uk/> [Accessed 29/06/2012].

management and proper use of intelligence and information (ISC 2002; ISC,2003; ISC,2005; and ISC 2009). The effectiveness of the ISC has been questioned in terms of its statutory nature, appointments process and Prime Ministerial control over subsequent published reports (Glees, Davies, and Morrison, 2007).

The *Independent Police Complaints Commission* oversees complaints against police in England and Wales, including allegations against the *Serious Organised Crime Agency (SOCA),* UK *Border Agency (*UKBA) and *HM Revenue and Customs* (HMRC). This is therefore also associated with the management and use of information and intelligence.

The Commissioners overseeing different legislative provisions offer an opportunity to strengthen accountability by the development of expertise and the establishment of professional working relationships. The fragmentary nature of oversight and accountability can be a weakness in itself (Gill, 2007, p.29), but the array of legislative provision is extensive, and a single Commissioners' Office could be unworkable.

Key legislative statutes

The primary legal framework underpinning information sharing are the *Human Rights Act* 1998 (HRA 1998), the *Data Protection Act* 1998 (DPA 1998) and *common law.* However, these Acts are just a small part of relevant information sharing legislative framework. Law Enforcement is cognisant of these legal requirements, and has made efforts to interpret the provisions in the context of policing. It does this through an array of internal and external policy, including codes of practice, guidance documents, threshold standards, Standing Operating Procedures and doctrine. The pre-eminent policing document with this regard is the ACPO (2010) *Guidance on the Management of Police Information* (2nd Edition), colloquially referred to as MoPI.

The first key statutory provision discussed is the *Human Rights Act 1998* (HRA 1998), incorporating the *European Convention of Human Rights and Fundamental Freedoms* (ECHR) into domestic law. Acting in a way incompatible with the ECHR makes public authorities vulnerable to challenge under *HRA 1998 Section 7*, and, if found to have acted unlawfully, subject under *HRA 1998, Section 8* to judicial relief or remedy. A number of the enshrined rights are applicable to police decision-making, and, as a consequence, influence information sharing practice and pathology.

Articles 2 (Right to Life), *Article 3* (Right not to be subject to torture, inhuman or degrading treatment), *Article 6* (Right to a fair and public hearing), *Article 8* (Right to respect for privacy and family life) and *Article 10* (Right to freedom of expression) all are fundamental rights when consideration is given on the appropriateness of information collection, its use and dissemination. The European Court has made judgements criticising operational teams' use of information, or lack of use. For instance, *McCann and others v United Kingdom* [21 ECHR 97 GC])[v] engaged rights under *Article 2.* In relation to *Article 8,* the judgement arising out of *Osman v United Kingdom [1998] [EHRR 101]* addressed issues about the failure to appreciate information received by police which the applicants held should have warned the police of the clear threat towards the applicants and their family. The judgement did not find a breach of *Article 2* or *Article 8,* but did find a breach of *Article 6* (Right to fair trial), in that the existing position on a blanket immunity that police owed no duty of care to the victims was not compatible with the ECHR. Orders requiring information to be disclosed have been supported by the European Court, subject to certain safeguards *(Chappell v UK (1989) 12 EHRR 1),* as have the collection and retention and non disclosure of material relating to national security vetting purposes *(Leander v Sweden (1987) 9 EHRR 433).* In certain circumstances, there are also positive obligations on a public authority to share information relating to the risk of environmental hazards *(Guerra v Italy App no. 307-B, para.92).*

Police decisions on whether they can share, or how they should share, turn on the definition of *'personal data'.* If information is information that is *personal* or *sensitive personal* data, then it falls under the auspices of the *Data Protection Act 1998* (DPA 1998), and is managed under its eight principles. Personal data, in this legal context, is information about a living person who can be identified from that data. Central here is an understanding of the circumstances around that personal data. Technically, a CCTV image of a person outside a shopping centre may fall under the *DPA 1998* definition, but clearly handling this information will be different to that of an image obtained by a hidden camera inside the person's house. The ethical dilemma involved requires proportionality which, in this context, means the more sensitive the information collected/observed, the greater the threshold of data management.

The *DPA 1998* was introduced to ensure compliance with the *EC Data Protection Directive 1995*[5]. Its predecessor, the *Data Protection Act 1984,* was limited to electronically-held data, and, at that time, most police intelligence was held on paper-based card indexes. It had limited remedies and minimal legal restrictions. The EC Directive and its UK manifestation, the *DPA 1998,* should mean that similar EU data standards in relation to personal information would allow it to be shared freely across member states, assisting Europol and the development of the police European data base, the *Schengen Information System* (Schengen II).

The *DPA 1998*, supplemented by other regulations and orders, only applies to personal information. It demands that those persons who hold or share personal information comply with eight principles of data sharing, and that processes are in place to safeguard the data. Individuals whose data is being processed are afforded a number of rights, including a right of access. These rights have caveats, in that organisations (including law enforcement) can rely on exemptions relieving them of the obligation to provide access, or comply with some of the other principle requirements. In essence, the Act allows the person who the data concerns 'Data Subject' rights over how it is used and managed.

To assist with interpretation and compliance, the ICO published the *ICO (2007) Framework Code of Practice,* which is not specifically focused at criminal justice organisations, but rather all organisations who exchange and disseminate information:

	The ICO Framework Code of practice
1.	Deciding to share personal information
2.	Fairness and transparency
3.	Information standards
4.	Retention of shared information
5.	Security of shared information
6.	Access to personal information
7.	Freedom of information
8.	Review

[5] Council Directive 95/46/EC on the protection of individuals with regard the processing of personal data and on the free movement of such data)

Element 1 requires the organisation to consider the objective of sharing the information. In a policing context, this may be to prevent, detect or prosecute crime. The element requires evidence of benefits and gain in criminal investigations, for example, the identification of offenders' locations as a consequence of sharing details of an address previously unknown, but now associated to the target of the investigation. This could be achieved by way of an electronic electoral roll or Voters Register. Considerations determining the sensitivity of information are a somewhat subjective judgement. Consequently, the risk appetite of an information holder may determine whether it is collected, accessed and shared with others.

Element 1, like *DPA 1998* Principle 1, asks what the legal basis for sharing is in statutory or common law.

Element 2 also has similarities with DPA 1998 Principle 1 (fairness), but clearly knowledge of information held on some subjects and locations cannot be disclosed without considering its use or origins, as it may have been provided by a *Covert Human Intelligence Source (CHIS)*.

Element 3 introduces information standards, an important aspect of any intelligence system – out-of-date information would lead to resources being wasted, inappropriate enforcement action (eg the wrong address searched[vi]) and reputational risk.

Element 4 introduces *'retention'* and, again, how long is justified can pose problems and disagreement (Bichard, 2004), and *Chief Constable of Humberside Police, Chief Constable of Staffordshire Police, Chief Constable of Northumbria Police, Chief Constable of West Midlands Police, Chief Constable of Greater Manchester Police v The Information Commissioner* [2009] EWCA Civ 1079.)

Element 5, the 'security of shared information', also poses challenges for policing, and has been a regular contributory factor in information sharing pathology (see Chapter 5). This security concern has contributed to arguably disproportionate requirements to regularly change passwords in different ways, leading to significant numbers of staff 'locked out' of intelligence systems[vii], and limitations on access to material.

Element 8's 'Review Period' has also attracted controversy, with challenges to police forces who continue to hold data on relatively minor criminal convictions. Attempts by the ICO to remove previous convictions from the Police National Computer (PNC) on the basis of Data Protection Principle 3 (excessive data) and Data Protection Principle 5 (data kept longer than necessary) failed, as police argued that they should have a right to store previous conviction data for their own use and for sharing purposes (*Chief Constable of Humberside and Anors v The Information Commissioner* [2009] *EWCA Civ 1079*). In this case, Lord Justice Waller stated that: '*If the police say rationally and reasonably that convictions, however old or minor, have a value in the work they do, that should, in effect, be the end of the matter*'. The Court's decision should bolster confidence that professional judgements of the police can carry some weight around information management. This judgement reinforced what a previous Information Commissioner had already stated, five years earlier:

> *'Police judgements about operational needs will not be lightly interfered with by the Information Commissioner. His office 'cannot and should not substitute [their] judgement for that of experienced practitioners'. His office will give considerable latitude to the police in their decision making. If a reasonable and rational basis exists for a decision, that should be the end of the story.' (Bichard: 2004:*136. Para 4.45.2.)

There is considerable misunderstanding around the *DPA 1998,* and training is negligible to the 'rank and file', even for those personnel undertaking dedicated intelligence roles. This lack of knowledge has an impact on information sharing. Some staff belief that they would be automatically obliged to provide access to police intelligence under the subject access request provisions under *DPA 1998 Part 7*. Even when a request arrives, there is uncertainty as to how to deal with it. Practitioners can often quote examples of officers who, until advised otherwise, would have disclosed everything, including sensitive methodology, or who would refuse disclosure to the applicant without explanation. The misunderstanding of the *DPA 1998* leads to unfounded concerns contributing to Sheptycki's *non-recording of information* pathology, due to a misplaced belief that recording the information may lead, eventually, to inappropriate disclosure. The reality is that the Act provides a number of exemptions to disclosure including *Section 28* (national security), *Section 33* (research and statistics), and *Section 35* (legal proceedings). Of particular relevance to police information is *Section 29,* which creates exemptions to certain data protection principles where data is processed or shared for the purposes of the prevention or detection of crime, and the apprehension or prosecution of offenders. The exemptions apply to certain principles of the DPA where the application of those principles would be *'likely to prejudice'* the purposes referred to above. These exemptions must be applied on a case-by-case basis and cannot be used to justify routine data processing.

In the case of X *(South Yorkshire) v Secretary of State for the Home Department and Another [2012] EWHC 2954 (Admin)* the High Court held that the offender should have a right of representation before a decision is made to disclose their details to person requesting them under the provisions of the non-statutory 'Child Sex Offenders (CSO) disclosure scheme. This provision allows the public to ask police for information on persons who has some contact with children with a view to ascertaining whether the person has convictions or other relevant information about them.

Where a specific or implied power does not exist for law enforcement to share information, but a police purpose is apparent, information may still be shared under *common law*, subject to an assessment of risk and management of further dissemination. The common law *duty of confidence* applies where information of a personal or sensitive nature is collected and recorded. A breach of confidence will apply when the information collected and recorded is used in an unlawful manner. There are a number of exceptions to the duty, specifically when:

- there is a legal requirement (either under Statute or Court Order) to disclose the information
- there is an overriding duty to the public (e.g. a criminal offence or life-threatening circumstances)
- the individual to whom the information relates has consented to the sharing.

The police also owe duty of confidentiality to victims and witnesses of crime, who may expect a greater level of privacy than offenders. A balance therefore needs to be struck between sharing such information, and the rights of victims and witnesses to privacy.

Consent does not need to be sought, for instance where a request meets a policing purpose and does not compromise operational procedures or an individual's safety. An assessment of the vulnerability of those at risk and the impact of the disclosure on the individual will need to happen before making a decision whether to seek consent.

The organisational anxiety over sharing information is best evidenced by the authority to share information with a school or an educational establishment about sexual offences, agreed by policing. It sets this decision and authority at Assistant Chief Constable, a rank relatively high (ACPO, 2010, p.63) when compared with other authorities: the power to strip search an individual (Constable[6]), the power to search a suspects house after arrest (Inspector[7]), a power to undertake directed surveillance on the coming and goings from a person's home (Superintendent or in urgent cases Inspector[8]), the power to undertake mass stop and search of a crowd looking for weapons (Inspector[9]), stops and searches under the *Terrorism Act 2000*[10] (Constable) and the power to forcibly take a non-intimate sample from a person at a police station (Constable[11]).

The *Regulation of Investigatory Powers Act 2000* (RIPA 2000) regulates public authority covert collection and use of information and intelligence. Its origin emanates from judicial criticism of the absence of statutory footing for covert policing within the UK (*Malone v United Kingdom* (Application 8691/79) (1984) 7 EHRR 14, ECtHR, (Application3 5394/97) (2000) 31 EHRR 45, 8 BHRC 310, ECtHR). Additionally, the *Human Rights Act 1998* requires policing activity to be 'lawful', and manifested in a substantive law expressly permitting the activity.

While some commentators hold that *RIPA 2000* has enabled informants to become more central to policing (Ratcliffe, 2008, p.217), and they caution against over-reliance (Innes, 2006, p.230), the reality appears to be different. An OSC Annual report (OSC, 2004, p.9) identified 5,900 CHIS authorisations by law enforcement in 2000, a figure which had fallen to 3,361 in 2011 (OSC, 2012, p.12). The number of law enforcement authorities for directed surveillance (ie the following of suspects or the observation of premises) recorded sharp decreases from 26,986 authorities in 2003-2004 (OSC, 2004, p.9) to 12,015 (OSC, 2012, p.12) in 2011-2012. What this has meant is the capacity and capability to deploy and collect information that can be subsequently assessed and shared within the organisation and partners has diminished, and appears to be in steep decline.

RIPA 2000 can be viewed as an enabler for information and intelligence collection, with the exception of its *RIPA 2000 Section 15* restrictions on the use and disclosure of product arising from telephone and mail interception, covert product can be used in court proceedings used for other purposes or shared further (Home Office, 2010a, p44). Information flows from warranted mail and telephone interception are restricted under *RIPA 2000 Chapter I, Part 1*

[6] *Police and Criminal Evidence Act 1984* Section 1, *Misuse of Drugs Act 1971* section 23

[7] *Police and Criminal Evidence Act 1984* Section 18

[8] *Regulation of Investigatory Powers Act 2000* Part II under Section 26

[9] *Criminal Justice and Public Order Act 1994* Section 60.

[10] *Terrorism Act 2000* Schedule 7 and section 43(1)

[11] *Police and Criminal Evidence Act 1984* Section 63 (9ZA)

Section 15, and its use in legal proceedings prohibited (RIPA 2000, Section 17). Public authorities permitted to use such methods are also limited ((Home Office, 2010b, p6). In effect, the Section provides a substantial restriction on the use of this sort of information. Unauthorised disclosure under *RIPA 2000 Section 19(4)* attracts up to 5 years' imprisonment:

> *'6.4 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to carry out those duties. In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed.*
>
> *6.5 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed...'*

UK legal restrictions to the wider sharing of intercepted product are not mirrored by European or US law enforcement, and, ironically, intercepted product obtained by foreign law enforcement agencies outside of the UK is admissible in UK courts (*R v Aujla [1998] 2 Cr App R 16*, and *R v P (Telephone intercepts: Admissibility of Evidence) [2001] 2 WLR 463* and R v Herbert Austin and Ors [2009] EWCA Crim 1527). Former MPS Assistant Commissioner Andy Hayman, addressing the Home Affairs Select Committee on the evidential use of interception product, observed:

> *'I think I am moving, as I know ACPO is, to a conclusion that in a selected number of cases, not just for terrorism but also for serious crime, it would be useful. I think also it does make us look a little bit foolish that everywhere else in the world is using it to good effect.'*[12]

A Government commitment to tackling organised crime led to the 2005 establishment of a new crime fighting body, the *Serious Organised Crime Agency* (SOCA). The accompanying *Serious Organised Crime and Police Act 2005* (SOCPA 2005) introduced provisions permitting the *'gathering, storing, analysing and disseminating information'*(*SOCPA 2005 Section 3 (1)* for crime reduction purposes. A specific list of bodies with whom SOCA may share information is provided, although the legislation also permits discretionary wider sharing *(SOCPA 2005 Section 2 (2) (d))*. There are specific powers in relation to use and disclosure of information, in that any collected as part of the exercise of any of its functions can be further used for any

[12] Home Affairs Committee, *Terrorism Detention Powers*, 28 February 2006, HC 910-iii, available at: http://pubs1.tso.parliament.uk/pa/cm200506/cmselect/cmhaff/uc910-iii/uc91002.htm

other activity in its remit (*SOCPA 2005 Section 32*). Furthermore, other provisions allow for SOCA to disclose information for permitted purposes *(SOCPA 2005 Section 33 (1) (2) (a –f),* vice versa to SOCA *(SOCPA 2005 Section 34).* This two way disclosure does not authorise exemptions under *RIPA 2000* Part 1, or the provisions under the *Data Protection Act 1998.*

SOCPA 2005 introduces a general duty to share between law enforcement and SOCA (*SOCPA 2005 Section 36*), although no such explicit power exists requiring police to share with other police forces, so top down and bottom up information flows may be unequal. The onward disclosure of information provided by SOCA by a recipient body is not permitted (*SOCPA 2005 Section 35*) without consent. This measure is partly needed for the continuing protection of sources, sensitive methodologies and duties of confidentiality, but it does impact on the level, volume and agility of subsequent information sharing. Under the provisions of the *Crime and Security Bill*, these powers are broadly re-assigned to SOCA's successor, the National Crime Agency which will go operational in late 2013.

Multi-agency working has also been a driver for legislative provision. Social services, probation and law enforcement increasingly work together, often co-located in *Child Protection Teams* (CPT), *Youth Offender Teams* (YOTS) and *Integrated Offender Management Units* (IOMU). Applicable legislation can either be agency specific or provide general sharing powers. The Social Services have a duty to investigate concerns over the welfare of a child as part of ongoing child protection inquiry, and the *Children Act 1989* gives implied powers to obtain information from other agencies to assess what action needs to be taken to offer appropriate protection. The positive obligation to protect life under *Article 2* of the ECHR is even more pressing when dealing with vulnerable persons such as children. Other child protection legislation implies information sharing powers including the *Children Act 2004 section 10, and section 11.* Interestingly, as a consequence of the Coalition agreement (2010:6) the children's database 'ContactPoint' was closed down in August 2010 as part of *'a full programme of measures to reverse the substantial erosion of civil liberties under the Labour government and roll back state intrusion'(Conservatives, 2010).* This, in effect, repealed the authority to establish the database under *Children Act 2004 Information database (England) Regulations 2007 SI 2007/2182.* ContactPoint, established in response of the failure to share information and intervene in the case of Victoria Climbie, had been accessible to 150 local authorities and at least 330,000 users (Ward, 2007, http://bit.ly/VyUaa6).

The *Crime and Disorder Act 1998* provides some power to share information, but not an obligation to do so. Its primary focus is to reduce offending, and requires partners, including probation, local authorities and police, to work together. The Act provides both implicit [13]and explicit[14] powers to share information in a host of operating areas, including planning to reduce crime and disorder, prevention of youth offending, and information on judicial disposals of child offending.

The information sharing between police and other agencies is not limited to criminal matters. Legislation permits the sharing of information between the public sector and private sector in relation to the planning for large scale emergencies such as floods, power loss and terrorist acts. The *Civil Contingencies Act 2004*[15] (CCA 2004) provides a legal basis to share information to carry out the *'duty to assess, plan and advise' (CCA 2004 Part I Section 2)* in matters of emergencies, provides power to disclose information*(CCA 2004 Part I Section 6)*, and makes provision for wider information sharing in urgent cases where a power does not currently exist *(CCA 2004 Part I Section 7).*

A key information sharing power associated with the management of dangerous offenders for public protection purposes falls out of the *Criminal Justice Act 2003 (CJA 2003)*. Sections 325-327 of the CJA 2003 place the sharing between agencies ('Responsible Authorities') on a statutory footing. This legislation permitted the sharing of information between the police, probation and prisons as part of Multi-agency Public Protection Arrangements (MAPPA) to assess risks, manage risks and monitor these arrangements with respect to sexual and violent offenders[viii].

The duty to cooperate in terms of information sharing by way of public interest and official inquiry is also found in Section 17 of the *Police Reform Act 2002,* placing a duty for police authorities and forces to supply information to the *Independent Police Complaints Investigation* (IPCC), examples of which are found in Chapter 5 of this thesis. The *Freedom of Information Act 2000* (FoI 2000) provides a duty, unless exemptions under section 30 are satisfied in relation to criminal investigations, to share information on request of the public. The *Criminal Appeals Act 1995* established the *Criminal Cases Review Commission,* which can

[13] *Crime and Disorder Act 1998* Sections 17, section 37 section 115.

[14] *Crime and Disorder Act 1998* section 115

[15] *Civil Contingencies Act 2004* http://www.legislation.gov.uk/ukpga/2004/36/data.pdf accessed 15th July 2012

order information from any public body, and the duty to comply *'is not affected by any obligation of secrecy or other limitation on disclosure'*[16]. Part IV of RIPA 2000 places a duty to cooperate with interception and surveillance commissioner during inspection and any Investigatory Tribunals. To maintain the security of sources and methodology, many of these duties to disclose are caveated with commitments not to further disclose the information to third parties.

The reoffending rates and continued criminal activities (Blakey, 2008) of remanded and sentenced prisoners warrants continuing law enforcement interest in prisons, as well as the active monitoring of the HM Prison Service. *Section 40D* of the *Prison Act 1952* (as amended by *Offender Management Act 2007*) places restrictions on the sharing of 'Restricted Documents' without authorisation in writing. The consequence of this section was to cause some confusion as to the role of the police Prison Intelligence Officer (PIO), often located with the Prison's security office. It has made some PIOs and their HMPS counterparts who are responsible for prison security units, more cautious about disseminating information concerning prisoners outside of the prison without explicit written authority.

Section 35 of *Prison Rules (*PR) provides the legal basis for the disclosure of information by the prison to law enforcement where it is necessary including in the interests of *'national security'* (PR 34 (3)(a), and the *'prevention, detection, investigation or prosecution of crime* (PR 34 (3)(b). In practice, this permits voluntary disclosure by the prison to law enforcement of prison material for use as intelligence and, with written authority, as evidence in court proceedings. An overarching national information sharing agreement exists to encourage greater two way flows of information, and many local information sharing agreements exist between forces and prisons located within these force areas.

Law enforcement information sharing doctrine and policy

The Bichard Inquiry, which examined the circumstances around the recruitment of Ian Huntley as a school caretaker in Soham and his subsequent conviction for the killing of two pupils, had a profound effect on policing and the management of information and intelligence. It proved to be a catalyst for a national implementation project[ix] of which information management was a core tenet. This is covered in the *ACPO Guidance on Management of Police Information,*

[16] Criminal Appeals Act 1995 http://www.legislation.gov.uk/ukpga/1995/35 accessed at 2nd august 2012

(ACPO, 2010), hereafter known as MoPI, a key document defining mutual police information management. Its introduction emphasised the important of the management of information in order that the police service can be effective in intelligence-led policing to protect the public, preventing crime and bringing offenders to justice. The document was geared towards strengthening the police service in terms of public protection, investigation and prosecution, and sought to maximise the benefits that would be brought by the Police National Database (PND), launched in 2011. The 2nd edition did not replace the statutory *Codes of Practice on the Management of Police Information* (2005) although it did replace a raft of other ACPO data-related documents, including the ACPO (2004) *Codes of Practice on Data Protection*, ACPO *Data Protection manual of guidance* (2006), the ACPO and HMCE (1999) *Code of practice on the Recording and Dissemination of Intelligence Material*, the ACPO and HMCE (1999) *Standards for the Recording and Dissemination of Intelligence Material* and the ACPO *Guidance On the Management of Police Information* (2006). MoPI went some way to codify the law enforcement library of process and procedure, but much remains to be done to enhance understanding and improve information flows.

Central to effective intelligence sharing is understanding what constitutes police information, defined by MoPI as information that is required for a policing purpose, which is *'protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice and any duty arising from statute or common law'*(ACPO 2010, p.171). ACPO hold that these five policing purposes provide the legal basis for police collection, recording, evaluation, sharing and retention of information. They do not, however, claim that MoPI's Code of Practice replaces or supersedes any legal power. Interestingly, the police position is that *'information can be collected for one policing purpose and used for another'* (ACPO, 2010, p.14). This may be at odds with other interpretations of the *Data Protection Act 1998*. This difference of interpretation may contribute to information sharing pathologies between law enforcement and other agencies, especially those operating outside of the criminal justice system.

The police interpretation is broad, in that information *'collected for one policing purpose may have a value to another; therefore, all police information should be treated as a corporate resource'* (ACPO, 2010, p.14). The MoPi guidance goes on to state *'Police information is a corporate resource for the whole police service; it should not matter where the information originated from and should be available to support all policing purposes across the country'*

(ACPO, 2010, p.15). Watson and Bessant (2009:174) differ, asserting that *'information should not be shared on the basis that it might be useful in the future'*. Watson and Bessant's approach could undermine efforts to collect and manage information to support predictive intelligence. Intelligence is not an exact science, and many believe that there is justification for holding information and sharing data whose worth is not immediately obvious in a specific operational sense, but clearly holds the potential of relevance. Investigations into terrorist acts, for example, often only emerge as they proceed from aspirations and an early preparatory stage to one where tangible efforts are made to implement a conspiracy. On these occasions, data (such as telecommunications) collected previously may be valuable, even though at the time this was not known or even suspected.

Decisions to not share, or reluctance and hesitation in sharing information, can rarely be justified in operational policing, as, once the policing purpose cornerstone of information sharing has been established, then criticism would be unlikely. However, officers still fail to share, even though the information they hold clearly should be passed on. Thematic reviews[x] of police intelligence units operating inside prison establishments in England and Wales during January and April 2012 identified regular failures to share information within the prisons' Security Unit. The reason for not sharing is usually the officers' lack of understanding as to when they could share, the reasons why they could justify the decision to share, and the inappropriate (sometimes simply wrong) intelligence handling management information (5x5x5) codes added to the original intelligence report, which, in essence, restricted onward dissemination to non-LEA agencies such as *HM Prison Service.* The Review identified the situation was exacerbated by inadequate supervisory arrangements, poor national strategic direction and support and insufficient training for intelligence officers operating in this specialist field.

MoPI distinguishes between types of police information, the most critical being *'public protection matters'* (ACPO, 2010, p.23). This information is primarily associated with those categories of offenders who fall within the *Multi-Agency Public Protection Arrangements* (MAPPA), but also includes related risk areas such as those arrested for murder or who are deemed Potentially Dangerous People.

MoPI acknowledges that police information may be recorded and held in separate systems, but stresses the importance that these systems should be linked to other records, echoing a number of the pathologies identified by Sheptycki, including *silo working* and *linkage blindness*. PND functionality now enables different major force systems to be accessed nationally. However other standalone or locally networked systems still remain to potentially ensure continued pathologies of *'silos'* or *'linkage blindness'*.

Many forces rely on *Information Sharing Agreements (*ISA), supported by MoPI, as their legal basis for the sharing of information to other agencies. ISAs are agreed between two or more parties. In policing terms, that typically means ACPO and another agency (ie *UK Border Agency, SOCA* and *HM Revenue and Customs*), or between a Force and a Regional area of a national agency. They are not, however, legally binding, nor are they required before information can be shared with another agency about a specific investigation. Compliance with the *DPA 1998* remains essential. What they do offer is clarity over the process of exchange, the rationale for the passing of the information, and mutual responsibilities in the management of that information.

How information is managed on a day to day basis should be underpinned by a Force Information Management Strategy (IMS), and the importance of this is highlighted by the delegation of responsibility to a Chief Officer to oversee it. In practice, this should identify what the information community is within the organisation, and how the information is managed. MoPI is very clear that an IMS should act as an enabler: *'It (the IMS) allows information to be exploited whenever it is needed within the force, and defines how barriers can be overcome',* but there is an explicit commitment to information sharing where necessary. The challenge is to determine why, as evidenced by the findings of many IPCC investigations, the reality is somewhat different. In essence, the IMS appears to operate as a police response to *DPA 1998* compliance, rather than a pro-active and creative enabler and exploiter of criminal intelligence.

The respective Force IMS dictates how each PIO deals with the requirements of MoPI. For effective information sharing to work, it is important that each prison identifies a single point of contact (SPOC) for prisons. The SPOC will be the conduit/gatekeeper for all requests, both to and from the police. However, as has been discussed earlier, not all prisons have a dedicated police officer. Wherever possible, all policing members should be proactively seeking opportunities to share information to further support the policing purposes. The most basic principle that underpins the exchange of intelligence and information is that police information is required for a policing purpose. The policing purposes are:

- Protecting life and property
- Preserving order
- Preventing commission of offences
- Bringing offenders to justice
- Any duty or responsibility arising from common or statute law.

There is no obligation to share police information with another party. The police service shares a common purpose for managing information, which means that forces can share information with one another without the use of MoU, Service Level Agreements and ISAs. Before sharing information outside the Police Service, it must first be determined whether a statutory purpose exists for that information sharing. Where the police are requested to share information with a partner, the agency receiving the information must identify the legal power that allows them to lawfully request and process such information.

Risk aversion and legislative anxiety

An overly cautious or inaccurate interpretation of legislation may lead to a failure to use the powers provided, and therefore undermine the collection or sharing of information. The Focus Group revealed that most of the participants would default to not sharing information if they were unsure of their powers. One intelligence officer stated:

> *'it's not always clear what information can be shared further; the information reports often have no provenance, even the unsanitised versions. As a consequence uninformed sharing may pose risks. It is better to err on the side of caution, and not share' (FG1).*

This aversion is not limited to policing, and is likely to be present in other public authorities, as identified by the Chief Surveillance Officer in the *Office of Surveillance Commissioners* (OSC), who, when commenting on the decline of covert authorisations, observed:

> *'**4.7.** The returns to me by non-law enforcement agencies show authorised directed surveillance on 6,455 occasions. This continues a downward trend (...) My inspections are revealing a continuing reluctance, by many local authorities, to authorise any covert surveillance. Many local authorities have been discouraged by adverse media comment (whether well-founded or not) and are unsure of the prospective impact of the Protection of Freedoms Act. In consequence, defensively, it seems likely that they are investigating fewer examples of possible unlawful behaviour (which may not be in the public interest) or are relying more on overt methods (which may be appropriate but may intrude on Article 8 rights) or are riskily resorting to covert activity which is not authorised and therefore not within the protection of RIPA. It will only become*

> *apparent which of these is happening by inspections over a number of years'.* (OSC, 2012, p.11)

This legislative anxiety also exists outside of the public sector, as one Force Director of Intelligence observed:

> *'We have the added problem of financial information: trying to secure it from businesses and the private sector is difficult. They are reluctant to share in case they are subsequently sued for breach of confidentiality, even if this means seeing the bad guy walk'.* (Interview 4)

The concern over 'getting it wrong' weighs heavily on Law Enforcement, both at a personal level and organisational level. One Director of Intelligence stated:

> *'In relation to risk management associated with the intelligence process, the default position adopted by the majority of the intelligence community is 'do not share if there is an identified risk'. They start with the belief that any sharing will lead to the 'worst-case scenario', specifically legal challenge or complaint. They do not consider the small likelihood of that risk actually happening'.* (Interview 1)

Concerns over the culture of risk aversion in policing have been around for some time, but the issue was first officially explored as part of an independent review of policing (Flanagan, 2009) originally commissioned by former Home Secretary Jacqui Smith. The findings culminated in the publication of the *National Decision Model* (ACPO, 2011). The principles contained within provide officers and police staff with a framework, in the context of MoPI 2010, which should give all greater confidence to share information further. Principle 1 states clearly that police (who are later described as *professional risk takers*) need to make decisions in difficult circumstances, and this will include decisions around sharing information in developing situations.

> *'Principle 1: The willingness to make decisions in conditions of uncertainty (ie take risks) is a core professional requirement of all members of the Police Service'.* (ACPO,2011, p.33)

The sharing of information is ultimately to protect the community from harm, preventing crime, identifying offenders and bringing offenders to justice. This aim should not be distracted by potential criticism, and should be progressed if it protects the public – this goal is laid out in Principle 2:

> *'Principle 2: Maintaining or achieving the safety and well-being of individuals and communities is the primary consideration in risk decision making'.* (ACPO, 2011, p.33)

The problem of risk aversion is still present in contemporary policing with some holding that it's the police approach to training that is a significant contributory factor:

> ***'Failures in training*** *– training was focused on procedures and legal use of police powers rather than on becoming an effective crime-fighter. The emphasis is on removing risk rather than proactive intervention.'* (HMIC, 2012, p.3)

The level of criminality being addressed may also determine the extent of the information sharing, and influence the risk appetite and aversion. One national senior law enforcement intelligence officer stated:

> *'Risk aversion in relation to information sharing is apparent at Local Basic Command Unit, let's say Level 1, but less so at Regional Level 2 and National level 3. With regard to non-ACPO Partners, while prepared to do so, many are still nervous about sharing outside of their agencies because of perceived legal consequences'.* (Interview 11)

A number of those interviewed stated that information sharing was rarely a problem when it related to immediate and real threat to life. However,

> *'The only information that appears to be shared without problems is that concerning 'Osmans' – no one dare sits on that. They share it because it makes it someone else's problem. I can see the visible relief on their faces when they hand it over to me and it's no longer their issue. It's risk aversion that motivates the sharing here'.* (Interview 4)

Even though information is required, the sharing can also be hindered as a consequence of its Government Protective Marking (GPM) (HMG, 2008). The GPM seeks to protect sensitive information held by Government, public authorities and other partners, including those in the private sector. A document assigned a protective marking is required to be handled and managed according to agreed procedure. Its access and dissemination is restricted, and the 'higher' a protective marking, the more there is an expectation of vetting. However, inappropriate use of a marking may result in it being shared further than necessary, or not shared at all. In the USA, concerns over inappropriately high classification and the consequences for information sharing led to the *US Congress Reducing Over-Classification Act 2010*. The 9/11 Commission (US Congress, 2004, p.412) had previously observed:

> *'(...) the security concerns need to be weighed up against the costs. Current security requirements nurture overclassification and excessive compartmentalisation of*

> *information sharing among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, legal, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long terms costs of over-classifying information, although these costs – even in literal financial terms – are substantial. There are no punishments for* ***not*** *sharing information. Agencies uphold a "need to know" culture of information protection rather than promoting a "need to share" culture of integration'*. (Section 13.3)

This is an area worthy of further research in the UK. Is the current GPM (see appendix A) too national security focused, and, as a consequence, inappropriately restrictive for volume and local level criminality? Do the protective markings and security arrangements around intelligence concerning the burglar '*Wayne from Dagenham*' need to be applied in the way they do an international terrorist?

Effective decision making relies heavily on access to relevant information, when and where it is needed by people involved in the decision making, and subsequent enforcement action. This will entail collection and sharing of information within a force, amongst forces and between different agencies. This is reinforced in its principles:

> *'Principle 9 Since good risk taking depends upon quality information, the Police Service will work with partner agencies to share relevant information about those who pose risk or those who are vulnerable to the risk of harm'.* (ACPO, 2011, p.35)

Legislative provision cannot take all the blame for information pathologies. The concern over risk appetite was captured in the *Independent Review of Policing:*

> *'Equally undoubted in my view is that, so far as the police service is concerned, while some of this has been placed as a requirement upon them, some of it has been 'self-created', usually as a perceived protection against some potential future review, inquiry or scrutiny. The risk of this approach is that there is created a culture of 'risk aversion' which can seriously dilute, or at worst remove, discretion or professional judgement. Distinction must thus be made between necessary and unnecessary bureaucracy and there must be greater discretion allowed for the exercise of professional judgement in making this distinction'.* (Flanagan, 2009, para. 1.4)

There is a general concern about risk aversity which may mean that, even where there is explicit enabling legislation, information still may not be shared. Even with an explicit 'duty to cooperate', problems still persist between different agencies. One commentator stated '*It seems to me that most personnel who work within a multi-agency framework understand the information must be shared, even if they don't always do it*' (Williams, 2010, p.154), and observed that enhanced training on researching data and intelligence may assist.

The negative culture identified above has developed partly due to disproportionate concerns over the harm associated with sharing data[xi]. Organisational standpoints on information sharing have fluctuated over the last decade, with the information sharing zenith achieved in the aftermath of the Bichard report (Bichard, 2004). However, recent years have seen increasing concerns over failures associated with information sharing, so much so that the *Law Commission* is about to take up the issue in its programme of work. (Law Commission, 2012b, p.12).

A more recent finding of failure to share information between agencies including the police is highlighted in the audit of information sharing between Accident and Emergency (A&E) departments (in England) and Community Safety Partnerships. The audit found that 1/5 of A&E did not share any information and it was only effectively shared in 1/3 of CSP areas. These significant information sharing failures meant that CSPs missed opportunities to inform violence reductions initiatives and consequently reduce assaults. (Centre for Public Innovation, 2013).

Why, within a few years post Bichard, has there been such a sustained decline in willingness to share? Institutional and legislative nervousness, hesitance in the face of criticism arising from data loss scandals, misconduct and criminal investigations associated with unlawful data access and persuasive civil libertarian views[xii], have no doubt all influenced attitudes. The trend poses a threat to effective policing and public protection. The integrity of police information relies on '*the information being trusted, acceptable, useable and accessible*'(ACPO, 2010, p.21), but it seems this is easily undermined.

Summary

There are over 130 statutory powers concerning the collection, use, protection and disclosure of information, many of which contain multiple sharing provisions dating back over 100 years (Bessant, 2009, pp.95-127). This plethora of legislative provision may be ready for review, amendment and codification, to aid understanding, decision making and information sharing. Law needs to realistically anticipate the weaknesses and operating environment of the structures/agencies which will implement it. Ambiguous wording may encourage personnel to err on the side of caution. The circumstances behind the original provision of a law need to be considered. Liberal construction of law, introducing implied or no obligation characteristics, dilutes its own impact.

Access to information for police officers and staff should be widening, training on knowledge management and legislation expanded. The inagile approach, whereby each item of information to be shared is assessed on a case by case basis, is now at odds in an age where information is required immediately to prevent direct harm. A vast volume of data needs to be located, accessed, analysed, evaluated and then appropriately disseminated, to inform effective operational responses often within collapsing time frames. Codified legislation is part of the answer, but intelligence and cultural change around information management is also required.

Chapter 4: Literature review – The development of police intelligence

Introduction

The emergence of various policing models, including *Intelligence-Led Policing* (John and Maguire, 2003; Radcliffe, 2008), *Community Policing* (Alderson, 1977; Alderson, 1979), *Problem Orientated Policing* (Goldstein, 1979; Goldstein, 1990), *Evidence-based Policing (*Sherman, 1998*)* and more recently, Metropolitan Police Commissioner Hogan-Howe's *Total Policing (*James, 2012*)* depend on the availability of information and intelligence to inform policing activity. Within the UK, all of these models are underpinned, to varying degrees, by elements within the *National Intelligence Model* (NIM)[xiii]. The NIM business process recognised the centrality of information to policing, and, as a consequence, sought to professionalise and standardise the functions of information and intelligence process within law enforcement.

This chapter details the organisational advancement of contemporary police intelligence processes, commencing with what is meant by 'intelligence'. It examines definitions of intelligence used, not only across only policing, but also with partner agencies. It adopts a developmental approach, exploring the reasons, the milestones and drivers for the increasingly importance of intelligence within policing. The relationship between intelligence and with key policing models, all of which rely on information collection and sharing, is explored. Finally, it will consider the influence of the NIM, and its impact.

Definitions of Intelligence

Interpreting information sharing pathologies requires an understanding of what actually constitutes 'information' and 'intelligence'. However, a universally agreed definition of intelligence is unavailable. To Laqueur (2005:8) *'all attempts to develop ambitious theories of intelligence have failed'*, and Richards (2010:3) observed *'a definitive concept of intelligence has proved somewhat elusive for many years'*. More recent developments in intelligence such as the growth of 'open source' have now *'blurred traditional distinctions between intelligence and information and the barrier between secret and non-secret'* (Andrew, Aldrich and Wark, 2009, p.2). Davies (2009:12) states that the need for a *'catch all definition (...) may be barking up the wrong [theoretical] tree'*, and that the focus should be understanding organisational cultures and the *'competing national ideas of intelligence'.* Hindering consensus is the absence of national and international common operating standards, varying and inconsistent descriptions of the roles and remits of intelligence personal, disparate judicial interpretation and contexts, differing operating organisational structures and contexts in which information is collected, evaluated and used, and the relational dynamics between collectors, analysts and decision makers. Nonetheless, having a workable definition is important in developing a theoretical approach to intelligence, essential in identifying the causes of intelligence failure and pivotal to finding solutions to recurring problems associated with intelligence, including sharing pathologies. A definition for intelligence will assist in increasing understanding of intelligence limitations, managing customer and public expectations of what intelligence can and cannot deliver, and assist with development of the professional intelligence operatives and its users.

Intelligence is defined in the Collins English Dictionary as *'military information about enemies, spies etc'* (page 803) and a Google dictionary search on *'intelligence definition'* offers 'th*e collection of information of military or political value'*. These are narrow definitions, revealing the military roots of intelligence, and its affiliation with matters of national security. Multiple meanings for intelligence are also applicable, including *'certain kinds of information, activities and organizations*' (Shulsky and Schmitt, 2002, p.1).

In the context of intelligence used by Governments, their agencies and law enforcement, definitions reflect local operating environments, organisation purpose, functionality and spans of responsibility. They can be dynamic, evolving to institutionalise and mirror new global socio-political and economic landscapes, threats and societal change.

The larger the organisation, the broader the concept that may apply, for instance *'the information - questions, insights, hypotheses, evidence - relevant to policy*' (Wilensky, 1967, p.ix). In a policing context, policy equates to decision making at both tactical and strategic operational levels. It has also been suggested that *'Intelligence deals with all the things which should be known in advance of initiating a course of action' (US* Commission on Organization of the Executive Branch of the Government, 1955, p.26). The latter definition features a number of components commonly found in more contemporary definitions, including the concept of actionability, predictiveness and recognition that <u>any</u> information may potentially be 'intelligence'.

Many definitions use the degree of restricted access to distinguish between intelligence and information.

> *'Intelligence is information, not always available in the public domain, relating to the strength, resources, capabilities and intentions of a foreign country that can affect our lives and the safety of our people'.* (Walters, 1978, p.621)

The definition belies the military and national security origins of intelligence, clearly includes a focus on a foreign threat, although it is wide enough to avoid limiting the 'intelligence' to information that is categorised as in some way 'secret'.

Another later definition places intelligence within the heart of Government and national security policymaking. It allows intelligence to include threats both domestically as well as foreign, and does not make the 'actionability' of the information to be a prerequisite for it to be defined as intelligence:

> *'Intelligence refers to information relevant to a government's formulation and implementation of a policy to further its national security interests and to deal with threats from actual or potential adversaries'.* (Shulsky and Schmitt, 2002, p.1)

Sims (1995:4) holds that *'Intelligence is best defined as information collected, organised, or analysed on behalf of actors of decision makers. Such information may include technical data, trends, rumours, pictures, or hardware.'* This definition recognises the systematic process that turns raw information into intelligence prior to it being disseminated to customers, without requirement of technological capacity and capability.

To Lowenthal (2009:1), *'information is anything that can be known, regardless of how its discovered. Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs'.* He describes intelligence as a sub-set of information, but he states that *'all intelligence is information; not all information is intelligence'* (Lowenthal, 2009, p.1).

Lowenthal's definition is useful in that it acknowledges that potentially all information may, depending on the context, become intelligence. A telephone book may be information, but if it contains the address of a wanted person then the telephone entry under that person's name may become intelligence. This does not mean, though, that the whole telephone book becomes intelligence.

A US perspective of an intelligence definition stresses the predictive component of intelligence, its contextual importance, and its strategic benefit of informing Government policy. *'Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us — the prelude to decision and action by US policymakers'* (Central Intelligence Agency, 1999, p.vii). No mention of secrecy is made, nor covertness of collection. It is, however, linked to informing decision making, and more importantly 'actionability'. Unlike the UK, the USA has ensured a legal basis for a definition of intelligence within the *Intelligence Reform and Terrorist Prevention Act* 2004:

> *'Sec 1012. Revised definition of national intelligence. Paragraph (5) of section 3 of the National Security Act of 1947 (50 U.S.C. 401a) is amended to read as follows:*
> *''(5) The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—*
> *''(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and*
> *''(B) that involves—*
> *''(i) threats to the United States, its people, property, or interests;*
> *''(ii) the development, proliferation, or use of weapons of mass destruction; or*
> *''(iii) any other matter bearing on United States national or homeland security.'*

The definition has evolved from its original 1947 version, showing the dynamic nature of intelligence. It now is no longer international, but also domestic and homeland security. In addition, it splits the national definition into *'national intelligence' and 'intelligence related to national security'*. In keeping with US commitments to creating an information sharing environment and establishing multi-agency intelligence fusion units, the definition includes national security agencies, intelligence agencies and also law enforcement.

Some consider collection methodology to be a key aspect of whether data is information or intelligence. Covert collection may come from CHIS undercover operatives, signal intelligence, foot or mobile surveillance or communication interception. Taplin (1989:475) introduces a link between collection and covert tactics when he maintains:

> *'intelligence consists of the collection, analysis, evaluation and dissemination of information for 'positive' intelligence and counter-intelligence and the conduct of Special Activities (Covert action)'.*

An Australian perspective holds that:

> *'Intelligence is covertly obtained information. While it make take a number of forms, the key characteristic of intelligence information is that it is obtained without the authority of the government or group who 'owns' the information'.* (Flood,P., 2004, p.5)

The most recent statements from Australian Secret Intelligence Service (ASIS) reaffirm the definition.

> *'Intelligence in our particular realm can be defined as secret information gleaned without the official sanction of the owners of that information'.* (Warner, 2012)

The UK Security Services' definition includes element of secrecy, but also acknowledges the multi-agency involvement in obtaining the relevant data. Collection, unlike the Australian perspective does not require 'covertness'. It also reflects opportunities that open source offers in producing and supplementing secret intelligence.

> *'Intelligence is information of all sorts gathered by a government or organisation to guide its decisions. It includes information that may be both public and private, obtained from many different public or secret sources. It could consist entirely .of information from either publicly available or secret sources, or be a combination of the two'.* (Security Service, 2012)

The 'secrecy component' in intelligence, especially in the context of national security, is the *'essential key for understanding what intelligence it and what it is not'*. (Shulsky, 1995, p.17) rejects a definition of intelligence without mention of secrecy, and Bruce and George (2008:8) hold that the key attribute of intelligence is *'the collection of secret information by secret means'*. Taplin (1989: 477) is unequivocal when he states *'if an activity does not involve secrecy, it is not intelligence. Thus, the overt collection of information is not a part of intelligence – even if the information being sought is classified or hidden'*. Shulsky (2002:172) hints at the covert nature of intelligence when he states 'F*undamentally, intelligence seeks access to information some other party is trying to deny'.*

The 'secrecy component' in many intelligence definitions may be a contributory factor in information pathologies including 9/11 (Sims, 2007, p.41). Not all agree that intelligence is made up simply of secret material. As one former Director of the US CIA said of non-governmental intelligence, *'a proper analysis of the intelligence available by these overt, normal and above board means would supply us with over 80 percent, I should estimate of the information, required for the guidance of our national policy'* (US Senate Committee, 1947). The Franks Committee report on decisions taken prior to the Falklands war also highlighted the importance of all source material (i.e. newspapers), not just traditional 'intelligence' being used in future assessments when it recommended the Government review *'arrangements for bringing to the Joint Intelligence Organisation's attention information other than intelligence reports'* (Franks, 1983, para.319). In essence, it was making reference to the lack of weight given to media articles in the Argentinean press:

> *'First, we are not sure that at all important times the assessments staff were fully aware of the weight of the Argentine press campaign in 1982. As a result it seems to us that they may have attached greater significance to the secret intelligence, which at that time was reassuring about the prospects of an early move to confrontation'.* (Franks, 1983, p.39)

Another definition which introduces the concept of business intelligence and the role of the private sector is:

> *'intelligence is best understood as the collection, analysis and dissemination of information by parties in conflict or competition. What turns the simple pursuit of information into the business of intelligence is its purpose: gaining competitive advantage over our adversaries'.* (Sims, 2007, p.39)

So whether something is 'intelligence' and not just 'information' depends on a number of sometimes contradictory variables; how it was collected, which agency holds it, its protective marking, the purpose of the collecting/holding organisation, the level at which the organisation/agency operates and the jurisprudence. Innes (2006:229) argues this is also the case in policing as well, stating *'all agencies across the policing and security sector make use of intelligence, although they define, understand, and use it in a variety of ways according to their organisational imperatives and concerns'.*

Generally, police intelligence may be viewed as a refined by-product of raw data or information, the result of a process that ultimately makes sense of collected information in the context of policing. *'Intelligence is about making sense of ambiguities or contradictions and recognising the relative importance of different elements'* (Grieve, 2004, p.35). Just because information has been collected by law enforcement, does not automatically imbue it with the characteristics of intelligence. There is an expectation that what happens to the received information determines its intelligence value. In this, *'intelligence is information designed for action'* (Storbeck, 1999, p.2; Grieve, 2004, p.25; and May, 1984, p.3). Block (2008:184) states that intelligence is *'information that enables law enforcement agencies to make decisions in order to successfully investigate crime',* linking its purpose to policing outcomes.

Intelligence and information are sometimes used inter-changeably. UK law enforcement has made a distinction between information and intelligence, although Innes and Sheptycki (2004:9) suggest *'that this unproblematic and dichotomized portrayal fails to capture the important interdependencies and overlapping connections that routinely exist between strategic and tactical forms of intelligence'.* Another valid perspective is that information is *'data which has been processed into a form which is meaningful to the recipient'* (Berry, Izat, Mawby, Walley and Wright, 1998, p.259).

One of the first attempts to define criminal intelligence was in the *Baumber Report,* which commented:

> *'Criminal intelligence can be said to be the end product of a process often complex, sometimes physical, and always intellectual, derived from information which has been collated, analysed and evaluated in order to prevent crime or secure the apprehension of offenders.'* (ACPO, 1975, para. 32)

Later definitions placed less emphasis on the actionability of the information, and more weight on the 'recording' of information, as being fundamental to the definition of intelligence.

> *'For working purposes we therefore define criminal intelligence records as containing inferential and speculative matters about criminals and crime that do not form part of the criminal record. It does not preclude the inclusion of some criminal record information such as summaries of convictions where it would be helpful, but we would expect this to be minimal and duplication to be avoided so far as practicable'.* (ACPO, 1978, para. 7)

This definition separated formal criminal previous convictions from its definition of criminal intelligence, a position which appears to dismiss the importance of motivation, predisposition and profile matches, all of which may be relevant to an investigation or analysis.

To some commentators, intelligence and information, though related, are at different ends of the same data continuum, with intelligence an outcome of an operation that processes raw information.

> *'Intelligence often refers to information that is significant or relevant to an impending event and that will be a contribution to the positive outcome of that specific event. It is paramount that one understands the monumental differences between information and intelligence. Information is nothing more than data that has yet to be screened and interpreted through professional analysis.' Once information has been analysed, then it becomes legitimate intelligence'.* (Taylor and Russell, 2012, p.186)

Senior UK police officers' attempts to distinguish between information and intelligence can be characterised by a belief that intelligence has to be *'developed through the analysis of items of information, usually from a number of different sources'* (Maguire and John, 1995, p.16). The analytical component is a mainstay of UK law enforcement definitions of intelligence, and its potential to future understanding. Innes and Sheptycki (2004:10) introduce an outcome element to their observation that intelligence is *'information that has been subjected to some form of analysis and evaluation with the intention of informing future acts of social control'.*

Grasping what each law enforcement understands by intelligence is important, as this will determine what is collected, recorded and subsequently made available for sharing. This is a challenge also at international level (Kleiven and Harfield, 2008). Maguire and John's (1995:16) research revealed that *'one force regarded sightings of known offenders as largely irrelevant and prone to fill the system up with 'dross'; another saw them as an important contribution to building up a fuller picture of the movements of target'* (Maguire and John, 1995, pp.17-18). The IPCC investigation into allegations against *Kirk Reid* (see Chapter 5) best illustrates the potential consequences of differing approaches, and the potential critical information loss arising out of non-recording.

Unlike intelligence definitions adopted by national security agencies across the world, there is more common ground between UK and US law enforcement. In the US, 'criminal intelligence' is defined as *'Information [that] is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity'* (US Department of Justice, 2003, p.27). Similarly, the most recent ACPO definition refers *'to all forms of information obtained, recorded or processed by the police, including personal information and intelligence'* (ACPO, 2006d, p.107). Intelligence is *'defined as information that has been subject to a defined evaluation and risk assessment process in order to assist with police decision making'* (ACPO, 2006d, p.108). Here, intelligence is distinguished from information, by having undergone a degree of assessment to support decision making. However, this distinction is not entirely clear cut, as information includes an element of assessment through its use of the term 'processed'.

There are a number of contradictory and confusing distinctions made around information and intelligence in UK law enforcement. For example, national guidance on neighbourhood policing states:

> *'A **neighbourhood profile** is a descriptive product and not an intelligence or analytical product. The neighbourhood profile brings together information about the area from a wide range of publicly available sources. The purpose of a neighbourhood profile is to record information about the neighbourhood and to assist the community engagement and collaborative problem solving process, it is not a Problem Profile'.* (ACPO, 2006a, p.9)

The description consciously separates this information product from 'intelligence' or the process of intelligence. Yet this is contrary to ACPO definitions which would place this product within the intelligence definition as a consequence of its collection process, its subsequent analysis and, evaluation for inclusion into the final knowledge product. A distinction appears to be made between criminal intelligence and community intelligence, the latter described as:

> *'Local information which, when assessed, provides intelligence on issues that affect neighbourhoods and informs both strategic and operational perspectives in the policing of local communities. Information may be direct or indirect and come from a diverse range of sources including the community and partner agencies'.* (ACPO, 2006c, p.14)

At a national level, the objective of intelligence is to support crime fighting: *'The primary purpose of intelligence is to ensure effective operations against serious organised crime with the aim of reducing the harm caused'.* (Home Office, 2005, p.19)

A more recent development of the definition is the concept of *'community intelligence'*, which has been defined (Innes and Roberts, 2006, p.3) thus:

> *'Community intelligence is information acquired either directly or indirectly from a community, that when analysed can be used to inform policing interventions. The information can come from variety of sources, but it will inform police about the views, needs and expectations of a community and the risks and threats posed to it or by it, either in terms of internal or external issues.'*

These commentators assert that community intelligence differs from *'criminal intelligence'* which is *'data on law breaking activities of particular actors'* and *'crime intelligence'* which is *'focused upon particular incidents or series of incidents'* (Innes and Roberts, 2006, p.3). They also introduce a fourth intelligence type, *'contextual intelligence'* which is *'data which provides insight into situational or contextual conditions which contribute to the make-up of a place or its people'* (Innes and Roberts, 2006, pp.3-4). There is some merit in differentiating between four types of law enforcement intelligence, as they reveal the complexity and range of intelligence, but in practice they are all interconnected, and it may prove difficult to collect against anyone separately. Taken together, they may offer a richer and strengthened picture of a particular policing problem, and this is endorsed in what is termed *'laminated intelligence methodologies'* (LIM) (Innes and Roberts, 2006, p.5), where the information is fused with other intelligence material.

The sharing of intelligence must embrace a commitment to the publication of an account based on the fullest provision of material possible without risking of operational compromise of methodology. This will entail judgements that balance the risk of too detailed information being provided against the danger of over-sanitation to the extent that it fails to spark any action with a sense of urgency and focus (IPCC, 2008c). Without sufficient details and a commitment to the widest possible sharing approach, it may be difficult to reduce uncertainty and rational decision-making in a fast moving situation.

For the purpose of this thesis, the adopted working definition, developed from Brown (Brown, 2007, p.340), is that intelligence is *'all information which is significant, or potentially significant, for a police activity, or potential action'*. In effect, this definition holds that, intelligence is simply information – it is the use to which it is subsequently put that determines its significance.

The development of police intelligence

Surprisingly, the concept of *'intelligence'* as a core professional policing competency is relatively recent. Whilst the collection of intelligence has always been practised, for many years it was associated with detectives and specialist police units rather than as core business of the *'rank and file'*. Its emergence has been incremental, event driven and controversial, but it is now an accepted part of policing. From its informal and ad hoc roots, intelligence, and its raw data sibling, information, has been systemised, organised and embedded into daily policing activity.

The collection of police intelligence has developed against a backdrop of a persistent societal stigma associated with intelligence and surveillance, and this has impacted on information sharing philosophy and practice. Why do the benefits of wider information sharing within police and between police and partners engage libertarian concerns? Why are efforts to enhance information sharing often characterised by the threats this will bring, the attacks on individual privacy rights and the fear of 'Big Brother'? Theoretic and social debate regularly link modern day perceptions of intelligence-based policing back to 18th and 19th century objections to policing and surveillance (Fijnaut and Marx, 1995; Norris and Armstrong 1999; Lyon, Wood Murakami, Norris, and Raab 2006), yet how relevant are these linkages when trying to tackle the challenges of the 21st century? It is a stigma that requires robust challenge, more balanced debate and a move away from auto-critical attack. Intelligence collection and its subsequent sharing is not automatically associated with a 'necessary evil' (Dintino and Martens, 1982, pp.1-3; Brodeur, 1995) within policing in democratic societies. It can be a force for good. Nonetheless, law enforcement agencies need to be proactive about this, as one ACPO Director of Intelligence commented:

> *'The police are currently unwilling to expose to the public the challenges faced in the collection and handling of intelligence and the operational dilemmas it brings. This feeds a critical perspective of intelligence and encourages a lack of public understanding as to what police are trying to achieve in deploying overt and covert collection techniques. The outcome is that intelligence is associated with 'Big Brother' rather than as a protector of communities and individuals'*. (Interview 10)

While contemporary national intelligence functions were not entirely new, they were usually temporary in nature, and supported a specific event or incident. One of the first 'intelligence' units was the Metropolitan Police Special Branch, established in 1883 and by the 1960's all forces had Special Branch capability. In the second World War, Criminal Intelligence Squads were established in London but these were poorly resourced (Gill and Phythian, 2006, p.42). The *Police Act 1964* provided for the creation of *Regional Crime Squads* (RCS) and, within a year, nine had been established (later reduced to six). They were established primarily to execute executive action, and not to become regional and integrated intelligence hubs. During the miner's strike in 1984-85, police set up a Central Intelligence Unit to analyse intelligence being collected from the scenes of various mining districts, but it was disbanded after the strike was settled (Joyce, 2006). In 1989, the *National Football Intelligence Unit* was established in response to high profile football hooligan incidents, but it acted as a repository for hooligan related intelligence and coordinating international deployments, rather than taking direct control of national policing assets.

One hundred and fifty years[xiv] after the establishment of the modern police service, the *Baumber Report* (ACPO, 1975) first endorsed, as national best practice, the establishment of a dedicated intelligence structure. This new legitimacy witnessed the introduction of Force Intelligence Bureaus (FIB), providing a force-wide overview of the disparate local police intelligence units. They were an attempt to overcome problems of intelligence collection/use that were a consequence of distinctly different local force intelligence practices.

Increasingly it was recognised that effective information and intelligence management had to be undertaken on a multi-agency cooperative basis. One of the first collaborative arrangements, as a consequence of the *Mountbatten Report* (1966), was within the area of prison intelligence. This inquiry examined the circumstances surrounding a series of high profile escapes from English prisons, including the escape of the convicted spy, George Blake, from HMP Wormwood Scrubs in 1966, the 'Great Train Robbers' Ronnie Biggs and Charles Wilson, and the escape of Frank Mitchell from an honour guard. The report made a number of recommendations around security and prisoner categorisation, and a system for moving high risk prisoners through a dispersal system around a small number of high security prisons was introduced. Another outcome was the establishment of a *Police Advisers' Section* (PAS)[xv], providing a high level police-prison liaison for the exchange of intelligence and information between the two agencies. The need for the continuing police –prison relationship around information sharing was reinforced further during the Learmont Inquiry (1995)

The requirement of a national intelligence reform was reinforced by the publication of the *Pearce Report* (ACPO, 1978), which stressed the need for forces to move towards a more collaborative effort in relation to collection and sharing[xvi]. The *Ratcliffe Report* (ACPO, 1986) sought to encourage the use of proactive dedicated intelligence officers known as '*Field Intelligence Officers*' (ACPO, 1986). However, the first truly national 'permanent' intelligence structure, born out of the *Dickens Report* (ACPO, 1990) was the *National Criminal Intelligence Service* (NCIS), formed in 1992. NCIS was subsequently consumed by the *Serious Organised Crime Agency* (SOCA) in 2005, which in turn will be absorbed by the *National Crime Agency* (NCA) in 2013.

The reports under *Baumber* (ACPO, 1975), *Pearce* (ACPO, 1978) *Ratcliffe* (ACPO, 1986) and *Dickens* (ACPO, 1990), while all commissioned independently of each other, provided the conditions for the development of the *National Intelligence Model* (NIM). They also strengthened the emergence of information-based policing models including Problem Orientated Policing (POP), and Intelligence-led Policing (ILP). Both policing models had dimensions that relied heavily on the collection and sharing of information and intelligence to inform and drive policing activity (Tilley, 2008; McPherson and Kirby, 2004). POP in particular emphasises the crucial role of analysed information in informing an appropriate community and police response to an identified problem. Properly evaluated information offers an opportunity to address problems on a more sustained basis, in contrast to repeated police reactivity to reported problem or crime.

In the 1980's, the management of intelligence was unsophisticated in a period that predated policing models[xvii] and relied heavily on quality information to inform operational activity. Policing was instinctive, rather than intelligence-led. Intelligence management was primarily paper-based, with criminal's details handwritten or typed onto A5 size 'collators cards'[xviii]. The collator's cards contained minimal information, often a duplication of information held elsewhere ie custody or stop and search records, and generally recorded without provenance. The information actually needed by the police was either not systematically collected, held in inaccessible files/documents, or within officers' own personally held knowledge. The *'need to know'* concept existed even then, but in practical terms it was more *'there's not much to know'*. Specialist intelligence at that time was something that was undertaken by 'New Scotland Yard' and more specifically, C11 (Laurie, 1970) which had its origins in the 1960s in the guise of C5(2). This effectively comprised a small unit employing a handful of personnel with an enhanced collator's card system.

Intelligence training was in reality, non-existent. The first stirring of the professionalisation of intelligence was with the introduction of the *'Systems for Investigation and Detection (SID)'* project in 1991. It was during the accompanying rolling 'road shows' across the Metropolitan Police Service (MPS) that many of its serving Police Officers would have been introduced first hand to the importance of structured intelligence, of prioritising resources to target those persons who committed most harm to the community, and the importance of securing intelligence that actually led to action.

As the information age dawned, and with it, the availability of accessible and affordable information management technologies, policing, like other sectors of society, began to recognise and embrace the opportunities for more effective information collection and management. The typical lone 'collator', working in a smoke-filled office in a station with their card-based intelligence records, was increasingly seen as inadequate to satisfy the demand for intelligence to inform contemporary policing.

Increasing volumes of information, a widening gap between police resources and policing demands, and Government (Audit Commission, 1993; Audit Commission, 1996a) support for effective management of intelligence, added further impetus to the professionalization of intelligence. The MPS, like most of its counterparts, started to recognise the need to professionalise the role of 'intelligence'. However, in practice, and relative to the size of the force, the MPS intelligence training 'programme' was under-resourced, ad hoc, and generally relied on the enthusiasm and a personal commitment of officers who delivered the training in addition to their key role.

The publication of *'Helping with Enquiries: Tackling Crime Effectively'* (Audit Commission, 1993) was a milestone in the development of ILP, ensuring the emergence of intelligence at the centre of policing activity and moving policing towards a model for intelligence. This publication espoused greater use of intelligence at a time when police were encouraged to provide best value by delivering service using established business principles.

> *'Their recommendations sought to achieve the greatest value for money from the police in the fight against crime and looked to move the police away from a reactive, crime focus to a proactive, offender focus. 'Helping with Enquiries' had three main arguments:*
>
> - *Existing policing roles and the levels of accountability lacked integration and efficiency;*
> - *The police were failing to make the best use of resources; and*
> - *Greater emphasis on tackling criminals would be more effective than focusing on crimes'.* (Ratcliffe, 2008a)

'Helping with Enquiries' (Audit Commission, 1993) included a raft of statistical data that appeared to support the case for proactive policing. The Audit Commission had expressed concern over the lack of ILP within the policing environment. It evidenced the cost effectiveness of intelligence as a means of identifying the main perpetrators of offences and the use of intelligence-led tactics to arrest and prosecute. A subsequent follow-up (Audit

Commission, HMIC and ACPO, 1996b, p27) highlighted obstacles to the police intelligence function, including failures by officers to share information, inadequate technology, and police officer/staff failure to understand the value of information.

After its involvement with the Audit Commission, Her Majesties' Inspectorate of Constabulary (HMIC) continued to examine forces' relationship with intelligence, and encouraged a move to a more professional model of intelligence. HMIC produced a thematic review of law enforcement agencies stating, *'The intelligence function must be at the hub of operational policing activities with commonality in procedures across the force'* (HMIC, 1997, p.1). Furthermore, it commented on structure and information flows:

> *'2.1 The ideal intelligence configuration has often been likened to a pyramid structure, extending from a broad based local policing tier through a force and inter-force level to upper echelons composed of national and international work. Indeed, the logical apex of this pyramid is not law enforcement agency territory at all, but is rather the work of national governments who co-operate on the basis of negotiated treaties. Governments, however, are kept informed by intelligence from various agencies within the UK this includes NCIS, ACPO and HMC&E in respect of crime matters. For this model to work effectively, intelligence has to flow freely on and between the levels and interchange smoothly between agencies'.* (HMIC, 1997, para.2.1)
>
> *'2.2 To facilitate this, police forces must have a structure which satisfies internal requirements and meets external demands. Forces are involved at two levels of the classic pyramid and form the foundation on which the structure rests. They are traditionally comprised of a collection of units usually referred to as local policing units of basis command units. These 'basic building blocks' operate in conjunction with a headquarters tier where specialist support functions and executive command are based. Large forces sometimes group these units into divisions or area'.* (HMIC, 1997, para.2.2)

The HMIC thematic review finding provides the first time that operational activity was officially discussed in the context of three tiers, an approach that subsequently informed the operating levels within NIM. Until this time, the development of intelligence structures was organic in character, with forces independently attempting to develop and deliver more effective intelligence processes. This is not to say that other aspects of NIM were not being practiced prior to NIM's 2000 launch. NIM, in a different guise, was evident in early versions in 1993 and 1994. The *Metropolitan Police Service* (MPS) was developing intelligence processes under the *'Systems for Detection'* (SID) Project from 1992 to 1999 (HMIC, 1996). The SID plan revealed processes not dissimilar to NIM, including Intelligence Units located within the Basic Command Unit (BCU) level (NIM level 1) dealing specifically with local crime, and at Force level (NIM level

2) the establishment of the *Service Intelligence Bureau,* a forerunner to the MPS Force Intelligence Bureau, the MIB). The MPS intelligence system initiatives received an unanticipated push as a consequence of the murder of Stephen Lawrence in 1993 (Grieve, 2008, p.21). The subsequent Inquiry acted as a driver for the collection of timely, actionable and community-based intelligence. Running parallel to these organisational intelligence developments was the pioneering work of Kent Constabulary, which introduced the *Kent Policing Model* (KPM) which some commentators (James, 2011, p.113; Tilley, 2003, p.313) regard as the direct forerunner of NIM.

As society, and by consequence, law enforcement, entered the new information age, how effectively the volume of data was managed became more pertinent to police forces. Additionally, the surge of reported and recorded crime, the increasing mobility, both geographically and socially, of the population, and increasingly sophisticated serious organized crime, added an impetus and sense of urgency to the management of police information and the need for an effective intelligence paradigm.

In 2000, the NIM was formally launched by NCIS after its collaboration development with ACPO forces. Strategic support for its use was delivered through the *National Policing Plan* (Home Office, 2003), which directed that a key milestone for police forces was *'the implementation of the National Intelligence Model'.* Implementation was measured against 11 thematic areas and 135 minimum standards, the process over seen by HMIC inspections. NIM's importance to the police service was enhanced further with ACPO support of NIM as agreed national policy, embedded into core policing through a code of practice introduced under the provisions of the *Police Reform Act 2002.*

The NIM is, in essence, the codification of a series of best practice documents, police and independent reviews of intelligence based strategies, and initiatives encouraged by police inquiries over the last two decades. These culminated in statutory codes that came into effect on 12th January 2005. The Introduction explains the purpose of the NIM model as:

> *'The National Intelligence Model is a business process. The intention behind it is to provide focus to operational policing and to achieve a disproportionately greater impact from the resources applied to any problem. It is dependent on a clear framework of analysis of information and intelligence allowing a problem solving approach to law enforcement and crime prevention techniques. The expected outcomes are improved community safety, reduced crime and the control of*

> *criminality and disorder leading to greater public reassurance and confidence'.* (ACPO, 2005c, p.6)

The NIM works at three operating levels, and, as a consequence, ensures its relevance to all Force, Regional and National law enforcement, national intelligence agencies and criminal justice partners. The three operating levels include *Level 1* with its focus on local crime and disorder impacting on Basic Command Unit (BCU), *Level 2* which operates at cross border, either more than one BCU or across a region and *Level 3* which is concerned with serious and organised crime operating on a national and international scale. These operating models meant that information sharing flows had to be both vertical and horizontal to service the needs of local, force, regional, national and international agencies.

The intelligence and information management failing identified in the circumstances leading up to Ian Huntley's 2002 murder of two children in Soham proved to be the catalyst for the biggest shake-up of police information management ever witnessed. The subsequent Bichard Inquiry (Bichard, 2004) recommended a clear code of practice[xix] on record creation, deletion and sharing be issued to all police forces. It also called for the introduction of a national IT system, financed by the Home Office, to share police intelligence.

Both the Government and Police recognised that a truly 'national intelligence' system could only be supported through an effective integrated infrastructure. The implementation fell to the National Police Improvement Agency (NPIA), who commenced the task by establishing the IMPACT programme. The interim IT solution was the *IMPACT Nominal Index (INI),* which allowed inquires to identify which police force held information related to an individual of interest. The system was delivered in 2005, and finally replaced in June 2011 by the *Police National Database* (PND).

As with the murder of Stephen Lawrence, the Soham murders provided added impetus for the professionalisation of intelligence within policing. To support this knowledge development, ACPO, NPIA and other bodies, published a raft of intelligence and information doctrine (*see endnote*[xx]) to support the police intelligence community. The golden thread running through all the documents was the NIM.

Nonetheless, the NIM was not consistently embraced through policing, with some specialist police units less committed:

> *'Special Branch is also affected by such issues as the general drive towards intelligence-led policing and the introduction of the ACPO-approved National Intelligence Model (NIM). In principle, this should be familiar territory to Special Branch but in some forces there is understandable discomfort over the requirement for the Branch to compete openly in Tasking and Co-ordinating Groups for resources to undertake sensitive activities'*. (HMIC, 2003, p.20)

This initial reluctance has somewhat dissipated as the flexibility and adaptability of NIM processes has been understood. Those Special Branch officers, previously hesitant, have also recognised that sharing with uniformed police colleagues can bring significant outcomes. In a HMIC review of Special Branch it reported *'greater efforts are now being made to brief front line police officers whose potential contribution to the intelligence picture arising from their position in the local community was often overlooked'.* (HMIC, 2003, p.16)

A characteristic of an effective and efficient information and intelligence management system is adherence to the NIM business model. Increasing numbers of public authority organisations have implemented, to varying degrees, elements of the NIM, especially where information and intelligence is central to the functions and business. This has not been limited to police agencies, local authorities are also encouraged to use the NIM (Home Office, 2007, p.126). Ironically, the military from who so many origins of police intelligence processes can be traced, have also moved towards the NIM (HMIC, 2006). Reports into both *HM Revenue and Customs* (HMIC, 2007) and the *UK Border Agency* (UKBA) (Independent Chief Inspector of the UK Border Agency, 2010) recommended adoption of NIM processes in support of its proactive policing and information management. Most recently, Her Majesty's Crown Prosecution Inspectorate criticized the *Serious Fraud Office* (SFO) FO for not adopting the NIM processes at a more detailed operational level (HMICP, 2012, p.12, para 3.21). The convergence of different agencies intelligence processes, albeit slowly, is a trend over the last 15 years that is likely to continue with increasing multi-agency collaboration and national commitment to interagency interoperability.

This pull towards the NIM of other partner agencies has increased opportunities for enhanced law enforcement cooperation and information sharing. Adoption of the NIM has enhanced interoperability in terms of common language, terminology and processes, although it is by no means seamless and beyond criticism. A Director of Intelligence for a large ACPO force stated:

> *'The priority is to redefine and relaunch the NIM – it needs to be more like its original incarnation, the Kent Policing Model, which focused its attentions and resources at nicking offenders rather than the bureaucratic business model people have made it. We have become slaves to a process'.* (Interview 1)

Another indirectly expressed concerns over how NIM has been misinterpreted and shaped his force's approach to intelligence by commenting:

> *'The whole process of intelligence and information management in the organisation is too highly regulated. If a response is not catered for in a policy or doctrine then it's not progressed. It leads to robotic responses from the intelligence officers'.* (Interview 8)

Sims (1995:6) had previously held that an agency responsible for national intelligence *'in its most efficient form, handles only that portion of the intelligence process that requires the security and secrecy such a service affords'*. This assessment has now been overtaken by events, and subsequent organisational responses. Richards (2010:7) recognised the important nexus between the national security and law enforcement, the local and the national and the domestic and international:

> '(...) *developments in the field of terrorism mean that the police officer working with local communities domestically increasingly needs to have a connection with intelligence analysts looking at the strategic international picture, and both need – ideally – to be exchanging intelligence to ensure identification and penetration of the terrorist networks.'*

Compelled by national strategies (HMG 2010; HMG, 2011) and financial and operational imperatives, police Counter Terrorism Units (CTU) and the Security Service are continuing to forge stronger and closer relationships through co-terminosity, fusion units, joint funding and tactical secondments. This enhanced integration recognises the importance of structural, procedural and cultural changes in information sharing in order to prepare for and mitigate against terrorist attacks. (HMG, 2011)

Pressure was also brought to bear on UK CTUs and intelligence agencies, first as a consequence of 9/11, and subsequently the London 7/7 transport bombings and attempted London 21/7 transport bombings:

> *'On the evidence, the gathering of intelligence around the country and the liaison between the Security Service and the various police forces has changed beyond recognition and brought with it considerable benefits. There were brief submissions on*

> *the possibility of greater integration of databases and a closer system of information sharing, but very little evidence on this topic'.* (HM Coroners, 2011, p.26)

This UK integrated work on intelligence and operations, to a lesser degree, mirrors the US Government's *National Security Strategy*. It brings together both the intelligence and law enforcement agencies, and emphasises the need to operate both within the USA and internationally: '*(...) our intelligence and law enforcement agencies must co-operate effectively with foreign governments to anticipate events, respond to crises, and provide safety and security*'. (US National Security Strategy, 2010, p.11) The UK National Security Strategy is not, on the face of it, so accommodating, with the UK National Security Council bringing together '*key ministers, military and Intelligence Chiefs*' (HMG, 2010, p.5), but not law enforcement. This relationship reflects an approach encapsulated by '*concentric circles of trust*' (Omand, 2010, pp.300-302) which, in effect, consigns law enforcement to an unembraced, less co-operative and trusted central position in national security: the 'B' rather that the 'A team', perhaps? However not all adopt the same stance. The Security Service Director General Jonathon Evans said in his Mansion House speech (25/06/2012)

> *'At home that means closer cooperation with the police service, with whom the partnership that we have forged in the last 10 years is viewed with envy by most other countries and is uniquely close and fruitful'.*

Intelligence structures and organisation approaches that may have worked in the past no longer work against new threats, and accordingly need to be rethought. These threats resulted in the establishment of the *Joint Terrorism Analysis Centre* (JTAC) in 2003, SOCA in 2005, and its successor, the *National Crime Agency* (NCA*)*, and the *National Fraud Intelligence Bureau* (NFIB) in 2010. All rely on effective information sharing. These developments reinforce the point that the 'police intelligence community' term is now too narrow and excludes key partners and contributors. Operational activity against national and international threats could no longer be the sole responsibility of any one force or agency, especially in a counter-terrorism context. Intelligence developments now anticipate issues at local and global level. This brings additional challenges in tackling 'police' information sharing pathologies: technological interconnectivity, international information sharing cooperation, enabling legislation, common language, interoperability, joint inspection capability and capacity and oversight arrangements. A police-driven intelligence model and information sharing reform programme needs to co-opt agencies that sit outside of forces. The early position that police held a legitimate quasi-monopoly on criminal information no longer holds.

Police intelligence now not only incorporates the intelligence agencies, and the wider law enforcement community, but now other criminal justice agencies and public authorities. The authors of 'Intelligence assessments' in whatever form, need to be alert to the possibility that police information systems hold only part of the information picture. A valid and credible understanding of a community threat can only be achieved through an integrated approach at tackling offenders and the information exchange between law enforcement, public and private partners, a view first articulated in the *Morgan report* (Home Office, 1991). To that end, *Community Safety Partnerships* (CSPs) were established, ensuring statutory involvement of partners in an intelligence led business process. This included local authorities, police forces, primary care trusts, fire and rescue services, and the probation service. To reinforce the importance of partnership and intelligence, the Home Office published hallmarks of effective partnership (Home Office, 2006) practice, espousing the importance of all partners using intelligence-led business processes.

Nevertheless, commitments to greater information sharing, even when embedded in published Government strategies, do not guarantee that the sharing will happen in practice. Numerous references to greater information sharing commitments are made in HMG crime reduction strategies, but substantive action is often disappointing. One example was the Serious Organised Crime strategy 'Extending our reach' (HMG, 2009):

> *'The new strategy will draw together and clearly communicate the various ways in which we can create a more hostile environment for serious organised crime in prisons. It will improve co-ordination and intelligence sharing to ensure that the most dangerous serious organised crime inmates are managed and monitored effectively whilst in prison'.* (Home Office, 2009)

The strategic commitment was announced in 2009, but a Thematic Review of Prison Intelligence Officers[xxi] in 2012 revealed that by June 2012, not one Prison Intelligence Officer (PIO) in 27 inspected prisons was in receipt of a complete list of organised crime nominals held within their prisons. The consequence was that both HM Prison Service and the Police were unclear on who should be monitored, and who information should be shared with. The prisoners were, with few exceptions[xxii], free to continue with their criminal enterprises, maintain contact with other organised crime members, and establish new contacts.

Greater multi-agency integration and cooperation is still likely, as police intelligence processes develop. Global terrorism and transnational crime will drive closer international cooperation on intelligence and information sharing, but technological dysfunctionality will slow the process:

> *'True, EU officials are helping to engineer a legal and technical revolution in the sharing of law enforcement data. But the new databases and procedures that are agreed are mostly developed in isolation from one another. This has the potential to make the lives of ordinary investigators harder, not easier: they have to learn several separate sets of new operating procedures and data protection rules. Faced with such complexity, they will almost always prefer the security of the informal 'old boy' networks that often fail to share intelligence well or widely'.* (Brady, 2009, p.15)

Another factor affecting the quality of information sharing at an international level will be differences in legal systems and law enforcement organisation (Block, 2008), and European Intelligence database access standing operating procedures (Kleiven and Harfield, 2008, p.200).

The future direction for 'police intelligence' is likely to be strengthened regional intelligence structures, closer private-public sector[xxiii], enhanced intelligence, and information sharing cooperation based on greater direct connectivity, the wider use and accessibility of open source intelligence, and the establishment of greater information sharing between law enforcement and social media (NPIA, 2010) participants, including *'citizen reporters'* (Omand, 2010, p.293).

Summary

Since the establishment of the 'new police' (Emsley, 2008) in 1829, the use and management of police intelligence has continually evolved, albeit on a sporadic, unsystematic and disorganised way. From the 1970s there was a growing strategic level awareness that more ordered information systems and information sharing could support detection and investigation (ACPO,1975; ACPO, 1978). Traditional reactive policing methodology was increasingly discredited (Goldstein, 1979; Weisburd and Eck, 2004) during the 1980s and early 1990s, with the spiralling and apparently endless upward trajectory of crime. Its 'investigative' led policing approach was found wanting, and an emerging consensus accepted the need for a different approach to operational deployments. The demand for police resources appeared to be outstripping supply but effective management of police information could challenge this *'demand gap'* (Flood B, 2004, p.39). In addition, the increasing availability and opportunities relating to new data, data volumes and technology to support its capture, storage and retrieval, also demanded enhanced law enforcement management ability to maximise operational exploitation (Ericson and Haggerty, 1997).

The *'New Public Management'* ethos (Golding and Savage, 2008, p.737) introduced a requirement for continuous improvement and performance driven targets, and the Government increasingly viewed law enforcement working practices and organisation as ready for a change in culture to a more business-orientated model. In this climate, the *Audit Commission* report (Audit Commission, 1993) triggered a series of organisational reviews of police intelligence processes. This momentum benefited those policing models, including POP and ILP, which were dependent on the availability of relevant, quality and accurate information.

> *'Intelligence-led policing is a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective , decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders'*. (Radcliffe, 2008, p.89)

A consequence of NIM implementation and these policing models was that information, and in particular intelligence, moved from the periphery to the mainstream of policing, and the information handling processes were subject to radical reorganisation and increases in resourcing (Home Office, 2003, p.12). This restructuring and professionalization of intelligence may have had far reaching consequences. Kotter (1978:10) holds that, *'all organizations import, convert, and export a variety of types of information and matter/energy in order to survive. The survival is guaranteed by making appropriate decisions about resource utilization and maintaining equilibrium with the external environment.'*

How policing survived, or at least avoided greater direct Government intervention, was by enhancing its intelligence structure within a traditionally rational legal, bureaucratic authority. The transformation from the lone 'collator' to a large bureaucratic department within police organisations is consistent with Weber's (Weber, 1947) view of the benefits of bureaucracy, although this may seem somewhat at odds when viewed through the lens of 21st century policing. Its organisational structure and rules are established to maintain control over its workforce, and, as a consequence, its relationship with internal and external partners. Intelligence activity is now typically delivered from within separate departments outside of response and neighbourhood policing teams. These departments are often further divided into sub structures ie *Dedicated Source Units, Surveillance Teams*, and *Technical Support Units*. These bureaucratic structures follow nationally approved doctrine, developed in light of legislation and service interpretation. The published rules are highly regulated and subject to close oversight from judicial[xxiv] and internal inspection. Intelligence Units are very hierarchical, with ACPO Intelligence leads, Directors of intelligence, Senior Authorising officers, Controllers, Senior and High Analysts. Formal and informal networks connect the Intelligence Unit to other parts of the organisation, with operational, private and public sector partners ensuring flows of information and patterns of cooperation. In theory, at least.

The rational legal bureaucracy appears unable to learn from its repeated information failures. The rigid hierarchy of modern day intelligence units, constrained by legislative and sector regulation, seems to stifle innovation and creativity.

In its early years, the NIM has made considerable contribution to moving 'intelligence' from the margins of day to day policing, and successfully addressed the absence of a law enforcement intelligence culture (Friedman, Friedman, Chapman, and Baker, 1997). Its 'national implementation' in 2004 should have tackled the information sharing pathologies highlighted by Sheptycki. Ironically though, the NIM and its accompanying doctrine may have contributed to the pathologies, by over-regulating information sharing, creating overload by the collection and generation of high volumes of information, and the rather bureaucrätic nature of meetings and processes.

The extent of information overload, insufficient allocation of administrative resources and poor management can be seen in the review of HMRC's management of Human Intelligence Sources (HMIC, 2011, p.26).

> *'HUMINT awareness has been greatly enhanced across BC (Benefits and Credits Directorate), but there is still a good deal of ignorance about what it looks like, and what to do with it. A particular example of concern was brought to the attention of BC senior management by HMIC during the process of the inspection. This involved a substantial amount of unsifted material (approx 30,000 pieces) which had come to light as a result of an earlier awareness visit (or visits) from the National Humint Centre team (NHC).' (Credits Report)*

A consequence of the current austerity measures has been a fall in resources allocated to the function of intelligence. An under-resourced, inadequately trained and poorly managed workforce will hinder future developments. When information sharing is ineffective, the quality of information declines, and with it an organisation's confidence in its information to form the basis of its decision making. Uninformed decisions impact on the quality of operational service, and ultimately community confidence in policing.

ACPO strategic leads are now considering moving on, or at least refreshing, the NIM, and it is fair to say that this is timely, as no systematic review has taken place in nearly a decade. The NIM process is viewed by some as too bureaucratic (Berry, 2010) and inefficient. The Head of ACPO Crime Business Area observed *'In policing we use the National intelligence Model (NIM) but we have accepted that this may no longer be best practice in its current format'* (Murphy, 2012). Without a NIM review, intelligence will not be able to regain its position as central component of core policing.

Chapter 5: Literature review – Police information sharing failures

> *'All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know from what you do; that's what I called 'guessing what was at the other side of the hill.'* Duke of Wellington **1852**[xxv]

Introduction

It is the business of law enforcement to prevent, identify and detect crime, and where appropriate, bring offenders to justice. This is achieved via the collection, analysis, assessment and dissemination of information, but Sheptycki's findings (Sheptycki, 2004) a decade ago revealed a process undermined by information sharing pathologies. This thesis examines whether these pathologies still apply, why that may be, and what additional issues may now feature.

Independent inquiries and investigations into concerns about the role of law enforcement and its partners form the basis of this examination. Cross referencing against Sheptycki's pathologies, it will pay particular attention to how information management and sharing failure played a contributory factor in the eventual findings. The publications are supplemented with material gleaned from strategic and tactical intelligence practitioners, through interviews and focus groups.

The methodological weaknesses of such an approach have already been rehearsed in chapter two, but by way of summary, a full analysis of the facts behind each inquiry are limited by non or partial-publication due to matters of *sub-judice*, statutory restriction, redactions based on duty of care obligations for those involved, and protection of sensitive operational methodology, including human and technical sources. Other incidents associated with information sharing pathology may have gone unnoticed or unreported. Success rarely attracts further attention, notice or inquiry.

Independent Police Complaint Commission (IPCC) investigations and judicial inquiries contain useful recent evidence against which Sheptycki's research can be compared, to provide insight into current information sharing practices. Each report will be reviewed against his lexicon of information pathologies, classifying their presence, understanding their contributory role, and identifying new challenges.

Independent Police Complaint Commission investigations

The IPCC investigations into alleged failings in law enforcement offer a rich vein of material into current information sharing pathology. The thesis reviewed all published investigations since 2004. Information sharing often played no role in the initial concerns, but in some reports it became a central theme.

The IPCC has overall responsibility for the police complaints system. Since April 2006, it has taken on responsibility for similar, serious complaints against *HM Revenue and Customs* (HMRC) and the *Serious Organised Crime Agency* (SOCA) in England and Wales. The IPCC's jurisdiction was extended in 2008 to cover *UK Border Agency* (UKBA) staff exercising police-like powers.

Established under the *Police Reform Act 2002*, the IPCC became operational in April 1 2004. The IPCC is responsible for ensuring the public have confidence in the investigation of complaints against police and other law enforcement agencies. The IPCC investigate the most serious allegations of misconduct or criminal behaviour including death or serious injury, serious or organised corruption and racism. It uses varied modes of investigation including *'Independent investigations'* carried out by their own investigators with all the powers of a police officer, *'managed investigations'* carried out by Professional Standard Units (PSDs) but overseen by the IPCC and PSD *'Supervised'* where the IPCC provide the terms of reference for the investigation and *'local'* investigations where the investigation is undertaken by the PSD, but the complainant, if unsatisfied, can appeal to the IPCC.

A *Commissioner's report* is not an *IPCC Investigation report*. The purpose of a Commissioner's report is to share with the public the key findings and summary of the IPCC investigation, including the Commissioner's own decision making, the outcome of any legal processes that followed from the investigation, and the learning recommendations. The report belongs to the IPCC Commissioner who retains oversight of the investigation. The investigation report is provided to the family or complainant, the police force, individual officers, and with a Coroner ahead of any inquest. The investigation report and related evidence is also provided to the Crown Prosecution Service when the IPCC considers that serious consideration should be given to whether or not a person should be prosecuted for a criminal offence. Investigation reports are published only in exceptional circumstances because of data protection or other legal restrictions.

IPCC investigation into Fiona Pilkington's death (IPCC, 2009e; IPCC, 2009g)

This investigation looked at police *contact* from 2004 - 2007 between Leicester Constabulary and Fiona Pilkington, prior to her killing of her vulnerable adult daughter Francesca Hardwick and her suicide. The inquest linked the deaths to anxiety about her daughter's future and anti-social behaviour issues. The Inquest posed the question *'What, if any, other factors operated upon Fiona Pilkington on October 23rd 2007 to cause her to act as she did?'* The verdict was *'Information sharing between agencies was not sufficient'* (IPCC, 2009g).

A review of the investigation report found *non recording* (IPCC, 2009e, p.117; IPCC, 2009e, p.120) on the Leicestershire Constabulary's *Crime and Intelligence System* (CIS), detailing warning letters or antisocial behaviour contracts concerning youths associated with intimidation of the victims. Furthermore, *'No intelligence logs were created in relation to the Pilkington family or the youths being complained about during the time period being examined in this report'* (IPCC, 2009e, p.135). The CIS intelligence system was not routinely used to record incidents of reported anti social behaviour. Officers who were dealing with related issues failed to record actions and activities, as a consequence, *'losing the opportunity to gather and share vital information'* (IPCC, 2009e, p.121). The non recording and non reporting ensured police had no searchable record of this or any subsequent action. This led to further pathologies of *linkage blindness* and *intelligence gaps*. As the report stated, *'The difficulty in recording and researching of police systems for those persons issued with harassment warnlngs and the failure to implement the repeat victim procedure may also have lead to the failure in identifying a trend or pattern of behaviour towards Fiona Pilkington and her family'* (IPCC, 2009e, p.140).

There was lack of awareness of functional capability of the force CIS system with the IPCC report noting 'PC "ASB" stated there was no electronic system *'to record the issue of warning letters et,c however the force's "Anti Social Behaviour Incremental Approach Policy" clearly states this should be recorded on an intelligence log in CIS'*. (IPCC, 2009e, p.120)

Technical dysfunctionality and user problems posed additional problems. The Force had an application that could link incidents, but *'Due to the volume of data a 'Genie search' could potentially generate, it was not a tool easily utilised by call takers'* (IPCC, 2009e, p.138). This concern over the amount of information produced for enquiring officers recalls the pathology of *information overload*. Officers were aware of the systems capability, but did not use it, with some choosing to use other systems' search capability. However, by searching just on CIS, results would only have included crime and intelligence reports. 'Genie classic' would have also brought up incidents. This revealed evidence of *digital divide* and *linkage blindness,* poor functionality and inadequate technical training standards within the force.

Since the tragedy, police have established a *Joint Action Quality of Life Team,* and co-located members of the Hinckley and Bosworth Borough Council Community Safety within it. Information sharing has improved, but the IPCC noted the incompatibility of partners' separate ICT systems as being a *'hindrance'* (IPCC, 2009e, p.176).

IPCC investigation into Operation Minstead (IPCC, 2009f)

Operation Minstead was an investigation into a series of burglaries and rapes that took place between 1992 and 2009, predominantly in the London area. There were numerous offences linked by method or DNA. In May 1999, a burglary took place which was later discovered to be linked to the Operation Minstead series, although this was not identified at the time. It is alleged that if this burglary had been investigated efficiently and effectively, included timely recording of information, the person subsequently charged with the Operation Minstead crimes would have been arrested earlier. It is claimed that because the burglary in Bromley was not investigated effectively, numerous other people became victims of rape and burglary. The person arrested on 15 November 2009 and charged ten years after the burglary in Bromley was Delroy Easton Grant. The investigation heard that intelligence was not added to the force intelligence systems until after three weeks.

IPCC investigation into contact with Lancashire constabulary regarding the safety of Ms A on 7th September 2010 (IPCC, 2010a)

This report detailed the circumstances into a brutal attack on Ms A, a vulnerable woman, by her abusive ex-partner, who was intent on causing her harm. She sought assistance from Lancashire Constabulary, but *'a shocking catalogue of errors left her alone and scared'*. The Force failed to access its own information to identify the history of incidents associated with the victim and her partner, which clearly indicated escalating violence. It failed to collect the information that would have shown her calls should have been prioritised. At the time of the stabbing by her partner, he was already on bail for another attack on her, and had bail conditions to not contact either her or her children. The police had been informed on numerous occasions by the victim that she feared she would be hurt by her ex-partner. A number of IPCC recommendations were made in their investigation, and one specifically related to call handling processes as the Operator who had handled the victim's call prior to her assault had failed to conduct any intelligence checks on Lancashire Constabulary's force systems, *'to ensure timely transfer of information between different Lancashire Constabulary intelligence systems'* (IPCC, 2010a, p.7).

The investigation revealed that simply recording information is not enough. The information needs to be accessed, shared and understood in order to inform appropriate action. Also, there is a suggestion of non-recording of information about the victim's contact with police which influenced the Protection Unit's prioritisation of the incident. The IPCC investigation's finding may suggest that there was an issue of professional incompetence and a *sub-culture* within call handlers of not understanding the importance of intelligence, or their role as first line investigators.

IPCC investigation into the use of ANPR in Durham, Cleveland and North Yorkshire from 23 - 26 October 2009 (IPCC, 2010b)

This investigation concerned the use of Automatic Number Plate Recognition (ANPR) by a number of North East England police forces. It came to light after the conviction in March 2010 of Peter Chapman for the kidnap, rape and murder of Ashleigh Hall on 25 October 2009. On the 23 October 2009 Peter Chapman's vehicle was highlighted on the Police National Computer (PNC) as he was wanted for arson, breach of his sex offender registration and theft. He was stopped by a police patrol in the evening of 26 October 2009 and arrested for the outstanding offences, but it only subsequently came to light he had murdered Ms Hall.

His vehicle had been the subject of 16 ANPR hits across three forces during the period under investigation, and not all were acted on by police forces involved. The IPCC looked at the issue of procedures for responding to ANPR activations.

It was not possible to say whether the use of ANPR and PNC may have prevented the murder of Ashleigh Hall, but it made a number of observations about information management as it relates to the ANPR. It stated that, *'Optimum use of ANPR can only be made where the system is managed well and the databases uploaded on the BOF are accurate and up to date'* (IPCC, 2010b, p.32). It recognised that ANPR had its limitations, partly due to the huge number of reads of number plates and 'hits' of registration numbers generated against various databases[xxvi], which it would not be possible for forces to assess exhaustively within available resources.

In essence, the IPCC report recognised the problem of *information overload,* noting *'It is clear if too many databases are monitored by FCR staff then this leads to an overload of information and a greater possibility of vital information been missed. This in turn would make it impossible to action or respond to hits'* (IPCC, 2010b, p.28). The solution is to ensure that databases are prioritised, that filters are put in place to ensure priority 'hits' are forwarded to response officers , for example those with a marker in relation to a person being wanted for an offence, or a marker relating to the possible possession of a firearm or drugs by the driver or occupant. Criminality is also a constant, vehicles are moving around the road network on a 24/7 basis and, as a consequence, 'hits' are being generated continuously. The IPCC stated that ANPR notifications should be monitored on a 24/7 basis. In practice, the ANPR system is not monitored in this way by most forces – it is one of a number of software and system applications 'open' on a control room at any one time.

Even when the pathology is not non-recording, information sharing problems may still arise with the recorded entries. The IPCC report noted in paragraph 147 that *'quality and accuracy of the databases is of significance. The information should be accurate and be capable of action. If the information contained within the databases is constantly found to be inaccurate or no specific action is required in response to a hit, then this does not instil confidence in the ANPR system.'* This will include basic issues such as misspelling, inaccurate circulation entry, and irrelevant reports remaining instead of being cleansed (eg the person has since been arrested and is not longer wanted but the PNC has not been updated).

IPCC investigation into Suffolk Police's response to Mary Griffiths and her subsequent murder **(2011)** (IPCC, 2011a)

Ms Griffiths lived in Bull Rush Crescent, Bury St Edmunds with her three children. Just before 6pm on Tuesday 5 May 2009, she made a non-emergency phone call to Suffolk Police to report that a Mr McFarlane was harassing her. The call was graded as requiring a non-urgent response and at around 9.45pm Suffolk Police telephoned Ms Griffiths back. With her agreement, they arranged to visit her the next day. At around 2.45am the following morning, Mr McFarlane broke into Ms Griffiths' home and shot her with a bolt gun. Within a couple of minutes, different call takers had taken three separate calls from people at the scene. Each caller provided varying degrees of information.

The IPCC report examined the actions of Suffolk staff in its force communications centre and control room. It looked at how they recorded a call reporting harassment, graded the call, utilised existing intelligence, and how they considered the allocation of resources.

They found that as the victim's call was categorised as a Grade 3, the call handler and dispatcher were only required to carry out a search of the Crime Intelligence System (CIS) and not previous police logs. Therefore, the police contact with Mr McFarlane on 3 May 2009 would not have been highlighted when they were dealing with Ms Griffiths' call. This fact reveals a number of related pathologies; the first was *linkage blindness* where the horizontal systems between the different databases are inadequate or non-existent. Secondly, systems holding too much data led to policies that limited accessing other databases to avoid *information overload*. Thirdly, the *digital divide:* the CIS system held different, but related, information, instead of police incident log records.

Another aspect of this case identified by the IPCC report is the errors in sharing information from the control room supervisor to the firearms tactical advisor. The IPCC commented on *'errors in fast-moving scenarios.... especially when copious amounts of information is being received, the importance of accurate information being supplied to the tactical advisor is clearly very important. This includes being clear about when information provided is certain or based on assumptions'* (IPCC, 2011a, p.7). *Information overload*, a challenge even during 'slow time' assessment, is exacerbated when dealing with a dynamic, evolving situation consistent with an emergency call. Training in intelligence handling and assessment for initial recipients is crucial here, and, as can be seen in this case, this relates not only to intelligence officers, but other policing roles.

IPCC investigation into police contact with Joanne Butler (2006) (IPCC, 2010g)

This report examined the circumstances leading up to the murder of Joanne Butler by two males in January 2006. Police received four telephone calls around the time of the murder, two of the calls came from her address and two from other residents of the street, including one from a man who would subsequently be convicted of Joanne's murder. The IPCC investigation revealed that an '*incident log was created that showed a check by the police call handler produced no historical information*' (IPCC, 2010g, para.13). This contradicted the IPCC's finding that '*Despite there being 20 incidents in 2005 where the police had been involved with Joanne, much of which related to her mental health, the control room staff did not have quick access to this information. Therefore they could not assess the situation as comprehensively as they should have been able to*' (IPCC, 2010g, para.27). On four occasions, the public shared information with police, three via 999 emergency calls that an incident was unfolding at Joanne Butler's address, but Leicestershire police did not send resources to ascertain what was happening at the scene. Without linking the call to the 20 previous incidents, the call was downgraded from Level 1, the highest response level, to Level 4, the lowest response level, signifying the call had been resolved without deployment. The circumstances revealed *linkage blindness, information silos* and raised questions of competency as to how information held by the force relevant to determining priority of police response was not accessed and therefore not part of the decision-making process. *Technical dysfunctionality* was revealed, in that the systems holding the key information were unable to be accessed easily by control room staff (IPCC, 2010g, para.25). The full facts behind this investigation are not known as the staff member involved did not cooperate fully with the IPCC.

IPCC investigation into the fatal shooting of Mark Saunders on 6 May 2008 (IPCC, 2010h)
This investigation looked at the fatal shooting of Mark Saunders by police officers from the Metropolitan Police Service. Mark Saunders had fired shots out of the rear of his property towards the public and police officers, with a legally held shotgun. During the siege he brandished his shotgun in a threatening manner and, as a consequence, was shot dead by police officers.

While information sharing was not a major part of the IPCC investigation, it did report on the establishment of an intelligence cell in response to the siege. This was done to assist with the management and sharing of information, prior to it being passed on to the negotiators. It also included a process whether decisions about non-sharing with the negotiators are made to avoid subsequent compromise with the subject of the operation (IPCC, 2010h, para.425). Senior police held that there was good information exchange between firearms and the negotiating cell, although the negotiating team felt the information sharing between them, the intelligence cell, and the officers with Mrs Saunders and Mr Saunders' friend could have been improved (IPCC, 2010h, para.1454). Detective Chief Supt Kennedy states that there is no documented evidence of information coming into the negotiating cell from the intelligence function, or from those officers with Mrs Saunders and Mr Saunders' friend.

IPCC report into Summary Contact between Banaz Mahmod and the Metropolitan Police Service and West Midlands Police, September 2005 - January 2006 (IPCC, 2008a)

This inquiry relates to circumstances concerning a young woman who refused to return to her husband after an arranged marriage failed. After her separation, Ms Mahmod formed a new relationship, deemed 'unsuitable' and 'bringing shame on the family'. She was subsequently reported missing, and the MPS began a three-month, high-risk missing person inquiry, eventually finding her body in a suitcase buried in a garden in Handsworth, Birmingham. In 2007, Ms Mahmod's father, Mahmod Mahmod, her uncle, Ari Mahmod, and a distant relative, Mohammed Hama, were convicted of her murder and sentenced to life imprisonment.

Between September 2005 and January 2006, Ms Mahmod came into contact during five separate incidents with police officers and staff from the MPS and West Midlands Police. These contacts were investigated. One substantiated complaint was that a detective failed to take necessary steps to arrest the suspect and '*carry out intelligence checks on Ms Mahmod*' (IPCC, 2008a, p.5).

West Midlands Police (WMP) report (supervised by the IPCC) into the death of Jordan McGann (IPCC, 2005)

This report was heavily redacted so the full circumstances of events could not be fully assessed. Nonetheless, enough was published to highlight information sharing issues.

In August 2004, an 18 month old child, Jordan McGann, died of her injuries caused by Darren Bennett, the partner of her mother Sarah Collins. Bennett was convicted of murder and Collins received 18 months for neglect. Bennett had a long history of domestic violence and assaulting children in the context of previous relationships. He had been stopped by police in July 2004, but not circulated for assault, even though he was wanted, due to internal policies around PNC circulation. This *non-recording* of information on the PNC meant that he remained free. The PNC related policy in place was more to do with reducing re-bailing of offenders and the costs that this incurred, rather than ensuring early arrests of suspects.

The investigation explored a number of issues, including whether the police, considering the information held on Bennett, recognised and responded accordingly in terms of managing him as a known violent offender, and the effectiveness of information sharing between agencies. Inadequate recording of information, specifically the full detail and nature of Bennett's assault conviction (IPCC, 2005, P.20), led to him not being re-categorised and treated as a schedule 1 offender within Multi-Agency Public Protection Arrangements (MAPPA). This subsequently contributed to an inaccurate risk assessment and Bennett not being treated as 'high priority'. The report held that failures in the police investigation were individual failures rather than systematic failure around child protection in the WMP. This raised questions about the professional competence of its officers and staff. Information flows between agencies clearly had scope for improvement. The *Birmingham ACPC Serious Case Review* (October 2005) held under Part 8 of *Working Together* made two points: the *'Flagging on IT systems of persons posing a risk to children' (Recommendation 1)* and *'improved information sharing (with West Midlands Probation Service) on offenders released from prison on license to improve recalls to prison where appropriate' (Recommendation 16).*

IPCC investigation into the circumstances surrounding the death of Mr Sean Beard, whilst in police custody at Burton on Trent police station in 2005 (IPCC, 2007d)

This substantial report addressed one issue concerning information sharing. It noted that during an earlier contact with Mr Beard, police information should have been generated and recorded on the PNC that would have noted concerns about his mental health and vulnerability. This, in turn, may have influenced the approach of police on the night he died in custody. At the time, the force technology did not support the generation of any report. The IPCC described this as a *'lost opportunity for significant information'* (IPCC, 2007d, para. 9.12). The IPCC investigation recommended that Staffordshire Police force ensured that procedures are in place to ensure that PNC Phoenix reports are always generated, to include risks identified, when persons are detained in police custody under section 136 of the *Mental Health Act 1983* (NB a Phoenix report is a report used to update or create a record on an individual on the PNC). This IPCC report highlighted non-recording and inadequacies in technology.

IPCC report into the Stirland Murders Investigation (IPCC, 2008c)

The IPCC published its report into communication between Nottinghamshire and Lincolnshire Police prior to the murder of John and Joan Stirland in Lincolnshire in August 2004. This was an investigation into a violent organised crime gang that involved many sensitive policing techniques and, as a consequence, the full facts of the circumstances are not contained in the report. The caution may have been informed by previous incidents when the crime family involved infiltrated Nottingham Police force through the use of two serving officers who were subsequently jailed. The IPCC looked at what intelligence was available to both Nottinghamshire and Lincolnshire police forces in the time leading by to the murders, what intelligence was shared between the forces, and what (if any) impact this may have had, on the potential risk to the lives of Mr and Mrs Stirland.

The IPCC held that Nottinghamshire Police did not supply Lincolnshire Police with enough information concerning the threat against Mr and Mrs Stirland, or the number of reprisal attacks that had taken place. It concluded that there was a *'lack of intelligence exchange between the various covert operations in Nottinghamshire and between the two forces* (Humberside and Lincolnshire)' and that 'intrusive management should be engaged in all major enquiries - ensuring significant intelligence is appropriately actioned and disseminated' (IPCC, 2008c, p.5). The report goes on to state: *'It was evident that senior officers were not always aware of significant intelligence and incidents that may have influenced their strategic decisions. It is recommended that senior managers should put measures in place to ensure staff understand what information needs to be brought to their attention, enabling them to formulate and/or review strategy'* (IPCC, 2008c, p.5). Lincolnshire Force were also criticised with the IPCC stating that the force should examine '(... *their intelligence system - to ensure it is fit for purpose and compliant with the National Intelligence Model)'* (IPCC, 2008c, p.6).

The report identified a number of organisational weaknesses that resulted in senior officers involved in the operation and liaison with another force not being aware of all the intelligence. The IPCC recommended that all their staff should understand what information should be brought to their attention to allow them to make appropriate decisions in future. It is concluded that the lack of intelligence exchange and assessment between the various covert operations in Nottinghamshire contributed to a lack of understanding of the clear and determined threat emerging against John and Joan Stirland, which resulted in a false sense of security in relation to their safety. This was a clear organisational failing. Secrecy surrounding the operation was paramount, which may have been appropriate, but it inhibited those who had taken responsibility for the care of the Stirlands, when assessing the risks and necessary measures to counter the threats and attacks. The IPCC believed that such situation was avoidable and *'when considering covert investigations in the future they do not allow the need for secrecy and the goals set for the original investigation to prevent them from meaningful review as new situations develop'* (IPCC, 2008c, p.29). The lack of intelligence dissemination, along with an absence of intrusive management of the operation and information management, was judged to be an organisational failing by Nottinghamshire Police.

The identified information sharing pathologies here included *non recording, intelligence gaps, institutional friction* and deliberate *information silos* based on concerns over information compromise, *linkage blindness* on the part of Lincolnshire and Humberside police and *noise* as the provenance of disseminated information was not fully understood by the receiver.

Tania Moore murder 2005 (IPCC, 2006a)

In 2005 Mark Dyche was convicted on the murder of Tania Moore. After more than a year of terror she was shot dead by her former partner. Mr Justice Bean said *'the failure to bring anyone to justice for the robbery in 2003 and the failure to act on Tania's report of the many harassing text messages are matters of serious concern. The Moore family and the public are entitled to a full explanation of what went wrong and the lessons that can be learnt from this tragic case'* (IPCC, 2006a, p.2).

Prior to her murder she had alerted Derbyshire police of her concerns on at least six occasions. Investigative response was 'abysmal' and signed off as undetected, even though basic investigation could have caught the offender. A number of *'fundamental errors'* (IPCC, 2006a, p.4) were made, including matters relating to information and intelligence. Not all intelligence systems were properly interrogated. Information sharing, and subsequent intelligence development with Staffordshire Police was hindered, as they were not given details of the robbery of Tania Moore. Information shared to police by Crimestoppers was not given proper consideration, even though it implicated Dyche in the robbery. Finally, Derbyshire Police failed to contact its own and another force's Dedicated Source Unit (DSU) and pass on information with a view to developing intelligence. The investigation highlighted professional incompetence in the use of information and intelligence. Existing databases held information that may have supported the investigation. Intelligence collection opportunities were missed by the investigative team, such as not sharing an intelligence tasking requirement with DSUs. The *digital divide* meant that a force could not undertake a single search, so other forces' intelligence units and DSUs had to be engaged.

IPCC independent investigation into the Metropolitan Police Service's inquiry into allegations against Kirk Reid (IPCC, 2010f)

This IPCC investigation examined the Metropolitan Police's work on a series of sex attacks across London along the A24 corridor. Eventually, on 26th March 2009, Kirk Reid was sentenced to life for 27 sexual offences and two cases of possession of indecent images of children. The number of offences committed by Reid is estimated to be between 80-100, in a series committed between August 2001- 2008, although one of the charges related to a rape in 1995.

There were a number of missed opportunities and failures in information management. This included focus on one suspect due to intelligence reports linking him to the offences, even though the DNA ruled him out. An intelligence report was submitted that named Reid, after he was stopped by police because of suspicious behaviour towards a woman in the area of previous assaults in 2004. This provided his address and car details. The reporting officer requested the information was shared with Sapphire Unit, which was investigating the offences. One of the indecent assaults recorded by the officer later featured in the indictment against Reid. The following day, the police officer submitted a further report adding that Reid was acquitted of an indecent assault in 1996, and she gave brief details of the charge. A subsequent cold case review of the linked crimes discussed two suspects, neither of whom were Kirk Reid. DNA seized from earlier scenes of crimes was not shared with the national database, and one of the other suspects was again arrested in 2005, even though his DNA was not a match. Approximately 50 outstanding crime registry documents which related to rape and other sexual offences were simply administratively progressed without effective and intrusive supervision.

In October 2006, an analyst from the Sapphire Intelligence Unit identified the fact that, of the 11 suspects named in the various crime reports, only three - including Kirk Reid - did not have their DNA confirmed on the national database. A decision to secure the DNA from Kirk Reid and two other suspects was only made in January 2008. Reid's DNA was found to be linked to three offences,, and he was arrested and charged the following month.

The IPCC stated that the Reid case was *'a sustained failure to get a grip on what was plainly a long-standing pattern of offences committed within a single borough. That failure was at the level of supervisory officers within the borough'* (IPCC, 2010f, p.12).

The IPCC recognised that inadequate resources were allocated to the investigation and pressures to tackle performance related offences played a role in diverting attention away from the series. Investigating sexual assaults was never a priority on the borough. The investigation reveals *information overload* as a consequence of the crimes occurring over a decade. There was unjustifiable attention on a suspect whose DNA ruled him out, meaning that Reid did not attract the interest he should have. The dismissal of crime reports, some of which related to Reid, meant opportunities to link information with the investigation may have been lost. Poor analysis and *linkage blindness* was apparent, and this meant it was over three years before the full extent of the crime series was identified.

IPCC investigation into the Metropolitan Police Service's inquiry into allegations against John Worboys (IPCC, 2009c)

This review found a number of issues, principally poor compliance with the Standard Operating Procedures by front line officers and their supervisors, for the investigation of rape and serious sexual assaults, as well as more systemic issues such as the lack of intelligence methods to initially identify and link offences. The report led to the organisational learning recommendation, *'Intelligence checks in accordance with revised Standard Operating Procedures to assist the identification and linking of serial offences'* (IPCC, 2009c, p.5).

The review also highlighted the 'Lack of facility to cross-check systems to link similar offences' (IPCC, 2009c, p16). At the time, no early warning system to alert the organisation when similar crime patters were emerging existed, nor was there any specialist training to supervisors in relation to the management of linked series of incidents.

Early opportunities to identify a pattern of criminality were hampered not only by the MPS but also national *information silos* and *linkage blindness*. Worboys' pattern of offending covered multiple boroughs and areas outside London, and it was not until February 2008 that four allegations of rape were linked by method, by the MPS sex offences unit, the Central Sapphire team.

This case also highlighted the role of community. The failure to identify the linked crime and publicise the dangers meant that women who had been subject of the assaults and had not come forward. When the investigation came to light, many women came forward who had not previously reported the attacks, as they feared not being believed. This victim information sharing assisted with new evidence and investigative information. Patterns of behaviour may well have become apparent sooner, had police shared their intelligence with other agencies, law enforcement and the public. In appropriate cases where there is a high risk to the community, police should consider sharing information with local agencies, in order to promote public safety.

IPCC report into Dano Sonnex and the 2008 murders of two French students London (IPCC, 2009d)

In July 2008, Dano Sonnex and one other were charged with the murder of Laurent Bonomo and Gabriel Ferez, two French students who were found murdered in South London on 29 June 2008. The crime caused considerable national and international public concern. The review looked at the police response to Dano Sonnex' prison recall notification. At the heart of the issue was whether police should have taken Sonnex off the streets 16 days prior to the murder.

Prolific and priority offenders, including persons subject to MAPPA, rely on timely exchange of intelligence between police, probation and the prison service. Police are responsible for making the arrests of those persons who have been recalled to prison. Dano Sonnex had been released on licence from prison on 8 February 2008 but remanded back into custody in April 2008 on a charge of handling stolen goods. He was subsequently released on the 16th May 2008 on unconditional bail. On the 13th June, a recall notification was sent to police and Sonnex was circulated as wanted. On the 29th June police found two bodies of the French students. On the 29th June the first attempt to arrest Dano Sonnex was made during a visit to his home. He was eventually arrested on the 10th July 2008.

However, the information sharing pathologies started before these dates. An intelligence record on Sonnex, created in January 2008, was not updated to include the relevant MAPPA details. Accordingly, officers did not contact Operation Jigsaw team or probation when they came into contact with him during their routine duties. His behaviour and his activity was relevant in determining risk and threat to the public, so information was crucial to inform this process.

The IPCC report recommended that appropriate entries should be recorded on records of all MAPPA offenders directing the need to contact probation and local Operation Jigsaw teams (IPCC, 2009d, p.5).

The case provided evidence of *non-recording*, *non-sharing* and issues of *professional competency*. *'The failing was a result of confusion, poor communication and weak procedures, rather than any deliberate act or wilful neglect, for which one officer has been disciplined'* (IPCC, 2009d, p.6). The response to intelligence information was slow, apparently because of other competing priorities. Even when standing operating procedures and memorandums are in place, this is by no means a guarantee of compliance. The original notification was not marked as urgent by the Ministry of Justice, and in so doing so would have influenced the response times of police. The IPCC recognised that the police have failed to protect the victims, but also linked this with other failings of partner agencies. Effective information sharing relies on good intra-agency procedures using commonly agreed language.

IPCC investigation into the Metropolitan Police Service's response to the stabbing of Peter Woodhams (IPCC, 2007a)

The murder victim was previously subject to a stabbing on 21 January 2006 in East London. This was investigated and classified as grievous bodily harm with intent. No suspects were spoken to or arrested, and on 17th March 2006 the investigation was marked as 'complete'. On 21 August 2006 Peter Woodhams was fatally shot in the Custom House area of East London. The allegation was that if the stabbing had been properly investigated, the second fatal incident may not have happened.

The IPCC investigation also found that officers had failed to input on organisational crime recording systems details of suspects, investigative enquiries and decision making as required by policy. Requests for information from the local authority assessing a re-housing application were not met, as the police required any request to be placed formally in writing. This was not forthcoming. The report here is not detailed, so it is unclear why the request for information had to be in writing – legislative 'cover' for the officer may have been one of the reasons.

Information was not shared effectively enough to support the investigation, one example being that even though the victim of the stabbing had told police the assailants were mixed race or black, he was shown witness albums containing photographs of white people.

IPCC report into the Counter terrorist raids at 46 and 48 Lansdowne Road, Forest Gate (IPCC, 2007c)

In June 2006, counter terrorist officers raided two houses, 46 and 48 Lansdowne Road, Forest Gate, in London. During the raids one occupier was shot in the arm. The raids were undertaken as a consequence of intelligence being received that a bomb was located in one of the two premises, and this device could be exploded remotely.

The IPCC stated they were satisfied that the information laid down before a magistrate to secure the warrant was an accurate reflection of the intelligence in possession of police at the time. The issue in relation to intelligence was that police operations '*should plan for the failure of intelligence, including making better provision for innocent people who are likely to get caught up in an operation*' (IPCC, 2007c, p.6), and that the MPS '*should publically explain the process by which they evaluate and act on intelligence, respond to some public perceptions that it can be misused*' (IPCC, 2007c, p.7). The IPCC suggested that where information fails, efforts should be made to '*explain to the victims of failed intelligence, and to the wider public, the process by which they evaluate and develop the intelligence they receive, and why they felt it necessary to act on it*' (IPCC, 2007c, p.7). This is an interesting extension of the need to share information which will have to be undertaken carefully, if confidentiality is not to be breached.

IPCC independent investigation into incident at V6, Bradville, Milton Keynes on 23 August 2004

In August 2004 a Vauxhall Astra driven by Abdu-l-Muqtadir Mustaqim was stopped by police officers in Milton Keynes. The driver, Mr Mustaqim, was in convoy with another vehicle, driven by his brother, which pulled in at the bus stop just in front of the Astra. Following a verbal altercation between the Mustaqim brothers and the police, Abdu-l-Muqtadir Mustaqim was arrested, and later charged with a public order offence, and with being in illegal possession of a lock-knife. The information sharing issue here was that information added to the PNC was out of date, stating a tax disc had expired. This was wrong as the tax had been paid a few days previously. The officer had undertaken the stop based on a belief that the vehicle appeared unroadworthy. The information pathology was not so much the recording, but the lack of compliance with procedures to update records when new information comes to light.

IPCC investigation into Greater Manchester Police (GMP) contact with Clare Wood prior to her death (IPCC, 2010e)

On 6th February 2009, Clare Wood was found dead at her home by her ex-husband. It is believed she had been murdered on or around 2 February. The suspect, George Appleton, was subject to a manhunt which came to a conclusion after he was found hanged in Manchester.

An officer ('Officer F') had de-arrested Appleton in relation to an alleged breach of police bail conditions. That decision was correct, as a breach of police bail is not a criminal offence. Unless Appleton had committed another criminal offence - or the original offence was ready for charge - there were no grounds on which to arrest him. Officer F issued Appleton with a warning. However, *'the officer failed to update GMP intelligence systems with this information and recorded Claré's surname incorrectly in his pocket notebook entry'* (IPCC, 2010e, p.9).

In this case, the IPCC review found failings in the GMP intelligence systems and *non-recording* of intelligence. Information of relevance (alleged sexual assault and breach of bail) was not shared by police with the CPS. The timely file submission and up to date information would have influenced how the CPS approached charges and prosecution against George Appleton. Police had access to information that clearly showed he was a threat to women who were previously partners, but this information was not fully appreciated by officers involved. The IPCC stated that there was no failure that could have been held to have been a missed opportunity to prevent the murder.

IPCC investigation into Greater Manchester Police (GMP) contact with Clare Katie Boardman prior to her death (IPCC, 2009c)

Interestingly, this investigation was linked to the Clare Wood case by the IPCC as the same mistakes were present, and this death occurred within months of Clare Wood's death. Katie Boardman was murdered in 2008 by her former partner Brian Taylor, who subsequently received a life sentence. The investigation also found incidents which were categorised incorrectly, and therefore did not come to the attention of the Public Protection Investigation Unit (PPIU), or were *'dealt with in isolation'* (IPCC, 2009c, p.8). Information from scenes was not recorded. In particular, of the 11 incidents, only one officer completed a detailed risk assessment. There were also some technological failings with the GMP system which led the IPCC to recommend that *'GMP amends its systems to allow them to search, not only for those incidents closed with a domestic violence code, but also those opened with one'* (IPCC, 2009c, p.9). This recommendation would increase the likelihood that crime series incidents could be linked to provide a clearer picture of domestic violence and inform appropriate police responses.

Investigation into the death of Hayley Adamson CTMS 2008/007843 *(*IPCC, 2008b)

This IPCC investigation explored the circumstances on the death of Hayley Adamson. On 19th May 2008, she was struck by a marked police vehicle as she was crossing Denton Road in Newcastle-Upon-Tyne. The police vehicle was responding to an ANPR warning within the officer's vehicle. The target vehicle was a Renault Megane, which had passed his police vehicle in the opposite direction travelling up Denton Road. The registered keeper of the vehicle had owned the vehicle for about two months prior to the collision. However, the intelligence stored on the Northumbria VIS hotlist for the vehicle related to a previous user, and was consequently out of date. Criticism was made of the lack of regular review of the ANPR entry by police, which should recorded the change of ownership, and determined whether a police response was still appropriate. The IPCC recommended that Northumbria Police should look at the ANPR review process to maintain the quality and accuracy of the ANPR information. This investigation highlighted the challenges of managing significant volumes of data. Moreover, even when 'push' technology exists to automatically share information with the person best placed to respond, professional competency and appropriate resources are still required to manage the data.

IPCC report into how Greater Manchester Police (GMP) were first notified about the shooting of Jessie James (IPCC, 2007a)

Jessie Marvyn James, 15 years old, was fatally shot in Broadfield Park, Moss Side, Manchester, at approximately 1am on Saturday 9 September 2006. Nineteen minutes later, Witness A, who had been working with GMP on a gun crime operation called the mobile phone of an off-duty GMP officer, Officer A. During the telephone conversation Witness A reported witnessing a dispute in Broadfield Park. Witness A said that there had been flashes and a body had fallen. The report stated *'Officer A tried to ensure Witness A was safe, noted the content of the call* *and returned to bed'* (IPCC, 2007a, p.2). GMP received a 999 call at 2:38am in which the caller reported that a friend was dead. The first officer arrived on the scene at 2:44am. Officer A contacted Longsight CID at 8:30am in relation to the information received from Witness A when he was informed there had been a shooting. GMP told the media and community that the first call they received about the shooting was at 2:38am.

The criticism was that Officer A had received information about the shooting some 79 minutes before the first 999 call and had failed to record the information adequately, as a notebook record was effectively an *information silo*, unsearchable and unlinkable. The IPCC said 'the conclusion reached is that the officer failed to appropriately action the information given by Witness A.' Technological problems during the incident with the GMP computer system meant that approximately 700 other 999 calls received were not recorded.

The non-recording of the information in an accessible format, or it being verbally relayed, meant that the community or media were not informed or given incorrect information. This added to the tension within the area, and undermined trust between community, media and police.

IPCC investigation into police contact with Joanna Michael prior to her death (IPCC, 2010c)
On 5 August 2009, Joanna Michael was murdered in her own home by Cyron Williams, who was subsequently sentenced to life imprisonment. The IPCC report focused on the call handling prior to the murder, and highlighted the need to close *intelligence gaps* where the information was concerned. It also highlighted that the victim was not provided with assistance because of *'a fatal combination of technological and human errors'* (IPCC, 2010c, p.1). The technological errors in this case related to phone calls made by the public, and the victim being rerouted to another force. The Gwent Police call handler who spoke to the victim did not record and share vital information with South Wales Police (SWP), including the suspect's vehicle details and the nature of the assault. This failure to share the information meant that SWP downgraded the response. The IPCC stated that, even allowing for the lack of training on domestic abuse, it did not excuse the Call Handler's *'basic lack of competence in obtaining simple information and passing on the crucial elements of it to South Wales Police'* (IPCC, 2010c, p.7). The IPCC introduced what in effect was the concept of 'noise', in highlighting that the transfer of information from one force to another has the *'potential for information to be diluted* (IPCC, 2010c, p.9).

Independent Investigation into the responses made by North Wales Police to reports of domestic abuse by Karen McGraw (IPCC, 2010d).

This IPCC looked at the North Wales Police response to reports of domestic abuse made by Ms Karen McGraw between 5 April 2009 and 22 July 2009 prior to her murder on 23 July 2009, by her ex partner Trevor Ferguson. There had been 13 police logs concerning incidents reported by Karen McGraw about Ferguson.

The IPCC held that *'Aspects of the call handling procedure, risk assessment process and information sharing could have been more efficient. It is not possible to say whether a different police response would have led to a different outcome, given Karen's attachment to Ferguson and reluctance to accept assistance from the police and other agencies'* (IPCC, 2010d, p.5). The IPCC noted that the Association of Chief Police Officers 2005 Guidance on Assessing Risk in the context of domestic abuse cases stresses that *'risk assessment and management are processes that can only be effective if full information is obtained about the parties involved and identified risk factors'* (IPCC, 2010d, p.6). In this case, the North Wales Police RMS database had *'a wealth of information in respect of the risk status of domestic abuse victims; this information is not, at present, readily accessible to Force Communication Centre (FCC) staff.'* (IPCC, 2010d p.8). North Wales Police were criticised in relation to supervision and adequate recording of information and risk assessments. Officers needed to take proper notes and record full records. It noted that *'FCC processes need to be more sophisticated in order that all relevant risk information is captured and shared'* (IPCC, 2010d p.6).

IPCC report into the death of Michael Spencer following his release from Wiltshire Police (IPCC, 2009b).

Michael Spencer had been arrested for assault on his partner. He reported to the custody officer that he was taking anti-depressant medication, had previously taken an overdose and had suicidal thoughts. These were recorded on the custody record. He had also said he had thought about jumping in front of a lorry. This was not recorded by police on the custody record. His relative telephoned the custody officer to warn of Spencers' mentally unstable state, and to pass a message to contact him if he needed anything. This was passed on, but no record was made on the custody record. The fact he was obvious a risk was not shared with others by placing the custody record in a high risk folder. Spencer was subsequently charged and released wearing his slippers, with no money, no mobile phone and no arrangements were made for him to be collected. Shortly after this, while a pedestrian, he was involved in a collision with a large lorry.

This learning report identified technical difficulties officers and staff had with a force custody record ICT database known as TROVE Information Technology system. Its functionality was complex, with access to documents and navigation difficult for staff. The challenges this system brought to officers was even acknowledged by the Assistant Chief Constable. When custody officers were trained, this was lead by a different force who did not include TROVE. The IPCC review revealed that often the training on the ICT system was not sufficient on return to force. The TROVE system is likely to result in officers/staff having hard copies printed, and therefore, when any policy is updated, the hard copies will not reflect the updates, as in this case, so outgoing and oncoming custody staff and detention officers were not able to brief each other effectively.

Independent Investigation into Devon and Cornwall Constabulary's response to enquiries regarding the welfare of Sally Ann Heppell, prior to her body being found on 10 April 2006 (IPCC, 2006c)

This report revealed a number of issues that were associated with inaccurate recording of details including Sally Ann Heppell's name, which led to confusion, and undermined information sharing between police and the social services. This failure to identify her correctly was very significant. Incident logs detailed Ms Heppell's mental health issues, but no police contact was initially made with the Mental Health Team. Agencies needed a single point of contact to deal with urgent information requests in emergency situations. The lack of information sharing was in part a product of ineffective joined-up working, and an absence of commitment to partnership and effective local contact. There was evidence of misunderstanding and anxiety over the information sharing legislation.

> *'Police Staff F recorded this incident as a Request for Contact. His entry on the log described that Sally's father was trying to get in contact with his daughter due to her mother's death. The daughter's name was recorded as Sally Ann HAPPLE (sic) and Police Staff F omitted to mention that Sally also used the surname SHEARING. Police Staff F read the previous log (335 of 22/05/03) but did not tell Sally's father any information because he was unsure of the restrictions in place due to the Data Protection Act. He then referred the incident to a supervisor to make contact with Sally's father'* (IPCC, 2006c, para. 11.1.2).

IPCC investigation into Craig Sweeney and abduction of child A (IPCC, 2006b)

This case concerned the abduction by Craig Sweeney of a child (Child 'A') from her home in Cardiff. The details of the suspect's car were given to police. In the early hours of the following day, officers from another force became involved in a pursuit with a car, the occupants of whom were unknown to police. During the pursuit the car crashed and rolled, throwing Child 'A' out of the car. After being taken to hospital, it was discovered that the child had been seriously sexually assaulted.

The subsequent IPCC investigation looked at the circumstances around the police response and the use of existing intelligence and information on Sweeney held on the PNC, Violent and Sex Offenders Register (ViSOR) and local force intelligence and information systems.

The IPCC investigation revealed that police had misspelt the name of Sweeney when undertaking a search on the Gwent intelligence systems, so the search returned no results. Gwent police had also asked South Wales police to conduct intelligence checks on their behalf, as the requesting officer from Gwent could not access ViSOR and he believed, as a result of his 'no result' search, that Craig Sweeney was not on the Gwent Criminal Intelligence System (CIS).

In fact, there was a log that the Control Room Inspector had been informed that Craig Sweeney was not on Gwent Intelligence System at 00:07. However, an entry on the Gwent log at 23:35 showed a warning marker suggesting Sweeney 'may revert to violence' on CIS. A restricted log was not created, but information was gathered by different parties, and not collated in one central point.

Access to intelligence by Control Room staff was limited, even though they were often the first responders to an incident, and clearly needed to quickly gather and make an initial information assessment. Access to intelligence was often determined by whether there was a police officer in the control room, or the ability to contact another department such as the PNC or CIS bureaux or another officer with CIS access.

The IPCC held that

> *'Front-line officers who attend an incident or stop an individual, are entitled to expect all information that would assist them in performing their role. In 2006 it should be standard practice that contact with a Control Room should generate a one stop check*

> *of all information and intelligence. This is vital when officers are attending many potentially high risk incidents. It is recognised that the Force intends to pursue this goal through enhanced systems; however, consideration should also be given to placing more trust in Control Room staff and providing them with sufficient access to CIS'* (IPCC, 2006b, p.34).

There was a lack of knowledge by officers responsible for managing this critical incident of what information the various force systems held, or in the case of ViSOR, what it was. The Control staff had access to PNC, but also did not know of the existence of ViSOR, so the warning marker on it concerning Sweeney was not identified and consequently not acted upon. The IPCC subsequently recommended that South Wales Police should enhance control room access to Force intelligence systems.

Technical and data management issues also meant that information on Sweeney transferred between Forces had been delayed, its transfer onto Gwent systems stripped off much of the data, and it had not been cleansed of previous historical information. Additional data had been added to Sweeney's record by another regional force prior to the abduction. This information crucially contained Sweeney's vehicle details. The impact of this omission was that, had there been a ViSOR access that night, the vehicle would not have been identified during the standard search. South Wales Police Force Control Room staff did not have direct access to ViSOR, while Gwent Force Control Room did, but they were only requested to search their local intelligence systems for information.

The IPCC recommended police allowing partners to have access to ViSOR, for access to be widened for staff, that staff are given training to access the intelligence system directly on a 24/7 basis, to promote awareness of ViSOR, and its data content. The IPCC also recommended strategic commitment and contribution by requesting that HMIC undertake a thematic inspection of their respective forces in respect of the quality of ViSOR data recording.

Up to this point the Chapter has examined published IPCC investigation reports. The statutory remit of this body is to focus on law enforcement. Policing, though, is rarely undertaken entirely in isolation from the involvement of other public authorities and Government agencies. The following inquiries covered all issues to do with information collection, management and sharing.

Other Intelligence related Inquiries

Bichard Inquiry (2004)

The Bichard Inquiry (2004) into the Soham murders was perhaps the seminal Inquiry into information sharing and police intelligence management failures. As is increasingly the case in contemporary policing, the failures to share information, including *non-recording,* were not simply failures within and between police, but also between police and other agencies, in this case social services (Bichard, 2004, pp.84-85).

The report highlighted a number of failings consistent with Sheptycki's pathologies and made detailed recommendations. *Digital divides, information silos* and *linkage blindness* were to be addressed by a national IT system to support police intelligence, flagging up reports on offenders held in different forces (Bichard, 2004, p.132). *Non recording* and *noise* were to be tackled by new codes of practice, inspections and transfers of responsibility to other agencies (Bichard, 2004, p.134). Greater clarity over recording and information sharing was to be delivered through a Code of Practice (Bichard, 2004, p.138) requiring decisions about not sharing information with the police to be recorded by other agencies, and these decisions would be reviewed (Bichard, 2004, p.139). This would have the effect of reducing *institutional friction* between police and multi-agencies. Verification that information sharing checks have been undertaken should be a requirement. Legal loopholes and *legislative anxiety* should be addressed in support of wider information sharing relevant to vetting between law enforcement and criminal records bureaux (Bichard, 2004, p.147).

The report also highlighted *professional incompetence* and *technological dysfunctionality.* There was little or no formal training to support officers and staff in terms of the management of information, and the expectation was they would learn 'on the job'. Knowledge of available information data bases and their functionality seemed limited (Bichard, 2004, p.86). Officers, even those deemed intelligence officers, had a lack of understanding of even the most basic aspects of the intelligence process (Bichard, 2004, pp.81-83).

Management of MAPPA arrangements of Anthony Rice (HMI Probation, 2006)

Anthony Rice was released under a Life Licence after a rape committed in 1999. On his release he went on to commit a serious assault on a female, and murdered Naomi Bryant in 2005. The

HMIP review *'found a number of deficiencies, in the form of mistakes, misjudgements and miscommunications at various stages throughout the whole process of this case that amount to what we call a cumulative failure (...)'* (HMI Probation, 2006, p.2).

This case offers a good example of information being held by many agencies in different information silos that, if shared widely and used effectively, may have prevented his original release and led to a more rigorous and intrusive MAPPA monitoring arrangements. Even when good quality information was shared between London Probation and the Hampshire Probation concerning Anthony Rice, they did not then share this with the MAPPA team which included police (HMI Probation, 2006, p.60). There were a number of occasions when information could have been more widely shared between the police, probation, prison that may have informed the decisions concerning release and prisoner re-categorisation. A contributory factor in the information pathologies in this case was the absence of an ICT system[xxvii]. A planned ICT system referred to in the report would offer a *'vastly improved coordination of information (that) would prevent some of the problems we have identified in this review'* (HMI Probation, 2006).

Zahid Mubarek Inquiry (2006)

In March 2000, Zahid Mubarek was murdered in his cell in YOI Feltham in West London. He was killed by his cellmate Robert Stewart, who was subsequently convicted of his murder. Again, this Inquiry revealed intelligence and information sharing pathologies involving both law enforcement and HM Prison Service. *Technical dysfunctionality* meant there was no way of electronically transferring intelligence and information between prisons.

There was a failure to utilise technology to collect and hold intelligence as a national resource, even though it was recommended in a separate inquiry in 1995. As of July 2012, HMPS' national intelligence database initiative, *Project Mercury,* had still not rolled out nationally across the prison estate. Sheptycki's pathologies were very much apparent. Details about Robert Stewarts' propensity to harm himself or others found their way to prison files, his history was detailed in intelligence databases at a previous prison. However, information regarding Stewarts' role in violence at another prison and his threats towards a woman were not properly recorded, nor were details of racist graffiti in a cell occupied by Stewart. The police officer deployed in a prison where Stewart had been held prior to transfer should have passed information on to the security unit about Stewarts' involvement in a stabbing. Police information about Stewarts' racist behaviour was not acted upon by the prisons security unit at HMP Altcourse.

'7/7 London Bombings Inquiries

On 7th July 2005, four men blew themselves up on the London transport system, causing the deaths of 52 passengers, and wounding over 700. A second, unsuccessful, attempt to attack London transport, was attempted on 21st July 2005. Whether this could have been prevented by better use of intelligence and information sharing has been subject to Inquiries, media investigation and public debate. The circumstances have been reviewed in two reports (Intelligence and Security Committee, 2006; Intelligence and Security Committee, 2009) and also by the Coroner's Office (HM Coroner, 2011). However, it is not possible to make an accurate assessment of information sharing failures due to security restrictions on sensitive material. The circumstances reviewed also confirmed the blurring of the lines between the intelligence services and law enforcement's role in national security issues. The reports covered not only the role of the Security Service, but also West Yorkshire Police, and the Metropolitan Police Service, demonstrating the relevance of *intra and inter rivalries pathology*. Initially, the then Home Secretary, Charles Clarke, claimed the four bombers were 'cleanskins', a term used to describe a belief that they have never come to the notice of the Intelligence Services. A subsequent review of the circumstances leading up to the attack by the *Intelligence and Security Committee*'s (ISC)[xxviii] report does not use the term in its report, nor does it entirely support the accuracy of the description (Intelligence and Security Committee, 2009).

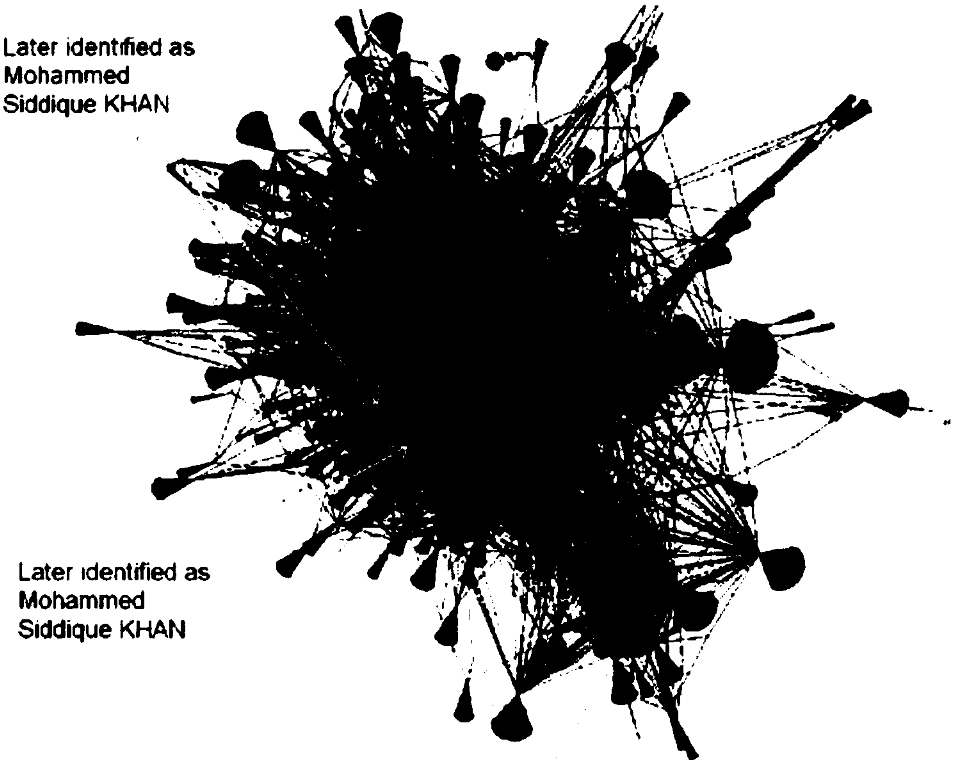
What can be surmised from the published reports were a number of failures in information sharing. Firstly, *information overload* to have hampered efforts to determine what, in the large amount of information collected, should be prioritised. The ISC acknowledged that this was a problem:

> *'The volume of intelligence received on terrorist activity can be overwhelming, and difficult decisions have to be made as to what priority to accord a particular piece of intelligence and whether that piece or another lead should be pursued in more depth'.* (Intelligence and Security Committee, 2006, p.21)

Associations were established between two of the 7/7 bombers (Mohammed Siddique Khan and Shazad Tanweer), and those subsequently imprisoned for the 2004 fertiliser bomb plot (Operation Crevice), in particular Shipon Ullah and Mohammed Shakil. This link was not prioritised with the focus of the investigation on Omar Kyham.

Why this link was not prioritised is self-evident. The Security Service did not have the resources, and this was just one of an association among thousands. The complexity and size of the task facing the Security Service was illustrated in the ISC report and the network chart below which demonstrated the link between Mohammed Siddique Khan and Operative CREVICE co-conspirators, a link which involved 'tens of thousands' of telephone calls:

Figure 1: Telephone contact network chart


Later identified as Mohammed Siddique KHAN
Later identified as Mohammed Siddique KHAN

In 2001, the Service was aware of 250 primary investigative targets, and by July 2005 this had risen to 800. Each of these targets had to the potential to develop into an intensive operation which would have had a knock on effect on other intelligence development activity. As the report stated, *'An intensive operation, for example into imminent attack planning, can* *consume almost half of the Security Service's operational and investigative resources'* (Intelligence and Security Committee, 2006, p.21)

The quality of product shared and the competency of the sharing process was subjected to criticism from the Coroner's Inquests (HM Coroners Inquiry, 2011) into the bombings. The photograph of Mohammed Siddique Khan and Shazad Tanweer was so poorly cropped that when shared with the US Authorities it was difficult to secure identification. Also, the ISC believed that the failure to share with photograph with a detainee missed an identification opportunity (Intelligence and Security Committee, 2009, p.87).

Implicit in the reports is that information relevant to the bomb attacks was held elsewhere, '*In making our judgements about whether anything was missed or overlooked, we have focused on the information available <u>at the time</u>*' (Intelligence and Security Committee, 2009, p.iii). The Head of MI5 explained to the Committee how they have continued to discover new information as their investigations have progressed: *'It is also very clear that we have come across a number of extra pieces of the jigsaw as we have continued to dig into our records, and as others have done as they dug into their records'* (Intelligence and Security Committee, 2009, p.54), adding also

> *'It has been a painstaking process – the story, at times, has not been clear and it has taken a great deal of work to uncover the chain of events described in this Review(...) However, as we have delved deeper, we have uncovered new information that even the organisations involved had not connected together* (Intelligence and Security Committee, 2009, p.100).

In light of these findings, it is reasonable to conclude that Sheptycki's *'digital divide', 'linkage blindness', intelligence overload',* and *information silos'* were the dominant information sharing pathologies at work, regrettably as well as that of *professional competence.*

Interviews and Focus Group (FG) observations

The IPCC reports and various inquiries provide evidence that Sheptycki's pathologies (Sheptycki, 2004) are still present and active, although the amount of influence each of these now have on information sharing has changed. The influence of some pathologies have waned, while others still appear to be key factors. These findings are also corroborated during the interviews and the Focus Groups.

The extent of the digital divide pathology is dependent on individual forces advances in data management technology. One *Director of Intelligence* of a large urban force stated:

> *'The problem with the digital divide is not as apparent as it once was in this force. We have undertaken regular purges on standalone intelligence databases including withdrawing organisational support for maintenance'* (Interview 4).

Directors of Intelligence from larger urban forces believed that the digital divide pathology was more prevalent in their force because of the sheer size of the force and the number of 'legacy systems' still in use. They also linked this ongoing problem to cultural differences and relationships between intelligence customers and the in-house police information technology departments:

> *'The digital divide is still an issue especially with the size of our organisation. It's important that intelligence have close relationships with their ICT departments but traditionally cops and 'techies' operate on different planets'* (Interview 4).

Although another stated that, while advances had been made, the problem still existed:

> *'We are still not as joined up as we should be although we now have a capability to search across crime and intelligence databases which previously required multiple and time consuming searches. We now have managed to achieve a force systems search using only two separate searches'* (Interview 7).

The improvements in addressing the digital divide are also based on the implementation of national intelligence systems and recognition that data mergers are a necessity:

> *'The digital divide is reducing to some extent and will do so more with the roll out of the PND and the convergence of BoF [Back Office Function] for the ANPR database. We're getting better and more sophisticated data mining technologies. There are virtuous forces in policing continually pressing for greater reliance on data'* (Interview 5).

The issue of linkage still appears to be an issue although it is more apparent when considered in the context of external partnership working.

> *'Linkage of crime series and offenders within this force still relies on personal networks and having a regional presence. We do not have functionality that offers automatic notification of new intelligence reports concerning current operational and investigative activity'* (Interview 7).

However some felt that this pathology, while it could be tackled through more effective national procurement processes and clearly defined user requirements, it would never be eliminated:

> 'The best cure for *linkage blindness* is hindsight, no amount of technology will get you past this. Technology, organisations and people are not infallible. Unfortunately there is an inevitability about future information and intelligence failures based on *linkage blindness*' (Interview 5).

Non recording appears to be a significant factor still. All the respondents raised this as an issue and connected it with a number of factors, unprofessionalism, resource limitations, legislative concerns and technological obstacles.

> *'The failure to record information is still a problem, but it is laziness on the part of officers and staff. However, there is an absence of meaningful measures to encourage and promote a culture of sharing which is still a problem'* (Interview 5).

> *'The non recording of information is down to laziness, clumsy technical systems and the lack of mobile data terminals for officers on the street. Most intelligence is still gleaned word of mouth on the streets, especially at level 1'* (Interview 4).

The issue of non-recording is not a pathology limited to law enforcement, and exists in other criminal justice agencies. One police officer working in the prisons made an observation, supported by five other members of the Focus Group, that:

> *'The amount of information I get from speaking to the officers and staff who work here, over and above what is actually recorded in the intelligence files and systems, is staggering. Most of the stuff about our targets is not written down or on the system'* (FG 9).

Some refer to the non-recording as a form of 'information hording', with the intelligence held in the officer's mind rather than in a standalone computer system or a protected format on a database:

> *'There is, frustratingly a cultural incentive to hoard information. It is difficult to quantify the extent of this, but there is substantial anecdotal evidence of action being taken with no or limited apparent recorded intelligence basis'* (Interview 4).

One Director of Intelligence made a distinction between the different policing cultures within a Force and the impact this has on non-recording:

> *'Non reporting and non recording is still a problem. The detectives are not doing it, and this sends the wrong message to the uniform. The (detective) will put information on the crime reporting system but will not cross reference this on the intelligence system. So it means both have to be searched to retrieve the information. This dual search requirement is not always done, so intelligence is lost' (*Interview 7).

Another respondent highlighted the disparity between information collected and recorded between police officers and Police Community Support Officers (PCSO's):

> *'If we are serious about intelligence then why do only 4.6% of our community deployed PCSO's contribute to the intelligence system?'* (Interview 9).

Information overload discussions brought contrasting responses from the Intelligence community. One felt that high volume collection was important:

> *'I'm of the school that says collect as much as you can. I'm not worried about intelligence overload. You never know when that car's number plate will come back to a murder. However, I will need better systems to store and weed the information than I have at the moment'* (Interview 6).

Meanwhile, others saw overload as a challenge to effective information management:

> *'Overload is one of our biggest problems, we appear to be seduced by the idea of collecting more and more information, just for the sake of it. It is slowing the intelligence process down'* (Interview 4).
>
> *'We have so much information that we potentially could get that 'full picture' but it is not ordered and arranged in a way that we can easily access it when we require it. We are a little bit overwhelmed by it especially when we are trying to make sense of something fast time'* (Interview 11).
>
> *'There are too many cops and not enough intelligence administrative support in Intelligence Units or in control rooms. That is where some of the resources should be directed, otherwise we end up with the most expensive typists in the country rather than specialist intelligence officers'* (Interview 4).

Institutional friction still appears to be a cause of information sharing pathology:

> *'Institutional friction was true then and is largely still true today. It may have been resolved through mergers, but force mergers are no longer supported by Government policy'* (Interview 4).
>
> *'There is a new intelligence IT system being introduced, linking the whole prison estate. I have not been put on the training list to allow me access even though I'm embedded*

> *in the intelligence security unit on a full time basis. The Governor said I'm not part of the prison service so he was not sure I should have the access to their material'* (FG 8).
>
> *'Even though I'm an accredited prison intelligence officer, the degree of access I have to intelligence databases in the three prisons I cover is determined on the individual whims of Security Governors. In some I have full access, in others I'm limited to scraps of intelligence. Those who cooperate with me get all of my information'* (Interview 10).

Intelligence Managers and users are generally more optimistic about partnership working and information sharing between agencies, but do express caution over believing this pathology is no longer a problem:

> *'Inter Agency cooperation is much better now compared to 10 years ago. National agencies, UKBA, SOCA, BTP, HMRC, HMPS all recognise the mutual benefits of information sharing. However there is still considerable room for improvement' (Interview 1).*
>
> *'Look, we have people from other agencies sitting in our intelligence office, directly accessing our systems. This was unthinkable 10 years ago. I'm not saying they have full access yet, but it's better than it was. It's not quite a level playing field though. I still have not got direct access to their systems yet'* (FG 12).

The importance of robust and visible leadership is clear in terms of challenging inter-departmental rivalry and its effect on information sharing. The following are comments from two Directors of Intelligence:

> *'We do not have a problem with sharing information between our in-house specialist intelligence desks, although that might be because I sit in the middle of them all and they know my views. Also if there is a problem it's dealt with, like a family squabble, then they get on with the business'* (Interview 7).
>
> *'Do people hoard information still? Yes. They are glory seekers. If there is an arrest to be done they want to do it. It's got a lot to do also with the performance culture. However, I'm in charge of the culture and I ensure there is no glory to be had by holding onto intelligence'* (Interview 4).

Even with new Law Enforcement Agencies being established, involving the merger of different agencies, tensions may still be a problem internally and externally:

> *'the big challenge for the National Crime Agency next year, is to test this institutional friction. It will have the tasking powers to do so. It will provide clarity to who is calling the shots in terms of organised crime strategy, who is in charge'* (Interview 4).
>
> *'The hardest bit about the new Police National Database is getting people and organisations to share. They use the well worn excuse of concerns over security of the source – and not very convincingly'* (Interview 4).

Some have acknowledged the 'reality' of corruption, and, with it, the need for measures to be in place to control access and restrict wider knowledge:

> *'The intelligence process is still overly bureaucratic. However, this is a consequence of securing a trade-off between corruption and information sharing. I do suspect the balance towards 'protection' in most cases, is a little overstated'* (Interview 12).

The issue of 'security' of information was raised by the majority of respondents, and, in particular, the issue of sanitisation of intelligence. Their views were captured by the following comments:

> *'There still remains a stubborn resistance to sharing intelligence more widely – it's a cultural thing about protection or so they say. What is clear is that when you look closely at the original information, with a bit more creativity and imagination with regard to sanitisation, it could have been more widely shared'* (Interview 12).
>
> *'Noise is still a problem although we are getting better at ensuring the provenance is recorded. Reports for onward dissemination are still oversanitised, which offers protection, but waters down the meaning and importance to a point where it fails to trigger action'* (Interview 1).
>
> *'Effective sanitisation is quite a skill, and our intelligence operatives do not appear to have mastered it, so the default position is play it safe and do not share'* (Interview 3).
>
> *'There is a problem with our collected product. How do we break it out to the users? We do not have the skills or the resources to sanitise effectively. It needs an experienced 'eye' which we do not have in great numbers in our intelligence department. We keep losing good intelligence officers on promotion or to other departments. As a consequence the intelligence does not go anywhere'* (Interview 7).
>
> *'Low grade intelligence is 'noise', absolutely, but so is over-sanitisation. This is a distinct problem and it's probably another type of failing to share in our and other police forces. The circumstances around the Stirland murders* (see Chapter 5 of this thesis) *is a case in point'* (Interview 4).

Professional competency and the quality of staff performing intelligence functions was another area commented on by the focus group and the interviewees:

> *'The organisation's Human Resource policy in the area of staffing intelligence departments has been incredibly short-sighted. They have a history of allowing intelligence departments to be staffed by disproportionately high number of restricted officers, selected not for their skills and competencies but because they are not fit to be*

deployed on operational duties. Key intelligence roles all along the process are held by the 'sick, the lame and the lazy'. I know it's a terrible term but its true' (Interview 6).

'Some of our staff responsible for the Police National Computer spend more time attending hospital appointments than they do at work' (Interview 9).

'Unless you're a restricted officer because of health issues you're not going to be able to secure an intelligence role. Also, other roles are now open only to civilians, a decision based purely on money and not on consideration of what a police officer can bring to the table in terms of experience and insight or a widening of the pool from which we could recruit' (Interview 7).

'One of the top challenges for police intelligence is getting the right calibre of officer and staff who possess an information sharing mindset and are prepared to challenge processes and systems' (Interview 2).

'Policing, especially in intelligence, is lacking high calibre intellectuals. However, how much talent can we afford? You look at our Intelligence Units and ask yourself: are they intelligent enough? Have we got the HR processes in place, a reward package attractive enough, a culture that supports it, and the ability to identify and recruit the 'right people' for our intelligence units? I do not believe so. Compare us with business and the intelligence agencies and we are amateurs at that sort of thing' (FG 11):

Efforts are needed to ensure that Intelligence staff are used in a way that takes advantage of their skills and experience:

*'I know I'm an intelligence officer, that's where my skills are, but intelligence is not my core business. I spend most of my time smoothing over tensions between my organisation and our partners, in addition to securing fast time management information for my boss prior to tasking meetings which are rarely used. I end up spending time typing and other administrative stuff rather than digging down and developing the intelligence collected' (*FG 12).

Many of the Focus Groups, and nearly all the interviewees, held a view that intelligence training was poor, of short duration, the trainers' experience drawn from too narrow a field and often not up to date. All of these factors impacted on delivery of intelligence services:

> *'My training for the role of intelligence officer was a five day course. My colleague has just attended a two week 'diversity at work' course. I'm not sure whether we take intelligence training seriously enough, and the expectation here is that I will pick up the skills while on the job'* (FG 3).
>
> *'All I have learnt is based on asking mates and colleagues who work in the same operating environment. They did the same. None of us know whether this is right or whether it once was best practice, but is the only option available'* (FG 9).
>
> *'Intelligence training is delivered almost exclusively by police, who, while often having experience in the art, are by no means the only actors in the field. Different perspectives on how intelligence can be collected, managed and used would also be worth hearing'* (FG 11).
>
> *'The private sector also has expertise and knowledge to bring to the table, but seems to be strangely absent. Open source intelligence is a classic example where policing could learn from and benefit from the private sector'* (Interview 10).

The absence of an intelligence career pathway in law enforcement and the perceived low value attached to intelligence work also was commented on as a reason for the high turnover and, on occasions, low skill level and limited experience of officers and staff working in intelligence.

> *'I would like to stay in intelligence, but I wish to get promoted. In my force promotion is based on evidencing neighbourhood policing not intelligence. In fact, intelligence is a death knell to career development'* (FG 7).
>
> *'There is a complete lack of understanding about intelligence. We need to demystify the whole area, we need to educate our staff, we need to retain good intelligence personnel, we need to impose sanctions on our staff for failing to record intelligence to change the culture, but balanced with the introduction of reward for good intelligence collection and coverage'* (Interview 9).
>
> *'Intelligence is not valued, it is seen as elitist, not proper policing. You're not going anywhere in the organisation if the CV does not have neighbourhood policing shown at each rank served'* (Interview 12).

Austerity was introduced in a number of interviews and Focus Group discussions, but not all suggested the cost cutting regimes to be a reason for non-sharing:

> *'The comprehensive spending review is producing better operational behaviour. It has acted as a health check for our systems including intelligence. Our systems are becoming leaner and decluttered'* (Interview 6).
>
> *'In the current climate, the cost of replacing our current systems, while needed, is simply too prohibitive. We should really build closer relationships with the private IT sector as the experts. What's the point of building an expensive system to hold information if it's already held elsewhere?'* (Interview 7).

> *'We have systems holding the information we want. We do not need new systems. We just need to be given access. This is not always forthcoming because either the user licenses are held with people who do not need access or the managers simply do not want to give us access. I don't know why, I suppose 'knowledge is power' sometimes'* (FG 11).

While many believe that law enforcement are good at collecting the required information, a significant minority of respondents (about 30 per cent) were not as convinced:

> *'Do we in policing seek to enter those dark corners of criminality such as cyber crime or do we continue to sit back and occupy areas where the intelligence just falls into our laps? I think we operate and fish in our comfort zones'* (Interview 1).
>
> *'I have serious doubts whether our intelligence collection is as comprehensive and detailed as it should be, whether we have identified and understood all the threats., whether we have received or shared the information as effectively and as widely as we should have done. As a consequence, I have doubts over the validity of our strategic assessments'* (Interview 3).
>
> *'Whenever I revisit an apparently full Subject Profile of a key organised crime member, I always find, without exception, more relevant information sitting in a non-traditional 'intelligence file' not collected or even considered. The consequences of this is that I may choose an inappropriate tactic, an unnecessarily expensive tactic or not fully understand a risk' (*FG 12).

Technology was also highlighted as an important tool in enhancing information collection and sharing, with most participants expressing concerns over how law enforcement is using this. Many expressed concern that new technology was not being exploited, in part as a result of an over-cautious law enforcement hierarchy who are often uninformed about its benefits:"

> *'The younger generation of officers and staff are much more information technology savvy, more so actually than information and intelligence managers and the intelligence and information strategist. They will access information via open source outside of existing rules. We need to ensure that they become discernible users of open source but equally the decision makers, the senior intelligence managers need to be prepared to handle and make use of open source intelligence'* (Interview 1).
>
> *'Open source information, collected from social media and Twitter opens up great opportunities, but already we are starting to see the over-cautious and unnecessarily complex regulation of access to this product. I think this has something to do with the fact that CT* (Counter-Terrorism) *are setting the agenda here. It's rather ironic that the 'run of the mill criminals' are using this and we are still struggling to comprehend its benefits and worth. Just who should be the technological leads here?'* (Interview 10).

This tendency for intelligence customers to undertake their own research, using other methods in response to a failure of the traditional intelligence generators to meet their needs, has been recognised by others:

> *'Networked consumers are increasingly exploiting alternative sources they find more useful and timely than intelligence products – or are simply 'good enough' – to meet their tight deadlines'.* (Gannon, 2008, p.216)

Connectivity also attracted comment, with all respondents raising concerns about the lack of similarity between systems, generating duplication of effort, added bureaucracy and incomplete search results. This leads to information sharing pathologies primarily around *non-recording, linkage blindness, duplication, defensive data collection* and *intelligence gaps.*

> *'Double keying into information systems is still a big problem, we have to input information across four different information systems none of which talk to each other, one arrest for burglary can require four systems to be updated with the arrested person's details – the duplication is both scandalous and ridiculous'* (Interview 6).

> *'We still have no interface between the force intelligence system and the HOLMES system* (This system is used by Major Incident Teams) *– entries onto the intelligence system have to be re-entered into the HOLMES system. The loss of intelligence concerning organised crime does not bear thinking about'* (Interview 3).

> *'Duplication of effort is still a problem. We have three specialist departments collecting information on gangs. This is in addition to local collection and murder investigation teams'* (Interview 11).

> *'My partners collect the same information as I do on the same subject and store it on their databases. A person of interest can have the same details added onto my force system, our regional intelligence system, the prison services system and the probation services system. If I looked further there would probably be more records held in local authority records, the Department of Work and Pensions, and any other place that had contact with him and his chaotic family. It's crazy, especially in this time of austerity that everyone is expensively dropping the same information into their systems'* (FG 2).

> *'Duplication is a waste of resources but our IT departments are not going fast enough to address this policing problem. Forces buy small as there is no incentive to collaborate, and as a consequence no ambition to joint up systems'* (Interview 4).

However, some blamed the duplication not on technical reasons (lack of connectivity, separate and siloed databases) but organisational cultures and functions:

> *'Intelligence collection against the same targets is increasingly a problem. With NCIS we had a workable system of operational flagging and deconfliction. With the establishment of SOCA we have gone backwards, and they are partly responsible. Too*

> *many different organisations and Forces were collecting against the same organised criminal and enterprise but not sharing the information. No wonder SOCA has fallen into disrepute and is being replaced after only 7 years'* (Interview 4).

The respondent also linked this organisation to another information pathology, *intelligence gaps*:

> *'The establishment of SOCA exacerbated the problem of intelligence gaps. The organisation deliberately distanced itself from policing. Its leaders chose to distance it from the NIM and in doing so created a Level 2 gap, then attempted to plug it by leaving police forces to fill in. It was a mistake to place so many people with spy backgrounds into a law enforcement agency. We need to make sure the same mistake is not repeated in the design build of its replacement body, the National Crime Agency'* (Interview 4).

Summary

The review of all published IPCC reports and relevant Government and Judicial inquiries since 2004, the one-to-one interviews with senior intelligence managers, Senior Authorising Officers (SAO) and intelligence practitioners in focus groups, has provided evidence of the continuance of Sheptycki's pathologies (Sheptycki, 2004), albeit with differing degrees of impact and regularity. The findings also highlight the emergence of three inter-related but new pathologies impacting on information sharing. These are those associated with legislative anxiety, professional competence and technology.

Chapter 6: Legislative anxiety, technical dysfunction and professional incompetence – 3 new pathologies, and how to avoid them

Introduction

Information oils the operational cogs that drive policing activity. Without it, the police cannot effectively protect the community. Information provides opportunities for pre-emptive action, disruption of criminals' intentions, support for investigations and the securing of successful judicial prosecutions. Availability of, and access to, information, fundamentally determines the value of police decision making, the appropriateness of tactical options, the allocation of resources and the prioritisation of a response to effectively confront threat.

Despite these self-evident benefits, law enforcement information sharing arrangements appear disappointingly inadequate. Although there has been new legislation, progress in data-management technology and a mainstreaming of information in policing strategy, this thesis reveals that Sheptycki's eleven pathologies still stubbornly remain. Moreover, this analysis of inquiries and investigations, practitioner interviews and focus groups, and reviews of academic literature, suggests that additional pathologies are now operating with such influence they can justifiably augment Sheptycki's original list.

The relationship between intelligence and core policing functions has evolved since the inception of the modern police force. However, its importance has been precipitated and expedited by the emergence of the information age, galvanising major organisational changes.

This expediential demand for overt, discrete and covert collection of information to support policing delivery has to be balanced against concerns over police legitimacy, accountability and transparency. The roots of contemporary policing are planted in a different time and society, so 18th and 19th century philosophical observations are not always helpful in the debate about intelligence. The ingrained deontological position adopted whenever collection and intelligence reform is aired within society often just hampers progress. Ironically, the positions taken by different constituencies, including politicians, has changed: the Liberal party has lobbied with ACPO in favour of new powers, while civil liberty pressure groups have continued to oppose them.

This caution can stigmatise law enforcement's attempts to access and utilise information. Community cooperation in providing information is described in pejorative terms – those assisting police are presented as 'nosey parkers or 'State agents', the conveying of information as 'grassing' or some sort of collective betrayal. The technical collection and storage is depicted as 'Big Brother' - a panoptical Orwellian nightmare.

If the purpose of intelligence was better understood, the latent public distaste outlined above could possibly be removed. Unilateral assumptions should be robustly challenged within a balanced debate that considers the ethical issues from differing perspectives. A legally authorised and justifiably deployed surveillance system should protect our freedoms, quality of life and civil society. Information can identify and rectify miscarriages of justice. It can ensure resources are allocated to areas that impact on 'hard to reach' and 'hard to hear' communities. It can ensure policing operations are more focused on the offender, thus reducing the impact of collateral intrusion on innocent parties. It can tackle police and state corruption (ACPO-NOMS, 2008) or malpractice, and prevent problems escalating before they undermine community confidence and well being. It is however acknowledges that retaining community support is crucial for intelligence collection. As ACPO have acknowledged:

> *'Public confidence underpins police legitimacy and has practical benefits. These include gaining intelligence about criminal activity within communities…'* (ACPO, 2013, p.2)

Contemporary society benefits from emerging, new and sophisticated technologies, methods of transportation and movement, and evolving attitudes and societal norms. The opposite is also true, as they also give offenders opportunities in the furtherance of crime, to extend the span of their control and influence, to move people and commodities across continents within hours, and to conceal the proceeds of crime. Intelligence is needed to tackle the contemporary, transnational criminal, and this relies on access to free flowing information. If properly shared, information creates opportunities for intervention, disruption, confiscation and arrests.

With these benefits apparent, it is troubling that information sharing failures feature routinely in judicial inquiries and IPCC investigations, as evidenced in earlier chapters. The causes for this vary, and specific information failures are rarely accounted for by way of single pathology.

A complex configuration of factors determines the extent of information sharing between the parties who need it.

Three new pathologies

This thesis holds that the dominant determinants frustrating progress in information sharing are associated with organisational intelligence culture, technological failings and misunderstanding/misinterpretation of legislation. These give rise to three new pathologies: *'legislative anxiety', 'technical dysfunctionality'* and *'professional incompetence'*. Other variables are relevant, but it is the synthesis of these three key pathologies that demand, at a national level, compelling remedial action. Without strategic commitment, the changes required will be difficult to implement, an opportunity to reverse an atrophying intelligence community will be missed, and with it, an opportunity to unlock the full potential of all source assessment in delivering policing.

Legislative anxiety is the first of three new information sharing pathologies to be added to Sheptycki's lexicon. It describes the reluctance to share information due to legislative uncertainty. It is both culturally and structurally institutionalised within intelligence organisations and their wider criminal justice partners. This anxiety is based on a lack of understanding of legislation. It engenders a fear of attracting criticism about sharing information, and, as a consequence, encourages the adoption of a risk avoidance culture. Relief comes by increasingly defaulting to a 'non-share position', an arrangement morally wrong but rarely attracting serious individual and organisation penalty.

Perhaps the most high profile example of legislative anxiety was illustrated by the Humberside Police Chief Constable David Westwood's explanation, during the *Bichard Inquiry,* why information was not shared further with agencies. He later admitted he was wrong not to share with Cambridgeshire Police nine allegations of sexual offences recorded against Ian Huntley by the Force. He had originally blamed legal constraints imposed by the *Data Protection Act 1998* which, he believed, prevented him sharing intelligence, as none of it related to convictions in law. Bichard commented on the nervousness of police when it came to data related legislation.

> *'It is evident that police officers were nervous about breaching the legislation, partly at least because too little was done to educate and reassure them about its impact'.* (Bichard, 2004, p.4)

Derbyshire Police were also subjected to criticism for not releasing the photographs of two murderers who absconded from prison in 2007. In defending their decision over public concerns, it emerged that part of the original decision making process took into account the prisoners' privacy rights enshrined by the *Human Rights Act 1998* and provisions of the *Data Protection Act 1998*. The images were subsequently released to the public by Greater Manchester Police, an area where the escaped prisoners had links. In another case, the *Ministry of Justice* refused to name 39 prisoners who had 'fled' HMP Hollesley Bay, stating to do so would breach obligations under the *Data Protection Act 1998*. In 2008 West Midlands Police officers refused to provide to their own colleagues details of prisoners who had regularly been arrested and tested positive for opiates. The purpose of the request was to identify opportunities for informants to target prolific and priority offenders. The officers justified their refusal to share by quoting potential breaches of the *Data Protection Act 1998*. Subsequent communication with the ICO stated it clearly did not. There appears to be a universal sense of *legislative anxiety* and the subsequent failure to share information, but it is not unique to this country.[xxix]

Legislative anxiety is exacerbated by a phenomenon concerning many (Flanagan, 2007), including a Government who proposed that *'action must be taken to challenge the culture of risk aversion that has developed in policing'* (Home Office, 2010c, para. 3.18). The IPCC, the author of many critical reports on inadequate police information management, also stated that:

> *'This [risk aversity] cannot be in the public interest – the police will not do their job effectively to protect the public and make communities safer if they are afraid to make decisions for fear of being blamed if things go wrong'.* (IPCC, 2011b, p.2)

There is no single source of legislation regulating information management. Rather, information sharing is governed by 'a *range of express and implied statutory provisions and common-law rule'* (Thomas and Walport, 2008, p.22). Legislation should be reviewed, codified and simplified; it should include a mandated duty to cooperate with law enforcement and partners where the information is reasonably likely to inform legitimate policing activity. There should be a presumption to share where the circumstances of the request suggest a *prima facie* case that disclosure would support prevention, detection, investigation and prosecution.

This default cooperative position would specifically assist in mitigating against a number of Sheptycki's pathologies, including *'linkage blindness', 'intelligence gaps', 'institutional friction', 'intelligence hoarding'* and *'negative operational sub-cultures'*. It would also deter additional pathologies identified during this research, including 'reputational defenders', 'data-knowledge deficit' and 'situational parochialism'. Law enforcement should submit proposals to the Law Commission[xxx] to review existing provisions associated with information sharing. Where they hinder sharing, the provisions should be modified, consolidated and codified. The moment is opportune, as the Law Commission will commence (Law Commission, 2012, p.12) a scoping study on data sharing between public bodies in late 2012, with a final report expected to be published late 2013. In announcing the work, it stated:

> *'There are persistent reports that public bodies have difficulty in sharing data, which prevents them from fulfilling their duties to citizens. There seem to us to be three reasons why this may be the case. First, there may be barriers in the substantive law which unduly restrict data sharing between public bodies. Secondly, even if the law allows for sharing, it could be that the law is so unclear that it is easy to misunderstand and misapply, creating perceived barriers to data sharing. Therefore, there is something wrong with the form of the law – the way it is expressed. Thirdly, it may be that there is simply a gap in education, guidance and advice on the law'.* (Law Commission, 2012, p.12)

This thesis holds that while much of the substantive law already exists to enable information sharing, its provisions are scattered across, and to some extent hidden in, an extensive legislative landscape, with information sharing language open to widespread misunderstanding and misapplication. Accordingly, the articulation and organisation of relevant law requires urgent attention. However, as with any legislative provision, this will require explanation to those who may be affected by its provisions either as users, as targets or as persons subjected to unavoidable collateral intrusion. Law enforcement, and, in particular, the intelligence community, will need to ensure legislative knowledge gaps are addressed.

The second new pathology added to Sheptycki's lexicon is *'technical dysfunctionality'*. Technology is not promoted here as a 'silver bullet' for repeated failures in information sharing. Even with an array of sophisticated and advanced data management tools, effective and timely information sharing can be stymied by organisational cultures. Nonetheless, technology offers a means of managing large volumes of data, of filtering data on the basis of relevance, of automatically pulling relevant data to the users and pushing to those who need it at a specific time and place.

'Technical dysfunctionality' describes the failure by law enforcement to optimally utilise its existing technology and embrace new technology in support of information sharing process. This pathology does not simply refer to technical functionality of the system itself; rather, it holds that inefficient and ineffective use affects functionality, the accompanying internally generated constraining regulatory policies, the overly cautious information technology security arrangements deterring creative and innovative technical solutions and the absence of customer inclusion in technology projects, all combine to undermine capability and capacity. This pathology is closely associated with, and causal to, a number of Sheptycki's pathologies including *'digital divide, linkage blindness'*, *'non-reporting and non-recording'*, *'duplication'*, and *'intelligence silos'*.

The extent of this technical dysfunctionality is still very much present in UK policing. In its report the HMIC commented

> ***Weaknesses in operational support*** *– intelligence systems lack the capability to provide officers with near real-time, relevant information and intelligence in the field. Also, the deployment of officers was rarely planned throughout shifts to achieve the best effect. Technology was patchy and varied and, where available, was often not fully functioning or adopted by officers. (HMIC, 2012, p.3)*

It found that in its inspection of six force areas

> *Out of the 19 basic technology operating systems now required by a constable to carry out frontline roles away from police stations, only one was consistently available and was not always effectual. (HMIC, 2012, p.3)*

Information database connectivity can establish, stimulate and enhance information sharing relationships; it can introduce enduring channels for seamless information flow within an organisation and between organisations. Rather than establishing a 'super-database', the approach should be one where gateways are established allowing auditable access to stored information, including passive data generators. These may include subscribers, call information, CCTV and ANPR reads, flight passenger notifications, contactless smartcards (eg London Oystercards), retail loyalty and rewards cards, and credit card usage. Currently this information is accessed either through court orders, information sharing agreements or legislative based authorities such as the *Regulation of Investigatory Powers Act 2000.*

This array of data sources now demands significant data analysis capability. Its underpinning techniques are crucial to coping with an information-rich age brought about by the internet, investment in education, 24/7 media and greater connectivity, and the mainstreaming of electronic data capture. Information flows need to be able to operate using different platforms and means, accessing and retrieving data from open and protected cyber space, be it in electronic, paper, oral, and physical formats. Information sharing needs to embrace new media, including social media. Information flows need to be mobile, crossing domestic and international borders at the press of a keyboard. Technological retrieval blurs the distinctions between home and overseas theatres, private and public operating arenas, national security intelligence space and traditional policing responsibilities.

Events and circumstances shape all organisations, and this is exemplified in technological innovation. Austerity means that securing funding commitments for costly items such as new data management technology, especially operating on a national scale, will be challenging. This does not mean that planning future user requirements, enhancing law enforcement and partner agreement on functionality and information sharing, and horizon scanning for future technical opportunities, should not be pursued. Even if funding was forthcoming for major investments, this does not automatically resolve the issue of information sharing. As FBI Director Robert Mueller (2007, quoted in Zegard, 2007, p.192-193) commented:

> *'I would love to be able to go out and get a contractor and say, 'okay come in and fix it'. Part of the problems is that you have to change your business practices as well. We've probably had the same business practices in place for ninety-eight years of our existence. And one of the things you do not want to do is just tell the technologists to go ahead and change it without changing your business practices'.*

For instance, the Government Protective Marking System (GPMS)[xxxi] offers protection from compromise of methodology and sources, but it also impedes and prevents information sharing. Over-classification can inhibit access, lead to failure to share information in a timely, actionable and accurate manner, and impose expensive protective controls. Over-classification creates confusion as to what can and cannot be shared, and slows down dissemination, as original owners are sought to provide permission prior to passing on information. The over-classification is antithetical to the creation and operation of the information sharing environment established under Section 115 of *Crime and Disorder Act 1998*. Another aspect of the GPMS is that it was developed with national security consideration in mind, involving attacks and infiltration by state actors. The capability and capacity of the average burglar or car thief is very different, and the use of GPMS may be using an operational security sledgehammer to crack a criminal nut. This issue was of such concern (US Congress, 2004a, p410) in the USA that it passed legislation to tackle over-classification in support for the Intelligence Sharing Environment (ISE). The Act's purpose is:

> *'To require the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information, and for other purposes'.* (US Reducing Over-Classification Act , 2010)

All policing models that have claimed to challenge the dominant reactive policing paradigm have, to varying degrees, required reliable, timely and accurate information. This demands structures and processes that can identify sources of information, where necessary collect from them, and store in a retrievable system for future development.

> *'Clearly, technologies, especially information technologies, have been the prime movers in organizational change in the last one hundred years. Yet, information systems alone do not change organizations; they must be attuned to simulate, stimulate, and respond to reflexive practice - the ongoing application of knowledge by people to their present and future decisions (...) It is not simply a matter of setting goals and objectives. It may come into conflict with leadership fantasies, political campaigns, media orgies, and feeding frenzies of either the positive or negative sort, or with the short-term goals of the chief and his/her staff'.* (Manning, 2008, pp.24-25)

Corralling different agency databases is not enough. The establishment of multi-agency intelligence units or fusion units alone cannot automatically deliver more effective information sharing. Regional policing initiatives have experienced significant difficulty in securing access to the participant force databases, often based on poor connectivity and reluctant information technology staff and Security Information officers. In the USA, where the concept of fusion units are more established, it was reported that a White House Commission studying intelligence failures visited *National Counter-Terrorism Centre:*

> *'The commissioners found that there were no less than nine levels of classified information stored in the center's computers. Analysts from different agencies had different clearances, making it difficult for them to talk to one another'.* (Klaidman and Isikoff, 2005)

A national intelligence agency and regional fusion units are by no means cast iron guarantees of success in information sharing. Little evidence is available to suggest they have delivered enhanced communication and coordination in counter-terrorism in the USA (Taylor and Russell, 2012). Co-location is not enough. Intelligence holders need to be directly connected to each others' intelligence systems, permission to access information and the ability to use it.

Interestingly, when the fusion structure focuses on crime rather than counter-terrorism, the information sharing appears to work more effectively (Taylor and Russell, 2012, p.198).

Terrorist attacks and the speed of terrorist targeting have underlined the need for pre-emptive intelligence which is speedily shared with partners for immediate action. This will require not only technological platforms and clear and unambiguous legislative provisions, but also an intelligence community that is competent, confident and capable of moving quickly on raw data. For it to have an operational purpose, and an ability to address an emerging problem, information has to be shared in an appropriate and timely fashion, and this is where professional competence is key.

The extent that *legislative anxiety* and *technological dysfunctionality* impact on information sharing is intrinsically linked to the degree of proficiency and capability of law enforcement personnel, and, in particular, the intelligence professional. An absence of talent management and intelligence career pathways geared towards securing, developing and retaining the best intelligence professionals, poorly trained intelligence staff, uninspiring management and an absence of dynamic strategic leadership on intelligence matters, all contribute to information sharing pathologies. Although these problems are not entirely new, what is different is the extent of these problems, which are at crisis point. A 'state of the nation' report on the police intelligence community would highlight its drift to the margins of the police organisation, a devaluing of its role, disproportionately hard cuts in this era of austerity, a weakened capacity and capability to undertake specialist collection, and a questioning of its automatic place at the high table of core policing. It's 'intelligence led policing model' zenith now seems a distant memory as it now moves inexorably to a pre-Bichard nadir. This perfect storm generates the third lexicon, *professional incompetence.* It contributes, in varying degrees, to Sheptycki's *'noise', 'intelligence overload', 'non reporting and non recording', institutional friction', 'intelligence hoarding',* and *'occupational sub-cultures including intra and inter subcultures'* (Sheptycki, 2004). However, the extent of the decline of the intelligence professional within policing is such that it warrants its own category of pathology.

The concept of the 'intelligence professional' came to prominence with the *9/11* where they held that *'a common set of personnel standards for intelligence can create a group of professionals better able to operate in joint activities, transcending their own service-specific mind sets'*(US Congress, 2004a, p.409). Current human resource driven practices sometimes negate this. Tackling professional incompetence improves personal and organisational capacity, confidence and capability, addresses the paucity of imagination, and reverses an apparent desensitised relationship with the customer.

Senior officers and staff, the strategic leaders, are the principal decision makers in the police service. Consequently, they directly influence success and failure within intelligence departments. A deterministic approach may dismiss the exogenous political, legal and economic constraints on these managers, but, more importantly, information sharing culture must be also driven from the bottom up. The change agents must include database managers, information security officers, intelligence managers, analysts, researchers, and in-putters, as well as ACPO level champions.

What is proposed here is a broader and multi-layered approach to the professionalisation of the law enforcement's 'intelligence community', with the key objective to enhance information flow. Three layers of development are needed to strengthen and build the information sharing environment. The areas; *Strategic Leadership, Talent Management and Knowledge Advancement* all place the development of the intelligence professional at its core. Each area can contribute independently, but combined, the synergy enriches and augments the intended outcome. The whole will then be greater than the sum of its parts.

Effective intelligence capability is best served with informed, committed and innovative strategic leadership. They need, like intelligence champions[xxxii] before them, to be able to mobilise organisational, political, and legal resources towards a shared goal of enhanced intelligence. One ACPO rank officer with responsibility for intelligence, commented:

> *'We need senior people at the national centre, calling the shots in relation to intelligence strategy and practice. It's not going to happen though, the Government are keen to decentralise, localism is the policy of the day'* (Interview 4).

However there are some who believe intelligence no longer an important area of policing. A Director of Intelligence for a large force stated:

> *'Basic Command Unit commanders see no real value in intelligence, it forms no real part of their promotion course or career pathway. They do not understand intelligence and as a consequence do not have the confidence in the quality of our organisations intelligence systems. The intelligence establishment numbers are under threat, for example analysis is not a luxury but many senior officers need convincing. We are*

> *making progress but Analysts are often only as good as those who task them. There is a need to educate the 'intelligence customer'* (Interview 12).

Leaders need to be able to step outside the current intelligence culture and initiate change, ensuring policy and practice becomes more adaptive, customer focussed, connected and cutting edge. The importance of culture at work is significant: *'Culture has an invisible but powerful hold, colouring how intelligence officials view the world and their role in it'* (Zegard, 2007, p.196).

Intelligence reform and information management needs a champion. The sector cannot rely on the 'Micawber principle'[xxxiii] in a changing policing landscape, where Government has removed nationally driven targets. The introduction of locally elected *Police and Crime Commissioners* (PCC) may also encourage a narrow operational focus[xxxiv]. Leadership must ensure that parochialism does not undermine intelligence reform, especially where national and regional considerations are part of the solution. This localism is not new:

'The policing territorial framework is reinforced through performance management regimes enshrining the twin principles of local policing; local delivery and local accountability(...) Whilst police powers are applicable nationally, performance focus is upon police forces and their constituent basic command units'. (Harfield, 2008, p.65)

Leaders need to identify indicators that demonstrate where and when the intelligence community is failing to support the organisation. Structure and resourcing determines how information sharing operates. Symptoms of decline are evident in police intelligence. Shrinkage in resources (Cameron, 1983) are reflected in the reduction of dedicated staff and ICT support. While many aspects of policing have seen reductions in resources, there has been a disproportionate austerity driven reduction in intelligence[xxxv]. Shrinking market (Harrigan, 1982) involves alternative providers of intelligence, via other law enforcement agencies, or the private sector. Negative profitability (Hambrick and D'Aveni, 1988) occurs when intelligence units are less able to contribute to crime reduction or community confidence. Convincing the public to support intelligence collection, especially where undertaken in a covert context, is crucial. The loss of legitimacy (Benson, 1975) is seen externally in complaints against police, negative media articles and exclusion from key decision making forums. Internally, fractured employment relations are manifested in grievances, tribunal claims, absence levels, high turnover and poor response to vacancies.

The requirement for leadership in the reform of law enforcement intelligence lends itself to the establishment of an *Office of National Law Enforcement Intelligence* (ONLEI), similar to one in the USA, overseeing all issues relating to law enforcement intelligence, including information sharing, collection techniques and standards. It is different from the ACPO Intelligence Portfolio in that the ONLEI concept is envisaged to be a dedicated multi-agency rather than a part time police only subgroup reporting to ACPO Crime Business area. It will also be distinctive from the intelligence functionality to be established under the NCA in that it will focus on intelligence impacting on all NIM Levels of criminality, rather than Level 3 national and international organised crime.

The ONLEI concept may expand incrementally to incorporate other non law enforcement agencies where intelligence is central to the business, *Secret Intelligence Service* (MI6), the *Security Service* (MI5) and the *Government Communications Headquarters* (GCHQ), such as the *Defence Intelligence Staff* and *Joint Intelligence Committee* mandated by the *Intelligence Services Act 1994*, HM Prison Service and other criminal justice agencies, business and community partners. Further scoping research is needed into how an ONLEI concept could merge with other UK machinery, so that law enforcement intelligence collection is on an equal footing with other agencies. Ultimately, all agencies relying on information and intelligence should integrate their collection capabilities to make sense of problems that society faces.

The information sharing rhetoric underpinning intelligence needs to be a more genuine aspiration. This can be delivered if coordinated nationally by strategic leaders/structures, and implemented regionally. An allocation of talent and resources to drive the wider changes is needed to improve intelligence structures and inter-agency information sharing. These must be dedicated resources offering an opportunity to take a long view of information management strategy, with trained staff, supported in an intelligence career pathway. Integrated within a talent management strategy, employees then have opportunities across specialist disciplines in both lateral and vertical career progression.

Private sector, governmental, NGOs, Armed Services and intelligence agencies all compete with law enforcement for high calibre staff *'in the war for talent'* (Michaels, Handfield-Jones and Axelrod, 2001). Efforts by police in this area are hampered by a series of regulatory, cultural and budgetary factors, some externally imposed, but others are a consequence of internal policy and organisational decision-making. The cumulative effect of inflexibility, nonadjustable remuneration packages, creativity and innovation deficit, when compared to other competitors, creates a drain on talent. Police human resource capability and capacity can be 'out of step' with modern talent management practices, and may be the 'tail wagging the dog'.[xxxvi]

Austerity measures have limited recruitment. Resource management strategies sometimes fill intelligence post vacancies with 'restricted officers'[xxxvii] rather than open posts to all staff with the necessary skills. Intelligence roles are deemed to be 'back office', not requiring warranted powers, and accordingly suitable for cost reduction by way of civilianisation. The recruitment net may be cast wider, but at the risk of excluding operational experience that can contribute to '*noise*' pathology. A mixed economy team, comprising of officers, staff, subject matter experts and informed volunteers, is more appropriate than a selection based primarily on financial efficiencies.

Arbitrarily enforced retirements under regulation A19 procedures[xxxviii] and compulsory police staff redundancy, almost irrespective of skills and competence, accelerate specialist 'brain-drain'. There is little scope to create targeted incentives. Winsor reforms have reduced initial starting pay and removed many financial benefits, but the impact on recruitment and retention of higher calibre staff is yet unknown. Initial recruitment into intelligence posts is weighted towards internal appointments.

Research generated by eleven police forces indicated that promotion is linked to evidence of uniformed neighbourhood rather than specialist policing. Promotion through the ranks generally means a deployment into general policing duties. This is particularly the case for the Constable to Sergeant rank, where supervising a response or neighbourhood team, or custody officer role, is the likely new post. Commitment to the traditional development of the 'omni-competent' police officer, capable of performing all tasks in any given situation, is no longer a credible response to an increasingly complex criminal justice environment and society. The goal should be to increase standards within narrower operational fields, such as an intelligence and covert policing career pathway, which should enable the profession to better grasp relevant legislation, procedure, technical functionality, and risk control issues.

Knowledge advancement and competency development

National policing *Integrated Competency Framework* (ICF) roles have now been replaced by *Police Professional Framework* (PPF) roles, but the category of the intelligence still remains. Published professional skill sets for all ranks to Chief Superintendent are available, along with professional skills sets from level 1 to 4 and professional skills sets for secondary roles working in intelligence. These PPF roles should be reviewed to reflect advances in technology, changes in intelligence doctrine, legal judgements, the impact of the global village and emerging threats.

Sponsored educational programmes in learning establishments overseen by dedicated academics are needed. Competency framework standards that are fit for purpose, mandatory and challenging, need to be agreed. Intelligence employees should be able to gain nationally/internationally recognised awards from a professional body to reinforce the value and status[xxxix] of the role and to encourage higher standards. This could be through a chartered, independent certification or accreditation body, so that intelligence professionals have a bona fide qualification to practice in the intelligence community.

UK police intelligence courses are relatively brief, the duration between two to five days, and some forces have no in-house training capability. Intelligence courses are also delivered in 'levels', best illustrated by the *National Policing Improvement Agency's* intelligence modules which include a *Core Intelligence* course (2 days), an *Intelligence Managers* Course (5 days) and a senior officers' *Strategic Management of Intelligence* Course (3 days). Their *Analyst Foundation* course takes 10 days. Whether these succinct 'short courses' are sufficient is debatable.

Better training has emerged through closer relationships between law enforcement and academia in recent years, but there is still no course dedicated to police intelligence. Courses of a similar vein do exist, but are heavily weighted towards complementary disciplines of national security and counter-terrorism. Criminal intelligence is either absent from the curriculum or a minor element of it.

The US has identified this as an important area to improve its intelligence processes and organisation. In 2002 the *Central Intelligence Agency* (CIA) established the CIA University[xl], and subsequently the *Federal Bureau of Investigations* (FBI) its *College of Analytical Studies.* The

Office of the Director of National Intelligence (ODNI) created a *"virtual' national University as a way to coordinated training across the intelligence community'* (Marrin, 2009, p.132). The *Pat Roberts Intelligence Scholars Programme* (PRISP) was established to encourage more high calibre recruits into the US intelligence and security sector by funding university students who in turn commit to 18 months working in the US Directorate of Intelligence on graduation. The *National Security Education Program (NSEP)* is a federal initiative which focuses primarily on building a large pool of US employees with critical languages and insight into different cultures of interest. This scheme requires, on graduation, a 1 year commitment to work for the US Government.

By contrast and to date, the UK has been less ambitious. In December 2012, the Coalition Government announced the establishment of a new professional policing body, the *College of Policing*[xli], which was officially launched on 4th February 2013. It is the successor body to the NPIA. No significant resources are allocated to improving national intelligence skills and practices. The effectiveness of the *ACPO Professionalising Intelligence working Group* has struggled to significantly progress major work and has since been consumed into the *National Analyst Working Group*. Detailed proposals for the development of law enforcement intelligence as part of a national strategy for improvement are not yet publically articulated. However, the College will:

> *'Set and enhance first-class national standards of professionalism to ensure excellence in operational policing: by developing a set of nationally agreed standards for officers and staff to attain; providing frameworks for standards to be tested and achievement rewarded; and by supporting national business areas support the education and professional development of police officers and staff: by developing and maintaining the national policing curriculum, assessment and accreditation frameworks; delivery of leadership and specialist training; accrediting and quality-assuring training providers; developing future leaders and expertise through effective talent management'.* (Home Office, 2012)

Vigorous competition in training and education advances the quality, breadth and depth of knowledge. It will encourage educational entrepreneurs and researchers to explore intelligence processes and outcomes, and identify solutions for intractable problems. Professional competency would be enhanced by a mandated requirement for continued participation in learning.

Accessibility to existing intelligence and covert information, presently fastidiously restricted to a small number of practitioners, could open up existing knowledge to new perspectives, tactics, applications, technologies and research. The Chair of the *Competition Commission* held that where competition is open and fair:

> *'The consequences are that prices will typically be bid down to an efficient level of costs, a diversity of product offerings will come on to the market that matches the heterogeneity of consumer needs and tastes, and the rate of innovation will be high'.* (Geroski, 2004)

This will be a cultural challenge, as information access has traditionally been restricted even amongst the wider police community. This extends to agreed national training competencies, non-law enforcement participation on ACPO Working and steering groups, and private sectors. The status quo undermines progress and marginalises specialist intelligence and covert policing. The restrictions are often unnecessary[xlii], disproportionate, and fuelled by self interest amongst police service and training providers who either deliberately or unwittingly exclude competitors. Legitimate concerns can be addressed, as they are in other sensitive areas of Government, policing and military, through vetting, agreement on security arrangements, customer selection criteria and standards controls.

Cross fertilisation of interagency ideas and best practice can be achieved through the logistically challenging but effective use of secondments of intelligence staff across different departments and agencies. This will help instil a culture of mutual understanding and sympathy between partner agencies.

Conclusion

The most obvious factor for intelligence failure is the very absence of it. Reported 'failures' must be balanced against undoubted successes. As one commentator stated:

> *'Perhaps there is some truth to the saying that in intelligence, failures become public while successes are kept secret'* (Marrin, 2012)

However, Government Inquiries and IPCC investigations into allegations of intelligence and law enforcement shortcomings often reveals that the information did exist, but it was not stored in a way that enabled it to be discovered. The inability to effectively search and retrieve the information, access it when required, and push it to those requiring it for subsequent action, is a significant flaw. Counter-measures are needed to avoid *'intelligence overload'*, *'duplication'* and *'noise'*, such as filtering, big data analysis capability, national common data intelligence standards and evaluation.

Effective information sharing is not simply about establishing technical connectivity between forces. Organised crime transcends not only police geographical boundaries but also other criminal justice agencies. It can effortlessly cross into and through other international jurisdictions. This requires technical gateways, open cultural and legal egress, but rigid rational legal bureaucracies struggle to adapt and establish these networks. Genuine 'all-source' assessment is beyond the realm of a single force/agency, but enhanced cultural, organisational and technical connectivity moves them closer to this goal.

Without 'all source' knowledge of the scope and nature of the threat and its impact on communities, subsequent decision making is fundamentally flawed from the outset. Tackling this lacuna forms the basis of effective collection efforts to satisfy the intelligence requirement. Poor information sharing management, including the competencies of intelligence professionals, makes closing intelligence gaps difficult, increases the likelihood of expensive duplication in collection and assessment, and undermines the agility and value of the information.

To enhance capacity and capability, the public police monopoly on sensitive criminal intelligence should be reviewed. Private sector skills, technology, and acumen in data management should be examined[xliii]. Again, the US is currently more inclined to do so (Taylor and Russell, 2012, p184). In 2008 the US *Office of Director of National Intelligence* confirmed that 29 per cent of intelligence agencies' workforce was drawn from the private sector (Priest and Arkin, 2010). Within the UK, the private security industry is building up its intelligence collection capability (G4S, 2011) and within privatised prison establishments, multiple private sector companies already oversee covert and specialist intelligence collection.

The current array of legal sources and provisions hinders an effective and proactive information sharing culture. Information sharing legislation has developed incrementally through enactment of various statutory arrangements and the system of judicial precedent. The result of this piecemeal approach is illustrated by Parliament choosing, on a regular basis, to create new statutory 'gateways' giving specific bodies express powers to sharing information, or mandating a duty to cooperate with other bodies. Often these are written in response to a specific Government crime reduction policy, lack of certainty over existing information sharing powers, or in response to a criticism by an Inquiry. Information sharing legislation should be codified into a single Statute, the provisions forming a key part of law enforcement basic and specialist intelligence training and a culture of reward for sharing information introduced.

A combination of a data sharing technological package, a codified information sharing legislation drafted to encourage victim focused dissemination, and organisational culture of intelligence professionals, offers the best opportunities to reduce failures in information sharing, and thereby enhance public trust and confidence in the police. Initiating and sustaining these changes will be challenging at a time of competing economic, social and political pressures, but they are crucial to reducing incidents of harm emanating out of poor information management and process.

The key factors undermining information sharing must be tackled, but the police cannot solve the problem alone. Even if access to information is relaxed, the data received needs to be re-checked and verified, understood contextually, corroborated through existing information, and developed further. Seamless sharing may aggravate one of Sheptycki's pathologies '*Information overload*.' To avoid this, filtering and data visualisation techniques should be applied. Efforts to address information sharing pathologies should also factor in international policing cooperation, if we are to grip serious organised crime. Information and intelligence need to be able to cross borders as easily as human traffickers, terrorists, criminal proceeds and commodities.

The thesis does not suggest there needs to be a revolution in policing intelligence, rather an expeditious evolution, gripped by intelligence champions and engaged communities. There is a need for a collective and shared responsibility to enhance information flows based on a commitment to delivering national and community security. This can be achieved by addressing legislative anxiety, tackling technological dysfunction and professionalising the intelligence community. Sharing information and knowledge is not about undermining human rights and unwarranted intrusions into private lives. It involves robustly attacking threat and harm, whenever and wherever they arise. It is about understanding the needs of different communities, and developing new capacities and capabilities for action. In an increasingly challenging time, technology aided shared information, secured and developed by a professionalised intelligence community and lawfully used, provides the first and last line of defence against criminals.

Appendix: A

Government Protective Marking

Top Secret

The compromise of assets marked TOP SECRET would be likely to:

- Threaten directly the internal stability of the UK or friendly countries
- Lead directly to widespread loss of life
- Cause exceptionally grave damage to the effectiveness or security of UK or allied forces
- Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations
- Cause exceptionally grave damage to relations with friendly governments
- Cause severe long term damage to the UK economy

Secret

The compromise of assets marked SECRET would be likely to:

- Raise international tension
- Seriously damage relations with friendly governments
- Threaten life directly or seriously prejudice public order or individual security or liberty
- Cause serious damage to the operational effectiveness or security of UK or allied forces
- Cause serious damage to the continuing effectiveness of highly valuable security or intelligence operations
- Cause substantial material damage to national finances or economic and commercial interests

Confidential

The compromise of assets marked CONFIDENTIAL would be likely to:

- Materially damage diplomatic relations, that is, cause formal protest or other sanctions
- Prejudice individual security or liberty
- Cause serious damage to the operational effectiveness or security of UK or allied forces
- Cause serious damage to the effectiveness of valuable security or intelligence operations
- Work substantially against national finances or economic and commercial interests
- Substantially undermine the financial viability of major organisations
- Impede the investigation or facilitate the commission of serious crime
- Seriously impede the development or operation of major government policies
- Shut down or otherwise substantially disrupt significant national operations

Restricted

The compromise of assets marked RESTRICTED would be likely to:

- Adversely affect diplomatic relations
- Cause substantial distress to individuals

	• Make it more difficult to maintain the operational effectiveness or security of UK or allied forces • Cause financial loss or loss of earnings potential to, or facilitate improper gain or advantage for, individuals or companies • Prejudice the investigation or facilitate the commission of crime • Breach proper undertakings to maintain confidence of information provided by third parties • Impede the effective development or operation of government policies • Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and/or the e-government Security Framework) • Disadvantage government in commercial or policy negotiations with others • Undermine the proper management of the public sector and its operation

Appendix: B

Bibliography

ACPO (1975) *Report of the ACPO Subcommittee on Criminal Intelligence (Baumber report).* London: Association of Chief Police Officers.

ACPO (1978) *Third Report of the Working Party on a Structure of Criminal Intelligence Officers above Force Level (Pearce Report).* London: Association of Chief Police Officers.

ACPO (1986) *Report of the ACPO Working Party on Operational Intelligence (Ratcliffe Report)* London: Association of Chief Police Officers.

ACPO (1990) *Report on the Regional Crime Squads (Dickens Report).* London: Association of Chief Police Officers.

ACPO (2005a) *National Intelligence Model Minimum Standards.* Wyboston: NCPE.

ACPO (2005b) *Guidance on the National Intelligence Model.* Wyboston: NCPE

ACPO (2005c) *National Intelligence Model: Code of Practice.* London: National Centre for Policing Excellence.

ACPO(2006a) *Briefing paper on Neighbourhood Policing and the National Intelligence Model* Wyboston: NCPE.

ACPO (2006b) *Guidance on the Management of Police Information.* Wyboston: NCPE.

ACPO (2006c) *Guidance on the National Briefing Model.* Wyboston: NCPE.

ACPO (2006d) *Practice Advice on Tasking and Co-ordination.* Wyboston: NCPE.

ACPO (2006e) *Data protection: Manual of Guidance.* Wyboston: NCPE.

ACPO (2007a) *Practice Advice: Introduction to Intelligence Policing* Wyboston: NCPE.

ACPO (2007b) *Practice Advice on Resources and the People Assets of the National Intelligence Model.* Wyboston: NPIA.

ACPO (2010) *Guidance on the Management of Police Information.* 2nd ed. London: NPIA.

ACPO (2011) *National Decision Model: Guidance for Trainers.* London: NPIA

ACPO (2013) *Policing in the UK. A Brief Guide.* London: ACPO

ACPO - HMPS (2005) Memorandum of Understanding for the exchange of information

ACPO – NOMS (2008) *Memorandum of Understanding: An agreement between the National Offender Management Service (NOMS) and the Police Service regarding the reporting and investigation of NOMS staff corruption.*

Alderson,J. (1977) *Communal Policing.* Exeter: Devon and Cornwall Constabulary.

Alderson,J. (1979) *Policing Freedom.* Plymouth: Macdonald and Evans.

Altrichter,H., Feldman,A., Posch,P., and Somekh, B. (2008) *Teachers Investigate their Work: An Introduction to Action Research across the Professions*.2nd ed. Routledge

Andrew,C., Aldrich,R.J., and Wark,W.K. eds.(2009) *Secret Intelligence: A Reader*. Abingdon: Oxon: Routledge.

Audit Commission (1993) *Helping with Enquiries: Tackling Crime Effectively*. London: Audit Commission.

Audit Commission (1996) *Tackling Patrol Effectively*. London: Audit Commission.

Audit Commission, HMIC and ACPO (1996) *Tackling Crime Effectively Management Handbook Volume 2*. Bristol: Audit Commission:

BBC (2007) *Anti-Terrorism spending to rise £1billion* [Internet], 09/10/2007. Available from: <http://news.bbc.co.uk/1/hi/uk/7036121> [Accessed 12/05/2012].

BBC (2005) *Fears over CIA 'University* Spies' [Internet] 02/06/2005. <http://news.bbc.co.uk/1/hi/4603271> [Accessed 03/03/2012].

Benson,J. (1975) Inter-organizational networks as a political economy. *Administrative Science Quarterly*, 20(3), pp.229-249.

Berger,P.L. (1966) *Invitation to Sociology*. New York: Doubleday.

Berry,G., Izat,J., Mawby,R., Walley,L. and Wright,A. (1998) *Practical Police Management.* London: Police Review Publishing.

Berry,J.(2010) *Reducing Bureaucracy in Policing Final Report.* [Internet] <http://www.homeoffice.gov.uk/publications/police/reducing-bureaucracy/reduce-bureaucracy-police> [Accessed 09/04/2012].

Bessant,C. (2009) Miscellany of legislative provisions. In Bessant,C. (ed). *Information Sharing Handbook*. Chippenham: Law Society Publishing.

Bichard,M. (2004) *The Bichard Inquiry Report A Public Inquiry Report on child protection procedures in Humberside Police and Cambridgeshire Constabulary, particularly the effectiveness of relevant intelligence-based record keeping, vetting practices since 1995 and information sharing with other agencies* .HMSO: London

Blakey,D. (2008) *Disrupting the supply of illicit drugs into prisons*: *A report for the Director General of National Offender Management Service.* [Internet] <http://www.drugscope.org.uk/Resources/Drugscope/Documents/PDF/Good%20Practice/blakeyreport.pdf> [Accessed on 27/01/2012].

Block,L. (2008) Cross-Border Liaison and Intelligence: Practicalities and Issues. In Harfield,C., MacVean,A., Grieve,J.G.D., and Phillips,D. (eds) *The Handbook of Intelligent*

Policing: Consilience, Crime Control, and Community Safety Oxford: Oxford University Press.

Brady,H. (2009) *Intelligence, Emergencies and Foreign Policy: The EU's role in Counter-Terrorism*. London: CER.

Braga,A., Piehl,A.M., and Kennedy,D.M. (1999) Youth Homicide in Boston. *Homicide Studies* 3(4), pp. 277-299.

Brodeur, J. (1995) Undercover Policing in Canada: A study of its Consequences. In Fijnaut,C., and Marx,G. (eds) *Undercover: Police Surveillance in comparative perspective.* The Hague: Kluwer Law International, Martinus Nijhoff Publishers.

Bruce,J.B., and George,R.Z,(2008) Intelligence analysis-the Emergence of a Discipline. In Bruce,J.B. and George, R.Z (eds) *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington D.C.: Georgetown University Press.

Butler,R.(2004) *Review of Intelligence on Weapons of Mass Destruction, Report of a Committee of Privy Counsellors.* HC898. London: TSO, July 2004

HMG (2008) *Security Policy Framework V 1.0.*London: Cabinet Office

HMG *Manual of Protective Standards*

Cameron,K.S. (1983) Strategic Responses to Conditions of Decline: Higher Education and the Private Sector. *Journal of Higher Education*, 54, pp. 359-380.

Central Intelligence Agency (1999) (Office of Public Affairs*), A Consumer's Guide to Intelligence: Gaining knowledge and Foreknowledge of the World around Us*. Washington D.C.: Central Intelligence Agency.

Central Intelligence Agency (2012) *Pat Roberts Intelligence Scholars Program – (PRISP)[*Internet] Available from: <https://www.cia.gov/careers/opportunities/analytical/pat-roberts-intelligence-scholars-program-prisp.html > [Accessed 12/04/2012]

Centre for Public Innovation (2012) *Information Sharing to tackle violence Audit of progress on delivering the Coalition Commitment 2012.* Gecko Social Health Outcomes LLP

ComputerWeekly.com (2007) *PITO goes as IT is streamlined.* [Internet], 03/04/2007. Available from: <http://www.computerweekly.com/Articles/2007/04/03/222818/pito-goes-as-police-it-streamlined.htm> [Accessed 11/11/2011].

Conservatives (2010) *Conservative Liberal Democrat Coalition Negotiations Agreements Reached 11 May 2010* [Internet], Conservatives. Available from <http://www.conservatives.com/News/News_stories/2010/05/Coalition_Agreement_published.aspx> [Accessed 10/07/2012].

Cohen,D., and Crabtree,B. (2006) *Qualitative Research Guidelines Project* July 2006. [Internet], http://www.qualres.org/HomeSemi-3629.html [Accessed 12/11/2011].

Cohen, L., and Manion,L. (2000). *Research methods in education.* London: Routledge Falmer.

Cope,N. (2004) Intelligence-led Policing or Policing-Led Intelligence? Integrating Volume Crime Analysis into Policing. *British Journal of Criminology* 44, 2, pp. 188-203.

Davies,P. (2009) Ideas of intelligence: Divergent National Concepts and Institutions. In Andrew,C., Aldrich,R.J. and Wark, W.K. (Eds) (2009) *Secret Intelligence: A Reader.* Abingdon: Oxon: Routledge, pp. 12-18

DiMaggio,P.J., and Powell,W.W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review* 48, pp. 147–160.

Dintino,J., and Martens F.T. (1982) Police Intelligence: A luxury, Necessary Evil, or Managerial tool?. *Criminal Justice Journal.* 1/7.July 1982, pp.1-3.

Emsley,C,. and Shpayer-Makov,H (2006) Police Detectives in History, 1750-1950.Gateshead: Ashgate.

Emsley,C. (2008) The birth and development of the police in Newburn,T. (ed) *Handbook of Policing* (2nd ed). Cullompton: Willan Publishing, pp.72-89.

Ericson, R.V., and Haggerty, K.D. (1997) *Policing the Risk Society.* Oxford: Clarendon Press.

Flanagan,R. (2007) *The Review of Policing Interim Report* Ref 283462. London: Home Office

Flood,B. (2004) Strategic aspects of the UK National Intelligence Model. In Ratcliffe,J.H. (ed) *Strategic Thinking in Criminal Intelligence.* Sydney: Federation Press, pp.37-52.

Flood,P. (2004) *Report of the Inquiry into the Australian Intelligence Agencies.* Canberra: AGPS.

Flynn,M.T., Pottinger,M., and Batchelor,P.D (2010) *Voices from the Field: Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Washington. D.C.: Centre For a New American Security.

Franks,O (1983) *Falkland Islands Review' Report of a Committee of Privy Counsellors.(The Franks Report).* London: HM Stationary Office.

Frey,J.H., and Oishi, .M. (1995): *How to conduct Interviews by telephone and in person.* Sage: London.

Friedman,C., Friedman,M., Chapman,C., and Baker,J.S. (1997) *The Intelligence Edge: How to Profit in the Information Age.* New York: Random House Publishing.

G4S ('n.d.') *G4S acquires The Cotswold Group* [Internet],G4S. Available from:<http://www.g4s.com/en/Investors/News%20Events%20and%20Presentations/Announcements/2011/04/08/Cotswolds%20Group%20Acquisition/> [Accessed 11/01/2012].

Gannon,J.C. (2008) Managing Analysis in the Information Age. In: George,R.Z.,and Bruce,J.B. (eds) *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington D.C.: Georgetown University Press. pp. 213-225.

Geroski,A.P. (2004) Is competition policy worth it?[Internet] Available from: http://www.competition-commission.org.uk/assets/competitioncommission/docs/pdf/non-inquiry/our_peop/members/chair_speeches/pdf/geroski_uea_140904 [Accessed 10/05/2012].

Glees,A., Davies,P.H.J., and Morrison,J.N.L (2007) *The Open Side of Secrecy.* London: Social Affairs Unit.

Gill,P. (2007) Evaluating Intelligence Oversight Committees. *Intelligence and National Security, 22(1),* pp. 14-37.

Gill,P. and Phythian,M.(2006) *Intelligence in an Insecure World.* Cambridge: Polity, p.42

Golding,B., and Savage,S.P. (2008) Leadership and Performance Management. In: Newburn,T. (ed) *Handbook of Policing* (2nd ed). Cullompton: Willan Publishing, pp.725-759.

Goldstein,H. (1979) Improving policing: a problem orientated approach. *Crime and Delinquency*,25 (2), pp. 236-258.

Goldstein,H (1990) *Problem Orientated Policing*. New York, NY: McGraw-Hill.

Greiner,L.E, (1972) Evolution and Revolution as Organisations Grow. Harvard Business Review July-August, pp. 397-409.

Grieve,J.G.D. (2004) Developments in UK Criminal Intelligence. In: Ratcliffe,J.H. (ed). *Strategic Thinking in Criminal Intelligence.* Sydney: The Federation Press, pp. 25-36.

Grieve,J.G.D. (2008) Lawfully Audacious: A Reflective Journey. In: Harfield,C., MacVean,A., Grieve,J.G.D. and Phillips,D. (eds) *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety*. Oxford: Oxford University Press. pp. 13-24.

Guardian (2009) *Jailed drug dealer gets 18-year sentence for running cocaine ring from his cell* [Internet] 18/08/2009. Available from: <http://www.guardian.co.uk/uk/2009/aug/18/drug-dealer-cell-cocaine-ring> [Accessed 22/12/2011].

Hambrick,D.C., and D'Aveni,R.A. (1988). Large Corporate Failures as Downward Spirals. *Administrative Science Quarterly,* **33**, pp. 1-23.

Hansard (1983) *Falkland Islands Review* (Cmnd. 8787.) *HL Deb 25/01/83 Vol 438 cc136-247* [Accessed 15/06/2012].

Harfield,C., and Harfield,K. (2008) *Intelligence: Investigation, Community and Partnership.* Blackstone's Practical Policing. Oxford: Oxford University Press.

Harfield, Clive (2008) Paradigms, Pathologies, and Practicalities – Policing organized crime in England and Wales. *Policing* (2008) 2:1, pp. 63-67.

Harrigan,K.R. (1982). Exit Decisions in Mature Industries. *Academy of Management Journal*, 25(4), pp 707-732.

Higgins,O. (2004) Rising to the collection challenge. In: Ratcliffe,J.H. (ed). *Strategic Thinking in Criminal Intelligence.* Sydney: The Federation Press, pp.70-85.

HMIC (1996) *MPS Specialist Operations Department Primary Inspections – February 1996* [Internet] Available from: <http://www.nationalarchives.gov.uk/ERORecords/HO/415/1/hmic/metso96.pdf> [Accessed 13/04/2011]

HMIC (1997) *Policing with Intelligence: Criminal Intelligence-A Thematic Inspection on Good Practice.* London: HMSO

HMIC (2003) *A Need to Know: A Thematic Inspection of Special Branch and Ports Policing.* London: TSO

HMIC (2005) *Closing the Gap - A Review of 'Fitness for Purpose' of the Current Structure of Policing in England & Wales.* London: HMIC.

HMIC (2006) *Royal Military Police Special Investigations Branch Inspection August 2006.* HMIC COI: London.

HMIC (2007) *Inspection of HM Revenue and Customs Handling of Human Intelligence Sources* London: HM Revenue and Customs Communication and Marketing.

HMIC (2010) *Handling of Human Intelligence Sources – Revisited: A Follow-up Inspection that Examines the Progress made by HM Revenue & Customs in Implementing the Recommendations of the HMIC report 'Inspection of HM Revenue and Customs Handling of Human Intelligence Sources'(2007).* London: HMIC.

HMIC (2011) *HMRC's use of Information and Intelligence to Counter Fraud in the Tax Credits system*. London: HMIC.

HMIC (2012) *Taking Time for Crime: A study of how police officers prevent crime in the field*. London: HMIC

HMCPI (2012): *Report to the Attorney General on the inspection of the Serious Fraud Office*. London: HMCPI.

Home Affairs Committee (2006) *Terrorism Detention Powers. Fourth report of Session 2005-06*, Vol.1, HC 910-I. London: TSO.

Home Office (1991) Morgan,J. (Chairman) *Safer communities: The Local Delivery of Crime Prevention through the Partnership Approach* London: HMSO.

Home Office (2003) *The National Policing Plan 2004-2007*. London: Home Office Communication Directorate.

Home Office (2005) *Serious Organised Crime Programme SOCA Intelligence Doctrine for the Reduction of Harm Caused by Serious Organised Crime RESTRICTED* (internal document)

Home Office (2006) *National Community Safety Plan 2006 – 2009* (Update November 2006) London: Home Office Crime Reduction and Community Safety Group.

Home Office (2007) *Delivering Safer Communities: A Guide to Effective Partnership Working: Guidance for Crime and Disorder Reduction Partnerships (CDRPS) and Community Safety Partnerships (CSPS).* HO 00870 G. London. Home Office.

Home Office (2009) *Extending Our reach: A Comprehensive Approach to Tackling Serious Organised Crime.* Cm7665. London:TSO.

Home Office (2010a) *Covert Human Intelligence Sources: Code of Practice*. London: TSO.

Home Office (2010b) *Interception of Communications: Code of Practice.* London: TSO.

Home Office (2010c) *Policing in the 21st Century: Reconnecting Police and the People*. CM7925. London: TSO.

Home Office (2012) *Strategic Policing Requirement: A non-statutory edition of the Strategic Policing requirement prepared in consultation with policing partners (July 2012)* http://www.homeoffice.gov.uk/publications/police/pcc/shadow-spr?view=Binary accessed 16th February 2013

Home Office: College of Policing: an introduction (2012) published 16/07/2012 accessed http://www.homeoffice.gov.uk/publications/police/college-of-policing-introduction?view=Binary 20/07/2012

HM Coroners (2011) *Coroner's Inquests into the London Bombings of 7th July 2005: Government response to the Report under Rule 43 of the Coroner's Rule 1984.* [Internet] Available from http://7julyinquests.independent.gov.uk/docs/orders/rule43-report.pdf [Accessed 02/02/2012]

HMG (2006) *Report of the Official Account of the Bombings in London on 7th July 2005.* HC1087. London: TSO.

HMG (2007) *Building on Progress: Security, Crime and Justice*. HMG Policy Review 2007. London: Cabinet Office.

HMG (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy. Cm7953.* London: TSO.

HMG (2011) CONTEST *The United Kingdom's Strategy for Countering Terrorism July 2011. Cm8123*. London: TSO

Independent Chief Inspector of the UK Border Agency (2010) *Preventing and Detecting Immigration and Customs Offences: A Thematic Inspection of How the United Kingdom Border Agency Receives and Uses Intelligence*. London: HO 01785 ICIU

Her Majesty's Inspectorate of Probation (2006) *An Independent Review of a Serious Further Offence Case: Anthony Rice.* London: HMIP.

Intelligence and Security Committee (2012) *Introduction: About the Committee.* [Internet] 29/06/2012 <http://isc.independent.gov.uk/> [Accessed 29/06/2012].

Intelligence and Security Committee (2002) *Inquiry into Intelligence, Assessments and Advice Prior to the Terrorist Bombings on Bali 12 October 2002. Cm5724*. London: TSO.

Intelligence and Security Committee (2003) *Iraqi Weapons of Mass Destruction – Intelligence and Assessments. Cm5672.* London: TSO.

Intelligence and Security Committee (2005) *The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq. Cm6469.* London: TSO.

Intelligence and Security Committee (2006) *Report in to the London Terrorist Attacks on 7th July 2005. Cm6785*. London: TSO.

Intelligence and Security Committee (2009) *Could 7/7 have been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7th July 2005. Cm7617.* London: TSO.

Information Commissioner's Office (2012) *Homepage* [Internet] <http://www.ico.gov.uk/> [Accessed 30/06/2012].

IPCC (2005) 'Misconduct investigation arising from the circumstances surrounding the death of Jordan McGann (18 months) in August 2004 Professional Standards Department West Midlands Police managed by the Independent Police Complaints Commission.

IPCC (2006a) *Tania Moore investigation*. Press Pack issued at IPCC Press Conference in Derby on Wednesday 1st November 2006. IPCC.

IPCC (2006b) *Independent Investigation into the Police Response to the Report of the Abduction of Child A from her home in Rumney on 2 January 2006*. Restricted Redacted report. IPCC.

IPCC (2006c) *Independent Investigation into Devon and Cornwall Constabulary's response to enquiries regarding the welfare of Sally Ann Heppell, prior to her body being found on 10 April 2006.* IPCC.

IPCC (2007a) *Executive Summary: Investigation into how Greater Manchester Police were first Notified about the Shooting of Jessie James, what Actions were Taken and what Information was Disseminated to the Media and Public.* IPCC.

IPCC (2007b) *Executive Summary Independent IPCC Investigation of the Metropolitan Police Service's response to the stabbing of Peter Woodhams on 21 January 2006.* IPCC

IPCC (2007c) *IPCC Investigations into Complaints made Following the Forest Gate Counter-Terrorist Operation on 2nd June 2006.* IPCC (February 2007)

IPCC (2007d) *IPCC Independent Investigation into the Circumstances Surrounding the Death of Mr Sean Beard, aged 39 , from Burton on Trent Staffordshire Whilst in Police Custody at Burton on Trent Police Station, Staffordshire on 21st November 2005* IPCC Reference CTMS 2005/012545. IPCC.

IPCC (2008a) *Independent Investigation -Executive Summary Contact between Banaz Mahmod and the Metropolitan Police Service and West Midlands Police September 2005 - January 2006.* IPCC.

IPCC (2008b) *Investigation into the Death of Hayley Adamson.* CTMS 2008/007843. IPCC.

IPCC (2008c) *IPCC Concludes Stirland investigation*: Press Pack issued at IPCC Press Conference in Nottingham Friday 22nd February 2008. IPCC.

IPCC (2009a) *Commissioner's Report IPCC Independent Investigation: Greater Manchester Police contact with Katie Boardman prior to her death.* IPCC.

IPCC (2009b) *Learning Report: External Managed Investigation by Thames Valley Police into the Death of Michael Spencer Following his Release from Wiltshire Police.* IPCC.

IPCC (2009c) *Commissioner's Report IPCC Independent Investigation into the Metropolitan Police Service's Inquiry into Allegations against John Worboys.* IPCC.

IPCC (2009d) *Commissioner's Report Following IPCC Independent Investigation into Metropolitan Police Service Response to the Prison Recall Notification of Dano Sonnex.* IPCC.

IPCC (2009e) *IPCC Report into the Contact Between Fiona Pilkington and Leicestershire Constabulary 2004-2007 Independent Investigation Final* IPCC reference:2009/016872. IPCC

IPCC (2009f) *Operation Minstead.* Final report CTMS reference 2009/023127. IPCC

IPCC (2009g) Fiona Pilkington – Inquest Verdict

IPCC (2010a) *Independent Investigation Commissioners Report: Investigation into Contact with Lancashire Constabulary Regarding the Safety of Ms A on 7th September 2010* IPCC reference: 2010/017377. IPCC.

IPCC (2010b) *Independent Investigation into the use of ANPR in Durham, Cleveland and North Yorkshire from 23 - 26 October 2009*. CTMS: 2010/004924. IPCC.

IPCC (2010c) *Commissioner's report Independent Investigation into Police Contact with Joanna Michael Prior to her Death.* IPCC.

IPCC (2010d) *Independent Investigation into the Responses made by North Wales Police to Reports of Domestic Abuse by Karen McGraw*. IPCC.

IPCC (2010e) *Embargoed 0001HRS 11/03/10 Commissioner's Report IPCC Independent Investigation: Greater Manchester Police Contact with Clare Wood prior to her death.* IPCC

IPCC (2010f) *IPCC Commissioner's report IPCC independent investigation into the Metropolitan Police Service's inquiry into allegations against Kirk Reid.* IPCC.

IPCC (2010g) *Independent Investigation into Police Contact with Joanne Butler Prior to her Murder Independent Investigation Commissioner's Report* IPCC Reference: 2010/001715. IPCC.

IPCC (2010h) *Independent Investigation into the Fatal Shooting of Mark Saunders on 6 May 2008 Investigation Report.* IPCC.

IPCC (2011a) Suffolk Police Response to Call from Mary Griffiths and her Subsequent Murder – Independent Investigation Commissioner's Report. IPCC.

IPCC (June 2011b) *IPCC Position Statement: Risk in police-decision making and accountability in operational Policing.* IPCC.

Innes,M., and Sheptycki,J.W.E. (2004) From Detection to Disruption: Intelligence and Changing Logic of Police Crime Control in the United Kingdom. *International Criminal Justice Review, Volume 14, 2004, pp. 1-24.*

Innes,M. (2006) Policing uncertainty: countering Terror through community intelligence and democratic policing. *The ANNALS of the American Academy of Political and Social Science 2006; 605; pp. 222-228.*

Innes,M., and Roberts,C. (2006) Community Intelligence in the Policing of Community Safety.*University's Police Science Institute*, [Internet] (2006), pp 1-16. Available from: http://www.upsi.org.uk/resources/communityintelligenceandcommunitysafety.pdf [Accessed 19/03/2012]

James, A.(2011) Doctoral Thesis '*The Influence of Intelligence-Led Policing Models on Investigative Policy and Practice in Mainstream Policing 1993-2007: Division, Resistance* *and Investigative Orthodoxy'* (London School of Economics and Political Science) accessed on 12/03/2012 at http://etheses.lse.ac.uk/221/1/James_The_influence_of_intelligence-led_policing_models_on_investigative_policy_and_practice_in_mainstream_policying_1993-2007.pdf

James,A (2012) Forward to the Past: Reinventing Intelligence led Policing in Britain Unpublished: University of Portsmouth, pp. 1-24.

Jennings, L.J. (1894) *The Croker Papers: The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, LL.Dm F.R.S, Secretary of the Admiralty from 1809 to 1830.* Vol.III, p. 276

John,T., and Maguire,M. (2003) Rolling out the National Intelligence Model: Key challenges. In: Bullock,K., and Tilley,N. eds. *Crime Reduction and Problem-orientated Policing.* Cullompton, Willan Publishing, pp.38-68.

John,T., and Maguire,M. (2004) *The National Intelligence Model: Early Implementation experience in three police force areas.* Cardiff University, School of Social Sciences: Working Paper Series Paper 50.

Joyce,P.(2006) *Criminal Justice: An Introduction to Crime and Criminal Justice System. Policing: Methods, Structure and Organisation.* Cullompton: Willan Publishing.

Kitzinger,J. (1995) Introducing Focus Groups. *British Medical Journal* 311:,pp. 299-302.

Klaidman,D., and Isikoff,M. (2005) *Look Who's Not Talking – still'* [Internet] Daily Beast 03/05/2005 http://www.thedailybeast.com/newsweek/2005/04/03/look-who-s-not-talking-still.html [Accessed 16/07/2012].

Kleiven,M.E., and Harfield,C.(2008) Europol and the Understanding of Intelligence. In: Harfield,C., MacVean,A., Grieve, J.G.D., and Phillips,D. (eds) *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety.* Oxford: Oxford University Press, pp. 195-204.

Kotter,J.P. (1978) *Organizational Dynamics: Diagnosis and Intervention.* Reading, MA: Addison-Wesley.

Law Commission (2012) *Eleventh Programme of Law Reform Presented to Parliament pursuant to section 3(2)of the Law Commissions Act 1965. HC 1401*.London: The Stationary Office

Law Commission (2012b) *Data Sharing between Public Bodies* [Internet] The Law Commission. Available from: http://lawcommission.justice.gov.uk/areas/data-sharing.htm [Accessed 17/07/2012]

Laqueur,W (1985) *A World of secrets: The Uses and limits of Intelligence* New York: Basic Books.

Laurie,P (1970) *Scotland Yard* New York: Holt Rinehart and Winston.

Learmont Inquiry (1995) 'Review of Prison Service Security in England and Wales and the escape from Parkhurst prison on Tuesday 3rd January 1995 Cm3020 London: HSMO

Lincolnshire Police Authority (2005) *Scrutiny of Lincolnshire Police National Intelligence model – 2nd report* dated 20/01/2005 [Internet] Available from: http://www.lincolnshire-pa.gov.uk/downloads/library/356.pdf [Accessed 11/05/2012]

Lowenthal,M.M.(2009) *Intelligence: From Secrets to Policy* (4th edition) Washington DC: CQ Press.

McPherson,I., and Kirby,S.(2004) *Integrating the National Intelligence Model with a Problems Solving 'approach* London: Home Office.

Maguire,M., and John,T. (1995) *Intelligence, Surveillance and Informants: Integrated Approaches.* Crime Detection and Prevention Series Research Paper 64. London: Home Office.

Maguire,M., and John, . (2006) Intelligence-Led policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK *Policing and Society: An International Journal of Research and Policy,* Vol. 16:1, pp. 67-85.

Malterud,K. (2001) Qualitative research: Standards, challenges and guidelines. *The Lancet.* 358: pp.483-488.

Manning, P.K. (2008) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control* New York University Press: New York and London.

Marrin, S.(2009) Training and Educating U.S. Intelligence Analysts *International Journal of Intelligence and Counterintelligence* 22:1, 131-146.

Marrin,S.(2012) Evaluating the quality of intelligence analysis: By what (mis)measure? *Intelligence and National Security,* 27: 6, pp. 896-912, December 2012.

May,E.R.(1984), (ed) *Knowing one's enemies: Intelligence Assessment before the Two World Wars* Princeton, NJ: Princeton University Press.

Metropolitan Police Service (1985) *Probationers record* The Yellow Book. London:MPS.

Michaels, E.,Handfield-Jones,H.,and Axelrod,B,(2001) *The War for Talent Boston:* Harvard Business Press.

Mountbatten report (1966) *Report of the Inquiry into Prison Escapes and Security* (1966) Cmnd 3175 London: HMSO

Murphy,J.(2012) Letter to Chief Constables, Commissioners and Agency Directors from John Murphy QPM Chief Constable Merseyside Police, Head of Crime Business area. 'Review of National Intelligence Model and Processes. 10/08/2012.

NCIS (2000) *The National Intelligence Model* London: NCIS and Quantum Blue Limited publishing.

NPIA (2010) *Engage and Social Media Engagement for the Police Service* [Internet] NPIA. Available from: <http://www.acpo.police.uk/documents/LPpartnerships/2010/20110518%20LPPBA%20dm_engage_v61.pdf> [Accessed 19/08/2012]

Norris,C., and Armstrong,G. (1999), *The Maximum Surveillance Society: the Rise of CCTV*, Berg, Oxford and New York

Office of Surveillance Commissioners (2004) *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2003-2004.*London: TSO.

Office of Surveillance Commissioners (2012) *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012* .London: TSO.

Omand,D.(2010) *Securing the State.* London: Hurst and Company.

Orlikowski,W.J., and Baroudi,J.J. (1991) Studying Information Technologies in Organisations: Research Approaches and Assumptions. *Information Systems Research* (2) 1, pp. 1-28

Powell,R.A., and Single,H.M.(1996) Focus Groups. *International Journal of Quality in Health Care* 8 (5), pp. 499-504

Priest,D., and Arkin,W. (2010). *Top Secret America.* Dallas Morning.

Ratcliffe,J.H. (2008a) Intelligence-Led Policing. In: Wortley,R., Mazerolle,L., and Rombouts,S. (eds) *Environmental Criminology and Crime Analysis.* Cullopmton: Willan Publishing, pp. 263-278.

Ratcliffe,J.H. (2008b) *Intelligence-Led Policing*. Cullompton: Willan Publishing.

Richards, J. (2010) *The Art and science of Intelligence Analysis*. Oxford: Oxford University Press.

Security Service ('n.d.') *What is espionage?* [Internet] Available from: <https://www.mi5.gov.uk/output/what-is-espionage.html> [Accessed 14/08/2012]

Sheptycki,J. (2004) Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-led Policing. *European Journal of Criminology Volume 1 (3),* pp. 307–332.

Sherman,L.W. (1998) Evidence Based Policing. *Ideas in American Policing* Police Foundation July 1998, pp. 1-15.

Shulsky, A. (1995) What is intelligence? Secrets and Competition Among States. In: Godson,R., May,E,R, and Schmitt,G. (eds) *US Intelligence at the Crossroads: Agendas for Reform*. Washington: Brassey's, pp. 17-27.

Shulsky,A.N., and Schmitt,G.J. (2002) *Silent Warfare Understanding the World of Intelligence*. Dulles Virginia: Potomac Books,Inc.

Sims,J. (1995) What is Intelligence? Information for Decision Makers. In: Godson,R., May,E,R, and Schmitt,G. (eds) *US Intelligence at the Crossroads: Agendas for Reform*. Washington: Brassey's, pp. 3-16.

Sims,J (2007) Intelligence to Counter Terror: The Importance of All-Source Fusion. *Intelligence and National Security*, 22: 1, pp. 38-56.

Stevenson,C., and Cooper,N. (1997). Qualitative and Quantitative Research. *The Psychologist*, 10, pp.159–160.

Taplin,W.L. (1989) Six principles of intelligence. *International Journal of Intelligence and Counterintelligence* Vol.3, No 4, Winter 1989, pp.475-491.

Taylor,R.W, and Russell,A,L. (2012): The Failure of Police 'Fusion' Centers and the Concept of a National Intelligence Sharing Plan. *Police Practice and Research: An International Journal*, 13:2, pp. 184-200.

Thomas,R., and Walport,M. (2008) *Data Sharing Review Report.* London: Ministry of Justice. Available from www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf (Internet)

Tilley,N. (2008) Modern Approaches to Policing: Community, Problem-Orientated and Intelligence-Led. In: Newburn,T (Ed) *Handbook of Policing*. Cullompton: Willan Publishing, pp.373-403.

The Times (1875) *The Times* (20/09/1875)

US Congress (1955) *Commission on Organization of the Executive Branch of the Government* [the Hoover Commission], 'Intelligence Activities' June 1955, p.26.

US Congress (2004a) *National Commission on Terrorist Attacks Upon the United States* (2004 -also known as the 9-11 Commission)

US Congress (2004b) *Intelligence Reform and Terrorist Prevention Act 2004 Public Law 118 STAT. 3638 108-458 Dec. 17, 2004 108th Congress.*

US Senate (1947) *Committee on Armed Services. Hearings on the National Defence Establishment* 1st session,1947', pp525-528 as recounted in Grose, P, Gentleman Spy: The Life of Allen Dulles (Boston: Houghton Mifflin, 1994), p275

US Department of Justice (2003) *The National Intelligence Sharing Plan* Third Printing 07/05

US Government (2010) *National Security Strategy* (2010) Washington. D.C.: White House

Van Duyne,P.C. (1999) Mobsters are Human Too. In: Canter,D., and, Allison,L. (eds) *Offender Profiling Series* Vol. 2. Farnham, Surrey: Ashgate Publishing.

Walters,V. (1978) *Silent Missions.* Garden City, NY: Doubleday, 1978.

Ward,L. (2007) ***330,000 users to have access to database on England's children***. [Internet} 18/06/2007. Available from *The Guardian* (2007) <330,000 users to have access to database on England's children> [Accessed 22/04/2011].

Warner, N (2012) *'ASIS at 60'* (Speech on 19/07/2012 by the ASIS Director General as part of the Lowy Distinguished Speaker Series) <http://www.asis.gov.au/about-us/speech.html> accessed 13/08/2012).

Watson,A. and Bessant,C. (2009) Information Sharing and Data Protection. In: *The Information Sharing Handbook*. London: Law Society Publishing.

Wax,R. (1971) *Doing Fieldwork.* Chicago: University of Chicago Press.

Weber,M., (1947) *The Theory of Social and Economic.* translated by Henderson,A.M., and Parsons,T (eds). New York: Oxford University Press

Weber,M. (1978) *Economy and Society* translated by Ross, G., and Wittich,K. London University of California Press

Weisburd, D., and Eck, J. (2004) What can Police do to Reduce Crime, Disorder, and Fear?' *The Annals of the American Academy of Political and Social Science*, 593:1, pp. 43-65.

Wilkinson, S. (2010) Research and Policing: Looking to the future. *Policing*, Vol. 4, No. 2, pp. 146-148 Oxford: Oxford University Press.

Wilensky, H.L. (1967) *Organizational Intelligence*. New York/London: Basic Books.

Williams,A. (2010) An epistemological chasm? Acturial risk assessment through OASys. In: Nash,M., and Williams,A. (eds) *Handbook of Public Protection*. Cullompton; Willan Publishing, pp133-161.

Wimmer,R.D., and Dominick, J.R. (1997) *Mass media Research: An introduction*. Belmont, MA: Wadsworth.

Zahid Mubarek Inquiry (2006) Volume 2 HC 1082II London: TSO.

Zegard,A.B. (2007) *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, New Jersey: Princeton University Press.

Appendix: C Research Degrees Sub Group
April 2012

Student's Declaration Form **Form RD10 (Decl)**

LONDON
metropolitan
university

Note: This form must bound into each copy of your thesis, plus a copy to be submitted to the Research & Postgraduate Office.

1. The student

Name of student: **Ian Stanier**

Degree for which thesis is submitted: Professional Doctorate

Title of Thesis (please insure grammatical accuracy): *Contemporary organisational pathologies in police information sharing: new contributions to Sheptycki's lexicon of intelligence-led policing.*

I have fulfilled the minimum period of registration for PhD (36 months PT)

Will you require a pc and projector for the viva examination? No

2. Statement of related studies undertaken in connection with the programme of research:

Not applicable

3. Concurrent registration for two or more academic awards:

* I declare that while registered as a student for the University's research degree, I have not been a registered student or enrolled student for another award of a UK university or other academic or professional institution.

4. Material submitted for another award:

* I declare that no material contained in the thesis has been used in any other submission for an academic award

5. Ethical Approval

I declare that my research complies with UK legislation governing research (including that relating to health and safety human tissues and data protection).

6. Supervisory Approval

I am submitting my DProf thesis *with the approval of my supervisory team.

Signature of Student .... Date 20th August 2012.

Appendix: D

Endnotes

[i] Sheptycki's eleven pathologies are digital divide; linkage, blindness; noise; intelligence overload; non-reporting; intelligence gaps; duplication; institutional friction; intelligence-hoarding and information, silos; defensive data concentration; and the differences of occupational subculture (Sheptycki, 2004).

[ii] The National Intelligence Model (NIM) introduces three criminal operating levels. *Level 1* concerns crime and disorder contained or managed within a police forces Basic Command Unit (BCU) and usually this can be dealt with using the BCU own resources. *Level 2* concerns criminality that crosses BCU's and / or Force areas. It usually reflects a level of criminality that would require the BCU to bid for additional resources to assist it in tackling the crime problem. *Level 3* concerns serious and organised crime that has a national and on occasions an international reach. There is often a requirement, at *Level 3*, for high end policing tactics including covert policing deployments.

[iii] The most well known are the US Congress (2004) *National Commission on Terrorist Attacks Upon the United States* (2004 -also known as the '9-11 Commission') and in the UK the *'Review of Intelligence on Weapons of Mass Destruction'* (2004 - commonly known as the 'Butler Report'), *Intelligence and Security Committee*'s *'Could 7/7 have been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7th July 2005* and the *Coroner's Inquests into the London Bombings of 7th July 2005* Report under Rule 43 of *The Coroner's Rules 1984.*

[iv] For details of Police Blog websites see http://www.vnunet.com/vnunet/news/2151977/police-blogs-shut-fears-careers accessed on 12/11/2011. It is accepted that these may not be some of the most reliable of sources due the difficulty in corroborating what was in effect an anonymous source reporting. Nonetheless, they can provide a degree of insight especially when triangulated with other source material.

[v] *McCann v UK* relates to the killing, by the SAS, of a Provisional IRA (PIRA) active service unit who were planning a bombing in Gibraltar. The ECrtHR (application 18984/1991) supported the actions of the soldiers based on their understanding of intelligence about the PIRA Unit and the methods it employed including the use of remote detonators. The breaches, that were found, centred on the use of the intelligence by the Authorities, i.e. were there opportunities for a non lethal intervention of the PIRA team earlier on in the attack planning? The UK was also criticised for not considering the correctness of the intelligence (which turned out to be incorrect) and finally the use of SAS who were trained to kill rather police officers which was considered a procedural failure. The full judgement can be found at: http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695820&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

[vi] Executing arrest warrants at wrong addresses is not uncommon. The reasons vary but often it is associated with information not being verified, the use of out-of-date information or inadequate planning. For examples See http://www.metro.co.uk/weird/33397-police-raid-wrong-house and http://www.edp24.co.uk/news/crime/pensioner_injured_after_armed_police_raid_wrong_house_1_902695

And http://www.mirror.co.uk/news/top-stories/2011/03/21/bungling-cops-raid-wrong-home-for-41st-time-115875-23004407/ Both accessed on 29/12/2011

[vii] In 2011, a large UK Metropolitan Force discovered that over 80% of its officers and staff were 'locked out' of their intelligence system with the consequence they could neither directly record, update or search their force intelligence systems.

[viii] Powers under Section 67 of the *Criminal Justice and Court Services Act 2000* ensured that 'responsible authorities worked together under what is known as MAPPA arrangements. This ensured cooperation between police, probation and the prison service. Provisions were re-enacted under section 325 of the *Criminal Justice Act 2003.*

[ix] The first national programme charged with the creation of a national accessible police intelligence system was known as the IMPACT programme which was formally closed in 2011 with the introduction of the Police National Database (PND).

[x] The content of the *Thematic Reviews* are classified as GPM 'Restricted' as they contain information on sensitive policing methods and provide an assessment of common operating standards of police

intelligence officers working within prison establishments. These Reviews are undertaken by Police Advisors (operating within the *National Offender Management Service* (NOMS) Security Group.

[xi] The Author attended a joint Police – Probation conference in central England in 2011. A presentation on information sharing within public protection partnership arrangements devoted 55 minutes of the 60 minute delivery addressing potentially problems and concerns associated with sharing and gave scant comment to the benefits of wider information exchange.

[xii] See The Times (22/1/13) *'Justice works across borders without Brussels'* by Dominic Raab (Conservation MP for Esher and Walton) In his article he reinforce the view that data-sharing is automatically bad in that he states *'but the proposal to sign up for pan European data-sharing on every citizen is Orwellian and dangerous'*.

[xiii] John and Maguire (2004) in Working Series Paper Number 50 *'NIM: Early implementation experience in three police force areas* have inaccurately described the NIM as being developed by the *National Criminal Intelligence Service (NCIS).* It was actually developed by a number of different ACPO forces and NCIS under the ACPO Intelligence portfolio and subsequently published under NCIS branding.

[xiv] Intelligence has always informed police activity. *The Times* (20/09/1875) reported that during the Whitechapel murders, linked to 'Jack the Ripper' murders, police were able to identify witnesses after being in receipt of 'intelligence'. For more examples of 18th and 19 century intelligence use see Emsley,C,. and Shpayer-Makov,H (2006) *Police Detectives in History, 1750-1950.*Gateshead: Ashgate.

[xv] In April 2012, *Police Advisers Section* (PAS) was merged into the newly formed *Operational Partnership Team* (OPT) located within NOMS Security Group. The name change reflected the multi-agency nature of the team which now included UKBA, HM Revenue and Customs and SOCA. Only two junior ranked police officers remain within the OPT with no direct police link into strategic forums. The OPT are 5responsible for overseeing the ACPO-HMPS *Memorandum of Understanding for the exchange of information.*

[xvi] It is interesting to note that this capability and capacity gap was reinforced in 2005 through the introduction of *HMIC Closing the Gap report*. This report recommended the merger of the existing 43 forces into small more strategic forces in order that it could effectively deliver protective services and deal with Level 2 criminality.

[xvii] Two models are prominent here. The first being *Intelligence Led Policing* which originated in a recognisable form in the 1990s in the *Kent Policing Model* and became more nationally embraced with the introduction of the National Intelligence Model. The second, Problem Orientated Policing (POP), a term coined originally by Herman Goldstein (Goldstein, 1979), which became more mainstreamed within UK policing in the late 1990's.

[xviii] The card index of local thieves was apparently maintained in each Criminal Investigations Department (CID) office in the 1920's. (See Grieve (2004) Developments in UK Criminal Intelligence. In: Ratcliffe,J.H. (ed). *Strategic Thinking in Criminal Intelligence.* Sydney: The Federation Press, pp. 25-36.

[xix] The Codes of Practice on the Management of Police Information were eventually prepared by the NCPE and published in July 2005. The codes were made by the Secretary of State for the Home Office under sections 38 and 39A of the Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997.

[xx] The ACPO/NPIA/NCPE produced doctrine on a range of issues including *Regional Tasking* (2004), *Tasking and Co-ordination* (2007) the *National Intelligence Model* 2005), a codes of practice on the NIM (2005), *Guidance on the Management of police Information* (2006 and 2010), *Guidance on the National Briefing Model*(2006), *Retention guidance on nominal records for the Police National Computer* (2006) ACPO *Practice Advice on Tasking and Co-ordination (2006),* ACPO *Practice Advice on Resources and the People Assets of the National Intelligence Model (2007).* ACPO *Practice Advice: Introduction to Intelligence Policing* (2007), ACPO *Data protection: Manual of Guidance (2006)* and *Practice Advice on Analysis* (2008).

[xxi] The Thematic Review of police Prison Intelligence Officers (PIO) was undertaken by the Author (12/01/2012 – 15/06/2012) in prisons located within two large multi-force regions in England & Wales.

[xxii] One serving prisoner was discovered to be arranging multiple drug importations from his prison cell. This involved him contacting, via an illegal telephone, another prisoner held in a Central American high security prison. For more details see *The Guardian* (2009) *Jailed drug dealer gets 18-year sentence for running cocaine ring from his cell* 18/08/2009 http://www.guardian.co.uk/uk/2009/aug/18/drug-dealer-cell-cocaine-ring (accessed 19/03/2012)

[xxiii] A recent example of an intelligence unit involving police, public authorities and the private sector is the *National Fraud Intelligence Bureau* (NFIB) which offers a centralised body to co-ordinate fraud intelligence across the public and private sectors. Launched in 2010, the NFIB representing industry, commerce and government was developed and overseen by the *City of London Police* as part of its role as a national lead on fraud. The *NFIB* employs analysts from both the law enforcement and private sector to undertake analysis of raw data and where patterns emerge of criminality, share the information with the relevant police force for investigation.

[xxiv] *The Office of Surveillance Commissioner* oversees covert human intelligence source use, directed and intrusive surveillance and the *Office of the Interception Communication Commissioners* oversee mail and telephone interception.

[xxv] Statement in conversation with John Crocker and Crocker's wife (04/09/1852), as quoted in *The Croker Papers: The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, LL.Dm F.R.S, Secretary of the Admiralty from 1809 to 1830* (1884), edited by Louis J. Jennings, Vol.III, p. 276

[xxvi] Authors own records: One Urban force records nearly 900,000 reads a day against vehicle's registration numbers moving around its Force area including over 30,000 'hits' against databases. The majority of these related to vehicle related interest reports including no insurance, no MOT or no vehicle excise license and approximately 500 related to *'crime'*.

[xxvii] The system now in place in the *National Offender Management Service* is called C-NOMIS, a national system linking probation and prison. However this system is not installed within police forces so written requests for information have to be made on an individual basis to NOMS.

[xxviii] The ISC is an independent parliamentary body, set up under the *Intelligence Services Act 1994*, whose role is to examine the work of the intelligence and security Agencies – MI5 (officially known as the Security Service), MI6 (officially known as the Secret Intelligence Service) and the Government Communications Headquarters (GCHQ). The ISC consists of eight MPs and one Member of the Lords – drawn from the Labour, Conservative and Liberal Democrat party – and is given access to a wide range of the Agencies' secret material.

[xxix] An unclassified, previously secret, report published in 2009 reviewed the failure to share intelligence in the USA prior to 9/11. The report *'Legal barriers to information sharing: The erection of a wall between intelligence and law enforcement investigations'* 9/11 Commission Staff monograph by Barbara A Grewe, Senior Counsel for Special Projects dated 20/08/2004 concluded *'It is clear therefore, that the information sharing failures in the summer of 2001 were not the result of legal barriers but of the 'failure of individuals to understand that the barriers did not apply to the facts at hand.'* Simply put, there was no legal reason why the information could not have been shared. (Grewe, 2004, p.35) http://www.fas.org/irp/eprint/wall.pdf accessed on 13/06/2012

[xxx] The *Law Commission* was established under the *Law Commissions Act 1965*. It is a statutory independent body whose purpose is to keep the law under review and to recommend reform where necessary.

[xxxi] The Government Protective Marking System (GPMS) comprises of five markings in descending orders of sensitivity; *Top Secret, Secret, Confidential, Restricted* and *Protect*. The scheme is used to protect information from inappropriate dissemination or access.

[xxxii] Preeminent amongst police intelligence 'champions' were Sir David Phillips QPM the Chief Constable of Kent (1993 to 2003) and ACPO President (2001 to 2003). His Force were the first to embrace and implement intelligence led policing laying down the foundation of the *National Intelligence Model.* Professor John Grieve CBE QPM, was the head of the Metropolitan Police Service's SO13 Anti-Terrorist Branch and its first dedicated Director of Intelligence. He was responsible for the Systems for Detection (SID Project) which transformed the organisation's intelligence approach to one based on an offender focus.

[xxxiii] Micawber, a character in Charles Dickens' novel *David Copperfield* known for his belief that 'something will turn up'. Interestingly, the failure of the British Government to predict the Argentinean invasion of the Falkland Islands in 1982 and its approach to the issue of sovereignty claims was characterised by the British Ambassador in Buenos Aires as a Micawberism (see Hansard *'Falkland Islands Review'* (Cmnd. 8787.)

HL Deb 25 January 1983 vol 438 cc136-247) retrieved 15/06/2012.

[xxxiv] The concern that *Police and Crime Commissioners* (PCC) will focus only on the issues directly impacting on their electorate and marginalise its regional and national policing contributions and responsibilities has been recognised by the Home Office. It has attempted to address this by publishing

the *Strategic Policing Requirement (SPR)* to ensure PCC take into account both the national and local policing requirements and ensure the availability of sufficient capability and capacity to support efforts at both levels. *Home Office Strategic Policing Requirement (*July 2012)

[xxxv] The Authors research revealed that since November 2010 to April 2012, the number of national Police Intelligence officers (PIO) deployed in prison has fallen from 140 to 90 with a further reduction anticipated of 15. One metropolitan police force has reduced its Source handlers from 90 Handlers to less than 30 in five years while also halving its surveillance teams.

[xxxvi] The author's research revealed forces where the criteria for positions within intelligence were based solely on officer restriction. This term 'Restricted Officer' is used to refer to an officer who, for an array of medical or disciplinary reasons, is not fully deployable on the street. One force actively moved intelligence officers from the department to make vacancies available for restricted officers. On three occasions during the research, police internal adverts for intelligence roles were published limiting the applicant pool to 'Restricted Officers'.

[xxxvii] 'Restricted' officer status is a classification of an officer's ability to be deployed operationally. It includes restriction based on a short term and permanent medical conditions.

[xxxviii] The powers under *Police Pension Regulations 1987*: 'Part A General provisions and retirement: *A19 ' Compulsory retirement on the grounds of efficiency of the Force'* have been used by English and Welsh police forces to deliver cost cutting requirements.

[xxxix] An ACPO respondent at interview stated that 'policing *in this area is hampered, to address it we need intelligent police in intelligence roles, it has to shed itself of the perception that the 'lame, sick and the injured' dominate police intelligence communities'*.

[xl] Although even this initiative was criticised in the UK by the Britain's Association of Social Anthropologists president, John Gledhill called the scholarships 'ethically dangerous and divisive'. He told the BBC News website the scholarships could foster suspicion within universities worldwide and cause problems in the field. See BBC *'Fears over CIA 'University Spies'* 02/06/2005 http://news.bbc.co.uk/1/hi/4603271.stm accessed 03/03/2012

[xli] The Police College (for England Wales) has taken on some of the functions of the NPIA including learning, development, curriculum and strategy, authorised professional practice, exams and assessments, international academy, and the National College of Police leadership.

[xlii] A review by the Author of three ACPO covert doctrine documents revealed much of the content was already publically available (and originally taken from open public sources), could be easily assumed from a review of academic material, case law, legislative provisions and inquires all drawn from open source. Even tradecraft is widely predictable and on occasions, can be more informative in open source material.

[xliii] It has been reported that in the USA that there are 1931 private organisations working alongside 1271 government organisations involved in delivering homeland security, intelligence collection and counter-terrorism. See Taylor and Russell (2012), The failure of police 'fusion' centers and the concept of a national intelligence sharing plan, *Police Practice and Research: An International Journal*, 13:2, 184-200 Routledge Taylor and Francis group