Journal of Economic Criminology 7 (2025) 100133

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

Following the money: Evaluating evidence gathering using financial investigation in the world of covert human intelligence source handling

Craig Hughes[a], David Kennedy[b], David Hicks[c,*]

[a] Former Head of Policing, University of Derby, DE1 1DZ, United Kingdom
[b] Lecturer in Policing, University of Derby, Derby DE1 1DZ, United Kingdom
[c] Senior Lecturer in Criminology, University of Derby, Derby DE1 1DZ, United Kingdom

ARTICLE INFO

Keywords:
Covert human intelligence sources (CHIS)
Financial investigation
Financial footprint organised crime groups (OCGs)
Intelligence-led policing

ABSTRACT

This research examines the possibilities for covert human intelligence sources (CHIS) handlers to gather financial intelligence against organised crime groups (OCGs). The focus will be on the financial footprint left by individual offenders and criminal enterprises for the purpose of targeting one form of the proceeds of crime, cash. The paper considers the practical utility of financial investigation techniques for routine use outside of the specialist area of asset recovery and confiscation. This is intended to provide balance with the traditional CHIS focus on commodities such as drugs, stolen goods, and firearms or evidence of serious offending such as murder or terrorism. After discussing existing policy, practice and research, the core method used in the paper involves primary research gathered by way of Freedom of Information (FOI) requests to all United Kingdom (UK) police forces. Analysis and discussion of that data illustrates that a substantial majority of forces varying exemptions cited under the FOI rules The authors assess the received data and information and offer further critical analysis of the force rationales for non-disclosure. Currently, the situation concerning the use of financial investigation techniques and CHIS remains unanswered. Financial gain is a strategic priority for OCGs and most offenders but, strangely, financial investigation is not a strategic priority for intelligence-led and evidence-based UK policing.

Historically, the use of covert human intelligence sources (CHIS) has predominantly focused on identifying particular commodities such as drugs, stolen goods, and firearms or evidence of serious offending such as murder or terrorism. There is a gap in the literature and professional practice in applying CHIS to routinely identify the financial footprint left by individual offenders or structured organised crime groups (OCGs). This research examines the possibilities for gathering CHIS intelligence against criminal enterprises for the purpose of targeting one form of the proceeds of crime, cash. The balance between a commodity versus cash and financial footprint orientation will be considered in the context of definitional and perceptual issues among policy makers and investigators. It is likely that the financial minutiae left by offenders is largely unguarded and this paper therefore considers the potential for CHIS handlers and their supervisors to utilise the financial footprint to target criminal cash and evidence more effectively. This approach considers the practical utility of financial investigation techniques for routine use outside of the specialist area of asset recovery and confiscation. This article first sets out the existing policy and practice for source handling and financial investigation application. It then moves on to analyse and discuss primary research gathered by way of Freedom of Information requests to all United Kingdom (UK) police forces.

Specifically, this paper will consider the concept of the financial footprint and its potential to be advantageously and routinely exploited by CHIS handlers, an area of evidence-based policing which appears to be under-researched. It seems that to date, research (Moffet et al., 2022; Scott, 2022) has concentrated mainly on the procedures for deployment of CHIS, any wrongdoings by law enforcement, using children as intelligence sources, all with a commodity focus as discussed above. There is little evidence to suggest a wider application of financial investigation in the deployment of CHIS or within the training and practice of CHIS handlers. It is currently unclear whether CHIS handlers routinely focus on identifying cash arguably regarded as a side issue to identifying the commodity under investigation. The structure of the paper will address CHIS handling, practice, historical background, and framework. It will then focus on financial investigation and intelligence and its links to the methods for this study. It will then address the FOI requests with an overview, analysis of refusals, consideration of the

* Correspondence to: Department of Criminology and Social Sciences, University of Derby, One Friar Gate Square, Derby DE1 1DZ, United Kingdom.
E-mail address: d.hicks@derby.ac.uk (D. Hicks).

https://doi.org/10.1016/j.jeconc.2025.100133
Received 30 August 2024; Received in revised form 20 December 2024; Accepted 7 February 2025

public interest test and general issues. The conclusion discusses the benefits and limitations of the project to highlight pathways for future research in this area.

Covert human intelligence sources (CHIS)

CHIS handling is regarded as a specialist area of law enforcement. Strict procedures are in place to prevent elements of mishandling individuals traditionally regarded as "informants" and attempting to prevent illicit behaviour which is known to have occurred in past policing activities (Home Office, 2022). Some aspects of CHIS handling have been subject to academic research, such as telephone interactions between handler and CHIS (Nunan et al., 2022), examining source handler considerations when dealing with the CHIS (Moffet et al., 2022) and attempts to identify the strengths or weaknesses of established practices (Atkinson, 2019). There is very limited research around the field of asset recovery, and any cross over into the sensitive world of CHIS handling.

Covert human intelligence source handling

In the UK, a CHIS is defined by section 26(8) of the Regulation of Investigatory Powers Act (2000) (RIPA) as "individuals who establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within Section 26(8)(b) or (c); who covertly use such a relationship to obtain information or to provide access to any information to another person; or

who covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship."

When reference is made to the connection between a CHIS and handler, a relationship is defined as being established or maintained for a covert purpose if, and only if, it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose (RIPA: 26 (9b). The handler may have various authorised purposes for the relationship but will keep the underlying purpose from the CHIS.

A further definition was added in 2013, under the RIPA (Covert Human Intelligence Sources: Relevant Sources) Order, whereby a source (now referred to as a "relevant source") who holds a position or rank in a public service, requires enhanced authorisation parameters. The term "Relevant Sources" refers to undercover police officers. Undercover officers, whilst technically CHIS, operate in a significantly different tactical environment. Their activities are not considered in this article. This article focuses on the activities of members of the public who are recruited into the CHIS role.

Current CHIS practice

This section explores the hypotheses that CHIS intelligence gathering practices are at best, opaque, and that the CHIS tactic is not used significantly to assist the gathering of financial criminality intelligence other than asset identification in some instances.

It is the epistemological experience of the authors that current intelligence evaluation structures do not encourage prioritising activity against financial criminality (College of Policing, 2024; Hughes and Hicks, 2025; NPCC Homicide Working Group 2021). There is a lack of training and knowledge amongst intelligence staff regarding financial investigation and that there is a reluctance to place CHIS at risk to gather financial data.

The CHIS tactic is one of the oldest and most successful covert tactics in history. There is evidence that the ancient Egyptians relied on 'spies in the enemy camp' to give them military and economic advantages (Crowdy, 2011). It is a simple tactic that requires no technology. It requires fewer resources than alternatives such as surveillance. It is a tactic that can gather and relay information 24 h a day.

The current UK CHIS environment has its origins in the 1990s with the creation of the National Intelligence Model (NIM) (CoP, 2024).

Historical background

Until the 1990s, UK police forces relied heavily upon the 'reactive', local response policing model. In the 1990s, the NIM was adopted due to a frustration with the lack of proactive, intelligence led policing and a desire to utilise technological developments. The increased use of computers by the police in some areas in the 1990s, created more effective data generation, collation and analysis. This resulted in a nationwide improvement of intelligence submission, recording and assessment.

In 1998, the Crime and Disorder Act placed information sharing responsibilities upon police forces and local authorities (LA), further extending the available data silos for crime and intelligence assessment.

The NIM flourished in this new computerised, data rich environment. It required intelligence data to be assessed by Intelligence Unit Analysts, who identified and evaluated operational risks and vulnerabilities. These intelligence products gave senior police managers the sound, evidence-based foundation upon which to allocate their resources and move beyond the traditional response policing model.

The NIM's quasi-scientific approach to intelligence assessment and analysis, also provided senior police managers with a consistent and largely predictable intelligence risk assessment structure. It has become a crucial, objective basis for management decisions.

NIM intelligence gathering is neither straightforward or uniform between policing areas. A brief study of police forces' current intelligence gathering priorities as listed on their public websites, indicates that there are many common themes. For example, Kent Police's priorities are, violence against women and girls, serious violence and harm, organised crime and exploitation. Leicestershire Police's priorities are drug, related crime, rape, child sexual exploitation, modern slavery and domestic abuse. Derbyshire Police's (more numerous) priorities are child abuse and sexual exploitation, residential burglary, rape and serious sexual offences, domestic abuse, modern slavery, county lines, killed and seriously injured on the roads, fraud and cyber-dependent crime, organised crime and vulnerability.

It is worth noting that fraud only appears in Derbyshire's list and this would not have been included had that force also limited itself to 4–5 priorities. Further research is required to assess accurately whether financial crime appears in the top 4–5 intelligence priorities nationwide, but the authors' experience is that this is very rare. Financial crime is itself a misnomer with regard to CHIS and routine policing. The tenet of following the financial footprint applies to all of the objectives cited. Individuals generally lead domestic lives contemporaneous with their criminality. While they may protect criminal earnings, they may not be so alert with everyday expenditure, and therein lies a weakness to be exploited. It raises a question for CHIS deployment and whether a review of the perceptions of what CHIS are being asked to achieve is required.

CHIS framework

The CHIS tactic aligns well with the NIM's structured approach to intelligence gathering. When NIM assessments identify risks such as gun crime as medium to long term key risks, Dedicated Source Handling Units (DSHUs) generate detailed plans to recruit gang members with knowledge of those issues. Because NIM assessments are predictive, DSHUs also create recruitment plans that address the 'next generation' of CHIS, ensuring that the flow of CHIS intelligence remains unbroken.

DSHUs aim to have several CHIS able to report on any given priority and when they can no longer report, those on the list of potential and reserve CHIS can be approached. This newly professionalized, analyst based, intelligence environment, greatly supported the deployment of covert tactics at a time when the legal environment became more

demanding, due to the introduction of the Human Rights Act 1998 (HRA).

The HRA brought the European Convention on Human Rights (ECHR) into UK domestic law. Drawing heavily from social contract theory, it defined the fundamental relationship between the state and its citizens (Hoffman and Rowe, 2013). Article 8 of the ECHR addresses the limits of state intrusion into citizens' private lives:

"Everyone has the right to respect for his private and family life, his home and his correspondence".

However, this is not an absolute right. Article 8 (2) confirms that the state can interfere with the right to a private life so long as it is properly authorised by law and is necessary to protect the basic needs of a democratic society. Because they gather information covertly through private relationships, CHIS directly interfere with the private lives of citizens.

Like other intrusive police activity, the CHIS tactic must operate within the lawful limitations of Art 8 (2). The Regulation of Investigatory Powers Act 2000 (RIPA) created a legal framework for the authorisation and lawful use of CHIS. If properly authorised, a section 29 RIPA authority satisfies this 'in accordance with the law' aspect of the HRA/ECHR.

RIPA and its accompanying Code of Practice created a statutory definition of CHIS (s26(8)) and a comprehensive legal framework for their operation. The newly professional and 'objective' intelligence environment greatly assisted authorising officers (AO) when they addressed and defined concepts such as 'necessity and proportionality'; essential when considering whether CHIS activity satisfies Art 8 (2) ECHR.

Whilst RIPA sets the lawful framework for CHIS operations, the day-to-day management of CHIS is governed by a Code of Practice (2022). Such are the risks associated with CHIS, only specialist officers from a DSHU are used.

This article seeks to address why there appears to be an apparent lack of CHIS engagement with financial investigation. We have already identified that the NIM model, focussing as it does on high-risk issues that cause the greatest direct harm, does not prioritise financial matters. This gap is illogical given the near universal acknowledgement that financial gain is the underlying cause of most serious and organised crime (HM Government, 2023) and there is growing agreement that the seizure of criminal proceeds is a vital aspect of law enforcement. It is also true that financial lifestyle (beyond asset recovery), is just as vital and may expose weaknesses that traditional methods of tasking and investigation may miss (Hughes, 2021; Hughes and Brown, 2022).

Forces must choose between allocating resources to tackle issues such as imminent weapon enabled, gang related violence, which may result in death or serious injury, or the indirect risks associated with criminal profits. This is again an instance where following the financial footprint, if correctly tasked and understood, can play a vital and as yet, apparently little used role.

Forces that fail to address imminent violent crime are likely to suffer an increase in gang violence, draw adverse publicity, suffer reduced community confidence and in the most severe circumstances, could be subjected to criminal investigation.

Failure to address financial crime rarely leads directly to the same severe outcomes. Financial crime often relies on structures and processes that change little and slowly, giving the impression that there is no urgency to address them in the absence of a specific risk of harm. This may be why the tenet of following the financial footprint to provide evidence rather than locate assets for recovery (confiscation), is confused as being the same thing and therefore little used (if at all).

Part 2 of the Major Crime Investigation Manual (2021), an NPCC comprehensive guide for Senior Investigating Officers (SIOs), identifies 14 key strategic areas for Senior Investigating Officers to consider. Financial investigation is not included despite the recognition (HM Government, 2023) that financial gain is a strategic priority for serious and organised criminality.

Traditional financial investigation often involves the assessment of large data sets and numerous court attendances for orders and injunctions and may thus be perceived as more burdensome to conclude than prosecutions for other forms of serious crime. SIOs tasked with dismantling and prosecuting drugs networks usually favour the familiar opportunity to identify and seize drugs and weapons directly. Prosecutions of this kind attract significant sentencing powers and SIOs generally consider financial offences as secondary legal action. Cash detention deployed using the Proceeds of Crime Act (2002) however, offers an effective and often under-used tactic. Whether this is effectively integrated within the CHIS environment is currently unknown. Historically, law enforcement have tended to focus on commodities rather than using aspects of legislation perceived too complex and specialist beyond their own remit (HMCPSI et al., 2010; HMIC et al., 2004; Hughes, 2021).

The deployment of a CHIS into any crime network is a high-risk undertaking. If compromised, a CHIS may experience social exclusion and displacement or in serious instances, a direct threat to their life. For this reason, CHIS should only be managed and operated by a properly trained DSHU.

DSHU staff are initially drawn from rank-and-file officers. They may be Detectives or Police Constables but are likely to have a background in Intelligence gathering. They are unlikely to be specialist Accredited Financial Investigators (AFIs) who, given the high cost and duration of their training, are usually discouraged from changing their career paths. It is unclear whether DSHU recruits have any awareness of financial investigation intervention possibilities including cash detention as well as feeding into, and drawing upon, the voluminous Suspicious Activity Reports (SARs) regime. SARs refers to confidential information mandatorily provided to the National Crime Agency (NCA) by the financial industry and regulated sector under the Proceeds of Crime Act (2002) and Money Laundering Regulations (2007) as amended.

DSHU staff work in a covert environment due to the sensitive nature of their work. This physical separation encourages a culture of 'isolationism' in which external policing developments, such as financial investigation, can be overlooked or considered unnecessary. Consequently, we would expect that there are few DSHU staff with any specialist financial investigative experience. This is also true of uniform and CID departments (Hughes, 2021). Skills and knowledge (if any) will usually be limited to a basic understanding of money laundering and (possibly) asset recovery (confiscation) powers generally contained within the Proceeds of Crime Act 2002.

To address this potential knowledge and skills gap, forces could consider whether their DSHUs employ an AFI within their structure, to capitalise on their specialist knowledge and to identify and maximise opportunities to gather intelligence on financial footprints. It may also assist better integration of skillsets if CHIS handlers had basic understanding of more routine financial investigation techniques as well as managers understanding what is available tactically when considering CHIS deployment.

As previously stated, modern UK money laundering legislation originates from 2002. Digital communications technology also started to evolve in this period, but it has evolved and been embraced by law enforcement, very differently. Investigations involving digital communications remain largely with rank-and-file officers. Specialist officers merely process the requests and report the findings. Whilst complex digital cases may require the assistance of an analyst, most digital communications data evidence remains the responsibility of the investigating officer. This contrasts strongly with financial investigation which remains largely the responsibility of specialist officers and AFIs. Financial investigation (in terms of assets recovery skillsets) remains a specialist discipline for good reason. It is complex and requires accreditation. Gathering financial footprint intelligence is not subject to these restrictions, it requires less specialist knowledge, and is accessible to all UK law enforcement. It is unknown as to any extent of involvement of CHIS in the digital environment.

The authors do not intend to address the issue of the evidential use of CHIS material in this section. There are too many complicating factors that require more detailed attention than can be afforded here.

CHIS often involve themselves on the periphery of the crime they are infiltrating, to be well placed to gather accurate information. Ideally they should not place themselves in the criminal evidential chain, otherwise prosecution of that issue can create compromise risks. But it is not uncommon for CHIS to unwittingly appear on surveillance footage or to have their fingerprints identified at scenes of crime, due to their close links to criminal networks. Financial investigation, heavily reliant as it is on auditable enquiries, is unforgiving to those identified within the evidential chain and is therefore a high-risk CHIS environment.

Financial investigation and intelligence

Financial investigation is a term which is not yet defined by United Kingdom (UK) legislation but, largely due to its drug trafficking related origins, has long since been perceived at all levels to be linked to asset recovery or confiscation (Brown et al., 2012; Hughes and Brown, 2022). This paper does not dispute the application of financial investigation in crime control measures as part of a policy to target the illicit gains from crime and remove them from the criminal economy (confiscation and asset recovery). It will, however, advocate a wider use of financial investigation techniques by general investigators to gather evidence and intelligence beyond the theatre of asset recovery and financial deprivation of offenders (Hughes and Hicks, 2025). Advocating wider use will be based on a proposed definition of financial investigation which attempts to overcome investigator perceptions that it is something only for specialists to apply:

*'Financial investigation is a technique to trace the complete or partial financial footprint of an individual or entity. It is a generic tool to inform strategic and tactical decision-making in the use of information, intelligence and evidence to support enquiries and investigations at all levels' (*Hughes, 2021*: 128;* Hughes and Brown, 2022*).*

In addition, the authors use a similarly newly proposed definition of what might constitute a better understanding of financial intelligence, again an attempt to move away from traditional investigator viewpoints that it must be related to bank accounts or property:

*'Financial intelligence is any information which assists in establishing the complete or partial financial footprint of individuals or entities and which can be utilised to inform strategic and tactical decision making for all investigation, prosecution and asset recovery purposes' (*Hughes, 2021*: 129;* Hughes and Brown, 2022*).*

It is a definition carefully considered in two aspects. First, to debunk the myths about what financial intelligence is usually considered to be. Second, to wholly integrate with the National Intelligence Model (NIM), once again attempting to move financial investigation focus away from asset recovery or the end game of confiscation after prosecution.

This article draws a distinction between two common terms used to describe financial investigation. First, and popularly used in television dramas and films (and then quoted offscreen by politicians and commentators is "following the money". It appears to have become a term synonymous with the money laundering trails of criminals at all levels, although of particular significance where organised crime is being commented upon or investigated (Wood, 2017). The problem in the literal sense, is that the money trail can run out. Concentrating on money laundering payments and asset identification potentially stops when nothing further regarding the money laundering can be found. This metaphorical cul-de-sac is not true of the phrase "following the financial footprint", a completely different approach to identifying and utilising financial investigation in non-specialist investigations and at routine level. This would include CHIS deployments where organised criminality is not necessarily involved.

The Financial Action Task Force (2012: 3) stated "the major goal of financial investigation is to identify and document the movement of money during the course of an investigation." This reinforces any perceptions, nationally and internationally, outside the theatre of asset recovery that financial investigation is asset derived, and of limited and specialist use. Some non-asset recovery aspects of financial investigation have been detailed elsewhere (Brown et al., 2012; HMCPSI et al., 2010; HMIC et al., 2004; Hughes, 2021; Hughes and Brown, 2022) but translating the potential for wider application of financial investigation into other areas of law enforcement remains problematic at all levels, policy, strategic, tactical and practice. It is here where altering the perception of financial investigation may begin to realise its potential for wider application away from asset recovery, in this instance relating to CHIS. The concept of the financial footprint (the lifestyle footprint of an individual) moves away from the mantra of "following the money." Rather, it moves towards following or exposing the financial minutiae of an individual to obtain information of evidential (or intelligence) value to lead to an operational intervention for example, a cash detention, premises or vehicle search, location of individuals and arrest opportunities.

Methods

There appears to be no clear picture of how financial investigation and intelligence cross over into the historically secretive world of CHIS handling. Interest in this area of policing and intelligence for the authors was originally piqued when primary research was conducted regarding financial investigation involving 345 survey respondents from 61 different UK law enforcement agencies (Hughes, 2021). Twenty questions were asked regarding the understanding of financial investigation and intelligence and of the 345 survey respondents, one was a police CHIS handler. It was evident that the individual possessed knowledge of suspicious activity reports (SARs) which are mandatorily produced within the financial and regulated sector regarding any suspicious movements of funds. Three questions were asked about financial intelligence; what is an item of financial intelligence, how many items of financial intelligence have you submitted in the last twelve months and on how many occasions have you used financial intelligence in investigations in the last twelve months? Responses from the CHIS handler were "bank accounts" to the first question and "none" to each of the other two questions.

The writers acknowledge, as did Hughes (2021), that a single respondent cannot provide any conclusions whatsoever, but the answers of that one participant did give rise to questions concerning whether financial intelligence is understood, applied or produced within the CHIS environment. It also raised questions regarding whether CHIS handlers receive any POCA input to enable basic decision-making concerning cash detention interventions. These questions seem particularly important if we are to believe the continued claims of successive governments, law enforcement and commentators, that we live in an age of effective intelligence-led policing (Parliament, 2008; Ratcliffe, 2010; 2016). Following the financial footprint should be accepted as a policing baseline performance tool to gather intelligence regarding not only assets but also primary evidence. Accepting this premise, it seems legitimate to query how the police service engages with the fundamental tenets of financial intelligence, either by using it or obtaining and recording it.

The core focus of the present study was to better understand the extent of integration between the different fields and in an attempt to confirm or deny any conclusions arrived at in these areas of discussion. The methods involved a literature review discussed throughout this paper as well as a freedom of information enquiry. Given the potential sensitivities around intelligence matters, the core approach for this project follows the pattern of "specified ignorance", to explicitly recognize what is currently not known as a basis for developing more knowledge on what needs to be known (Merton, 1987). The FOI queries were conducted with all UK police forces whereby four considered questions concerning CHIS and financial investigation were asked:

- **Q1**- How many intelligence logs in total were created in 2023 (by the selected Police Force)?
- **Q2**- Of these logs, how many are linked to financial investigation or Proceeds of Crime (POCA) enquiries in 2023 (by the selected Police Forces)?
- **Q3**- How many intelligence logs were submitted by the Dedicated Source Handling team (DSHU/CHIS tactic) in 2023 (by the selected Police Forces)?
- **Q4**- Of the logs submitted by DSHU, how many relate to financial investigation of POCA enquiries in 2023 (by the selected Police Forces)?

It was hoped that by asking generic questions, a baseline of information could be assimilated based upon primary information of a general nature only, from the Police Forces themselves, thereby avoiding academic conjecture based only on available linked publications or policy directives.

Of the 42 police forces asked, all responded in some way to the request:

26 agencies supplied data for Q1 and 16 agencies refused data for Q1.

All 42 agencies refused data for Q2, Q3 and Q4.

Responses to Q1 are examined later in this article as are the negative replies to the remaining questions. Without fail regarding Qs 2, 3 and 4, all replies were completely negative. Some forces stated they did not hold the information in any easily recoverable state, some refused to state whether the information was held or not, some stated it would cost too much to search for and produce the data, and some stated they held the information but were exempted from producing it due to four reasons:

- Section 24(2) National Security; claiming that by confirming or denying that any information relevant to the request exists would render Security measures less effective. This could lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.
- Section 30(3) Investigations; claiming that by confirming or denying that any information relevant to the request exists would disclose what facts may or may not exist in relation to an ongoing investigation. If doing so would harm that investigation, denying justice to the victims or jeopardising an investigation from reaching a satisfactory conclusion then it would not be in the public interest to do so.
- Section 31(3) Law enforcement; claiming that by confirming or denying that any information relevant to the request exists, it would hinder the prevention or detection of crime, undermine the partnership approach to law enforcement, which would subsequently affect the force's future law enforcement capabilities.

Section 38 Health and Safety: claiming that disclosure on these grounds would be likely to endanger the physical or mental health or safety of any individual.The various responses raise even more questions. It is difficult to understand why some police forces are able to provide the number of intelligence items submitted in the last year. Only a total number was requested under the FOI request on the understanding that this could in no way reveal any details of what investigations were or are underway, from which sources information originates or how it might be utilised. It was expected that all police forces would be able to produce an overall total of intelligence items submitted as it is known that unique reference numbers are applied to items being entered into known intelligence systems. This assumption on the part of the authors appears to have been erroneous as 12 Forces replied they are unable to provide numbers for the simple request in Q1, due to no central recording system for intelligence. In an intelligence-led policing environment this approach and the efficacy of such systems must be questioned. It is presumed that cost is only an issue for police forces with non-centralised systems as 26 other forces were able to furnish totals for Question 1 without issue (after due consideration and a public interest test).

Public accountability

The authors do not believe that the disclosure of data comparing CHIS intelligence with overall intelligence submissions undermines policing to any significant degree. What inferences are to be drawn if 50 % of a force's intelligence logs are created by CHIS in contrast with only 10 %? The public, including criminal networks, are aware that law enforcement uses CHIS and would expect that a percentage of information would result from this activity. Would a high CHIS percentage indicate effective use of the tactic or a lack of activity from other tactics? CHIS reporting is not limited to the county borders of the home force, so even fewer inferences can be drawn based upon specific force data. Few operational inferences of value can be drawn from comparing the data, indicating that it will be of little use to criminal networks. For instance, if we ask the question, "how will a criminal network respond if it knows that 20 % of CHIS intelligence relates to financial issues?", it is difficult to understand how networks can effectively alter their methods given that 80 % of intelligence may relate directly to their primary criminal activity. Data of this kind lacks the detail to be of use to criminal networks and is incapable of identifying if a certain criminal group is the subject of an investigation.

There is an important public interest issue at stake. Chief Constables (CC) and Police and Crime Commissioners (PCC) are scrutinised and held to account for their performance against policing priorities. Forces that publicly claim to be addressing community priorities should be obliged to provide data to support any such assertion. FOIs that request such data are key to public accountability. FOI requests that identify a persistent lack of intelligence in key priority areas may provide an explanation for poor performance and guidance on how to rectify it.

Freedom of information (FOI) requests

Section1(1) of the FOI Act (2000) places a general duty upon public bodies to disclose whether they hold information relevant to a public request and if they hold such information, to disclose it. This section focuses on the refusal grounds and numerous exemptions allowed under section 12 of the FOI Act and in particular the ones listed in the replies from the 42 agencies who were contacted. A summation of the relevant FLI sections is as follows:

Section 12 allows bodies to refuse disclosure if it creates too great an administrative or financial burden. The accepted limit is 18 h of work or £ 450 costs. (COST)

Section 24 allows bodies to refuse disclosure on the grounds of 'safeguarding National Security'. (NS)

Section 30 allows bodies to refuse disclosure if material is held for the purpose of a criminal investigation. It specifies information used to ascertain whether criminal charges can be brought. (INV')

Section 30 (2)(b) creates a specific exemption for material relating to the obtaining of information from confidential sources. The term 'confidential source' is not specifically recognised in the Regulation of Investigatory Powers Act 2000 (RIPA) but it is usually applied to any person giving information in confidence. This is a broader category than CHIS. (CS)

Section 31 allows bodies to refuse disclosure on the grounds that it would prejudice (a) the prevention or detection of crime, (b) the apprehension or prosecution of offenders, (c) the administration of justice. (LE)

Section 38 allows bodies to refuse disclosure on the grounds that it would be likely to endanger the physical or mental health or safety of any individual. (HS)

However, Section 17 (3) of the FOI Act requires public bodies to justify why they have refused disclosure, by means of a simple public interest test.

It is questionable whether the FOI returns were sufficient and justifiable. The data gathered from UK police forces raises some concerning issues. Whilst almost all forces responded to the request, no force supplied all the required data. Most returns refused data, citing the 'impracticality of providing the data', or undermining 'national security', the 'integrity of investigations', and the ability to 'conduct law enforcement'.

The authors take issue with this. Using the East Midlands as an example, both crime and intelligence data are held on a single computer system called NICHE. A simple search enquiry can identify the number of intelligence logs submitted by any Force in the region. This simple request (Q1) has generally achieved compliance.

There was no compliance beyond Q1. The grounds for refusal by the police forces asked to participate in relation to each of the four questions highlights issues of interest.

CHIS activity, including the creation of intelligence logs, is recorded on a Source Management System (SMS). CHIS activity requires a secure system that cannot be accessed by non DSHU staff due to the sensitive nature of the work. Intelligence logs generated by CHIS activity are disseminated to NICHE via the DSHU Controller. It is a simple process to search for the number of CHIS generated intelligence logs on the SMS. The authors believe that it is not impractical to supply this simple data. Any intelligence system, whether NICHE or SMS, must have effective search mechanisms, otherwise forces are undermining their compliance with lawful disclosure requirements of the Criminal Procedure and Investigations Act 1996 (CPIA).

Isolating logs that relate to financial investigation may be a more complex issue, both on NICHE and SMS systems. Forces maintain their own crime classification systems for intelligence on both NICHE and SMS and this will create inconsistent returns. Nonetheless, given the demands of NIM and modern performance management, the authors believe that forces can identify the volume of crimes and intelligence in any given crime type; to lack this ability would be a failure of management.

FOI overview analysis

For the ease of the reader, results of the FOIs submitted in respect of the four questions outlined above are contained within the tables below (Tables 1 and 2).

The fact that some police forces supplied data for Q1 (what should be a simple query within an intelligence database) and some did not appears to identify a disparity in the way intelligence and risks associated with it are perceived across policing. It is unclear why 39 % of agencies were unwilling or unable to comply with the disclosure request, particularly using cost as an excuse not to do so. It is concerning that some forces do not appear to be able to provide a total number of intelligence items without incurring considerable cost, a situation in some cases apparently due to disparate recording systems being used. In the current climate of so-called intelligence led policing, this is an unexpected response. It immediate raises questions about the effectiveness of intelligence being produced if even the number of responses cannot be easily obtained (see Table 2).

The varied responses raise the concern that agencies may have vastly differing intelligence databases, some of which cannot easily retrieve data. This seems unlikely to be the case. Police Forces share their intelligence data with the Police National Database (PND), which requires significant interoperability, consistency and minimum operating standards, all of which facilitate basic data retrieval. UK policing is also divided into 9 Regional Organised Crime Units (ROCUs). ROCUs also require interoperable intelligence systems. As an example, within the East Midlands ROCU, the five forces share a combined intelligence database and management recording system. As the process of data retrieval for Q1 is identical for each East Midlands force, responses ought to have been identical.

Table 1
Table showing results for Question 1 – how many intelligence items were submitted during 2023.

Force	Number of intelligence items	Reason for not supplying
Bedfordshire	36,047	
British Transport Police	30,097	
Cambridgeshire Police	114,548	
City of London Police	3902	
Cleveland	38,103	
Cumbria Constabulary	47,594	
Derbyshire Constabulary	47,319	
Devon and Cornwall Police	42,201	
Dorset Police	42,201	No reply
Durham Constabulary	45,179	
Dyfed Powys Police	24,557	
Essex Police	Nil return	s12 (too costly)
Gloucestershire Police	30,907	
Greater Manchester Police	86,155	
Gwent Police	20,411	
Hampshire and Isle of Wight Constabulary	Nil return	s12 (too costly)
Hertfordshire Police	21,112	
His Majesty's Revenue and Customs	Nil return	s12 (too costly)
Kent Police	76,191	
Lancashire Police	54,250	
Leicestershire Police	Nil return	s24/30/31 exemptions
Lincolnshire Police	24,431	
Merseyside Police	Nil return	s24/30/31 exemptions
Metropolitan Police	Nil return	s12 (too costly)
Ministry of Defence Police	3371	
Norfolk Constabulary	Nil return	s12 (too costly)
Northamptonshire Police	Nil return	s12 (too costly)
Northumbria Police	Nil return	s12 (too costly)
North Yorkshire Police	45,200	
North Wales	23,113	
Nottinghamshire Police	Nil return	s31 exemption.
Police Scotland	315,000	
South Yorkshire	45,120	
Staffordshire Police	29,718	
Suffolk Police	Nil return	s12 (too costly)
Surrey Police	39,324	
Sussex Police	Nil return	s12 (too costly)
Thames Valley Police	Nil return	s12 (too costly)
Warwickshire Police	Nil return	s12 (too costly)
West Mercia Police	42,131	
W. Midland Police	129,091	
West Yorkshire Police	Nil return	s12 (too costly)

It is interesting that of the five, East Midlands forces contacted, 2 supplied data for Q1, 1 refused on cost grounds, 1 refused on grounds of National Security/undermining investigations/law enforcement and 1 refused on law enforcement grounds (see Table 2). The cause of this discrepancy is unclear. It is noted that Northamptonshire refused data on cost grounds but then supplied the information for Q1 inadvertently in its explanation for why processing 54,252 intelligence logs was too burdensome.

There seems insufficient evidence to refuse data for Q1 on grounds of National Security, Investigations or Law Enforcement. Public interest justifications for refusal, offered by police forces under s17(3), are generic and refer to common themes such as:

FOI replies are not private disclosure so confirming that logs exist would "provide valuable intelligence" to terrorists. The replies do not state what the intelligence benefit might be or how it might be used.

Force comparison of POCA submissions may benefit terrorists. Police forces suggest that forces with lower submission levels would be targeted by terrorists. This wrongly assumes a direct link between levels

Table 2
Refusal figures to Qs 1 – 4.

JUSTIFICATION FOR NON-DISCLOSURE.	s12 TOO COSTLY	s31 UNDERMINES: LAW ENFORCEMENT.	s24/30/31 UNDERMINES: NATIONAL SECURITY. INVESTIGATIONS. LAW ENFORCEMENT.	s24/30/31/38 UNDERMINES: NATIONAL SECURITY. INVESTIGATIONS. LAW ENFORCEMENT. HEALTH AND SAFETY.	s31/38 UNDERMINES: LAW ENFORCEMENT. HEALTH AND SAFETY.	No reply
Q1 NUMBER OF INTELIGENCE LOGS CREATED IN 2023.	12	1	2			1
Q2 NUMBER OF LOGS RELATING TO FINANCIAL INVESTIGATION OR POCA IN 2023.	15	1	24	1		1
Q3 NUMBER OF LOGS GENERATED BY THE DSHU (CHIS TACTIC) IN 2023.	13	2	24	1	1	1
Q4 NUMBER OF LOGS CREATED BY THE DSHU RELATING TO FINANCIAL INVESTIGATION OR POCA IN 2023.	13	2	24	1	1	1

of submissions and the ability to police effectively. It does not allow for the quality or accuracy of logs to be considered or that other agencies may supply the intelligence picture.

Refusal analysis

Attention now turns to why without exception, all forces refused to answer questions 2 – 4 but with different rationales. Refusals to Q1 are included for completeness.

Inconsistencies relating to questions 2–4 are immediately apparent. Using East Midlands forces as an example, all refused to supply data for any of the questions. Despite sharing intelligence systems, the grounds for refusal again appear inconsistent:

- Northamptonshire refused all 3 requests on cost grounds.
- Nottinghamshire refused all 3 requests on LE grounds.
- Lincolnshire, Leicestershire and Derbyshire refused all 3 requests on NS/INV/LE grounds.

It is unclear why there is a lack of consistency from forces that share an intelligence database.

As mentioned above, s30(2) creates a specific exemption for the disclosure of data relating to ‘confidential sources’.

It is not clear why this exemption alone has not been used to justify non-disclosure for Q3 and Q4, both of which relate specifically to CHIS material.

Not one Force has made specific mention of this exemption. Instead, non-disclosure has been justified, often in great detail, on anything other than that specific exemption.

This may be the result of a lack of understanding by FOI staff regarding ‘confidential source’ material or an over-reliance on pro forma responses that are perceived as justifying non-disclosure against a wide range of information categories.

Confusingly, there is evidence that Forces regularly disclose FOI data relating to the CHIS tactic and payments awarded (West Yorkshire Police, 2023).

Surely this FOI data is of similar operational value and risk to the data requested in this article; no inferences of any operational value can be drawn, yet the reward information is routinely disclosed. We do not have access to the rationale given for disclosure of financial reward data but for disclosure to have occurred, forces must have been satisfied that the public interest test favoured disclosure and that the data was easily available and retrieval not overly burdensome. CHIS reward data is held on the SMS database. It remains unclear why disclosure is accepted for CHIS reward data but refused for the authors’ similar numerical log data. Further research is required to clarify this issue.

Consideration of the public interest test

The public interest test was used by respondents to justify non-disclosure for all non-section 12 refusals. North Yorkshire’s response presents a good example of the generic public interest justification.

Where National Security was used as an exemption, North Yorkshire stated that any comparison between forces enables terrorists to identify areas of the UK that were vulnerable to financial crime. Where Undermining Investigations was used as an exemption, North Yorkshire stated that disclosure would, “disclose police practises used, thereby exposing operational procedures and investigative protocols”. It would “reveal police tactics”. Where Law Enforcement was used as an exemption, North Yorkshire stated that it, “could compromise law enforcement tactics”. It further stated that reduced law enforcement effectiveness would lead to increased terrorism as geographic vulnerabilities were identified. Their justification refers to arrest and charging data and search data from 2020, that could be used to guide terrorist policy. This does not appear relevant to the application. It suggests their replies are based on outdated material or are a block

response to avoid tailoring information to specific requests such as in this FOI enquiry. Either reason seems unacceptable, and it is reiterated that the questions required non-specific information only.

The Ministry of Defence's (MOD) response included a 'Health and Safety' exemption (section 38). They were the only force to consider this relevant stating that s38 disclosure would undermine confidence that the MOD could maintain the safety of individuals who gave information. The MOD did not state how confirming the existence of CHIS and financial crime logs would compromise their ability to safeguard sources. Criminal gangs will already be aware that police use informants. Confirmation of this is unlikely to prejudice this or any other police tactics.

The response from Kent Police was more detailed than most and presents a good example of the public interest exemption, equating the volume of intelligence submissions with intelligence operational capability. However, intelligence effectiveness is rarely related directly to quantity of logs and 50 timely and accurate logs are more likely to be of greater benefit that 250 delayed, vague and inaccurate ones. An absence of logs from any one tactic, in this case CHIS, is not necessarily an indicator of an intelligence gap or weakness. Substantial intelligence may flow from alternative tactics, such as local officer patrols, the general public or surveillance, negating the need to risk the safety of registered informants in that area. An absence of intelligence in one area may reflect a genuine lack of risk and criminality. Consequently, terrorists and criminals cannot draw accurate or valuable inferences regarding police tactics, from general intelligence data on broad topics, including high level CHIS figures.

To be of real value to criminals, data would need to inform the applicant about specific organised crime groups or specific crime incidents. The international nature of financial crime all but guarantees no inferences can be drawn as to whether intelligence submissions relate to local or global issues. Additionally, a complete absence of intelligence submissions does not suggest that criminals can act with impunity in a specific crime area. Entirely reactive investigations can generate arrests and prosecutions irrespective of the flow of intelligence.

General issues

The section 12 cost exemption does not require forces to consider the burden against each question. If one aspect of the application is believed to be too costly, no other aspect of the application need be considered. Northumbria made specific reference to this in their grounds for refusal. This administrative rule has significant implications for applicants, who must consider whether multiple data requests should be requested in phases so that simple requests are not compromised by those that are genuinely burdensome.

The operational refusal grounds to Questions 2 and 4 raise general concerns. Forces state that they cannot retrieve intelligence data regarding crime type, without manually checking each log. If this is true, it would place an unreasonable burden on forces. It seems unbelievable that force intelligence units, whose primary purpose is to assess intelligence, are unable to conduct simple data searches based on crime type. If this is not possible, how would analysts create subject or problem profiles relating to any crime type? Even if some debate as to what constitutes financial intelligence is allowed, forces would not be able to conduct basic intelligence led policing if they were unable to quickly search for intelligence relating to financial issues in general. Unless they totally depend only on suspicious activity reports (SARs) discussed above.

Refusal grounds for Q3 seem just as inconsistent. Like Q1, it was a simple request for a count of log submissions. This data is known to be recorded on SMS and from the authors' own experience, can be easily retrieved. Therefore, it is unclear why Q3 data was refused on cost grounds. It also remains unclear, despite the protestations of the forces, as to why the number of CHIS submissions should not be public knowledge. Regarding refusals for Q4, it is quite possible that no one has considered recording whether interventions or arrests have resulted from financial information. Cash detention interventions should be more easily recognised and are recorded independently on a standalone system by the NCA, the Joint Asset Recovery Database (JARD) which was designed in 2002 to record all assets seized or confiscated using POCA (2002). They may not be recorded internally by forces as resulting from CHIS intelligence. Again, the question is raised that if forces do not know the productiveness of certain information channels, then how can law enforcement proclamations that we live in an age of intelligence-led policing be successfully quantified against the claim.

Conclusion

The FOI request failed to gain the bulk of the required data for this paper.

Q1 and Q3 were technically simple requests. However, 39 % of forces refused data for Q1 and all forces refused data for Q3. None of the justifications given by forces appeared to be reasonable and may provide grounds for an appeal/complaint. Further research is required.

Reasons for non-disclosure provided by forces seem inconsistent and varied despite many forces using identical databases. Refusal responses varied greatly, suggesting that there is a lack of professional consensus in this area or a block response which until now, has not been questioned from an evidence-based academic perspective. There is, as explained earlier, the section 12 cost exemption which applies to all FOI questions and can be used to refuse all aspects, even if only one aspect of a request is considered burdensome. This allows forces to refuse data that may be easy to retrieve and disclose simply because other aspects are too costly. This appears to be a 'loophole' that many applicants may not be aware of. It may also be one that, to date, has remained unhighlighted within public consciousness.

The public interest test refusal explanations addressed similar, generic issues and used similar language, suggesting that the responses were produced pro forma. On occasions the detail did not appear to relate directly to the application, further suggesting the responses were pro forma. Responses had the feel of a block response and the language used in the refusals was significantly similar.

Another aspect of the inhibitors which this article seems to have unearthed is whether force FOI teams are aware of what intelligence data is available or who is best placed to retrieve it. FOI teams may be unaware of intelligence unit structures and capabilities. They would not necessarily know which search facilities exist on covert databases such as SMS (or on non-covert systems for that matter) and may not direct enquiries to the appropriate team. There may be a disconnect between force intelligence units and FOI departments, aggravated fear that intelligence revelation of any kind, undermines operational security. Such an environment could easily lead to a mistaken belief that intelligence data retrieval would be burdensome and require specialist attention. Whilst not justifying non-compliance, this potential disconnect may be responsible for high-cost refusal exemptions. More research is required to assess the knowledge and training of FOI staff regarding the application of the section 17 'public interest test'. The issue seems a practical one which law enforcement should want to remedy as their own data is potentially inaccurate where it is possible to retrieve it.

This research started out to investigate the level of integration between CHIS deployment and financial investigation. At the end of this project, the authors remain no closer to establishing whether the two fields integrate at all, whether training is sufficient to the task, whether strategic governance includes financial investigation considerations as a matter of routine, and whether internal recording is sensitive enough to provide effective intervention points in investigations utilising financial information. It has largely failed in its objective, instead identifying what appears to be a flight mentality the instant intelligence quantification is mentioned. This appears further exacerbated by anything related to questioning the effectiveness of CHIS, despite high level questions being formulated so as to avoid specific data or any

investigative practices. The general reaction to the FOI request appears one of 'knee jerk' reaction' at the mention of the CHIS environment. The evidence from the FOI responses does appear to underline that position and the authors have explained why the rationale provided in respect of refusals is questionable.

Although the main thrust of this article was not achieved, serious points for consideration are raised concerning the nature and effectiveness of so-called intelligence-led policing. Currently, the situation concerning the use of financial investigation techniques and CHIS remains unanswered. Financial gain is a strategy priority for serious and organised criminality but, strangely, financial investigation is not a strategy priority for UK policing.

Stock FOI responses preserve the opaqueness of intelligence and gives rise to question the effectiveness of it in certain (if not all) remits, points which the authors would suggest is not in the interests of transparent and evidence-based policing. It seems flawed to think that something can be measured effectively if it cannot be recorded consistently and accurately. Forces are obliged to provide accurate data to support business, performance and Intelligence objectives. This appears to be undermined by a varied, and possible technologically flawed approach to data management (in this case financial intelligence in the CHIS environment). With regard to financial information, effectiveness cannot be measured accurately if recorded information is not easily discernible, or worse, not appropriately recorded, or recorded on systems making it hard to retrieve (or costly to do so). FOI responses suggest that financial investigation remains unmeasured in general intelligence terms and apparently to minimal levels within the CHIS environment, perhaps the last bastion of what appears to be non-transparent policing data. The question remains as to how we can successfully take cash out of serious and organised crime (or any crime) if we do not know how effective we are being at any level or within any specific sphere of policing activity?

CRediT authorship contribution statement

David Kennedy: Writing – original draft, Visualization, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Craig Hughes:** Writing – original draft, Visualization, Supervision, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **David Hicks:** Writing – review & editing, Supervision, Project administration, Methodology, Investigation, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

"No acknowledgements".

References

Atkinson, C., 2019. Mind the grass! Exploring the assessment of informant coverage in policing and law enforcement. J. Polic. Intell. Count. Terror. 14 (1), 1–19 Available at: https://www.tandfonline.com/doi/abs/10.1080/18335330.2019.1572913 [Accessed 21 June 2024].

Brown, R., Evans, E., Webb, S., Holdaway, S., Berry, G., Chenery, S., Gresty, B., Jones, M. (2012) . [pdf] Research Report 65. London: Home Office. Available at: , and The Contribution of Financial Investigation to Tackling Organised Crime: A Qualitative Study〈https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116518/horr65.pdf〉[Accessed 14 June 2024].

College of Policing(2024) National Intelligence Products APP. Available at: https//〈www.college.police.uk/search?query=nim〉[Accessed 23rd August 2014].

Crowdy, T., (2011). . Oxford: Osprey Publishing. p15.The enemy within: A history of spies, spymasters and espionage.

Financial Action Task Force(2012) – . [pdf] Paris: FATF. Available at: Operational IssuesFinancial Investigations Guidance〈http://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf〉[Accessed 09 August 2024]..

H.M. Inspectorate of Constabulary, H.M Crown Prosecution Service Inspectorate, H.M. Magistrates Court Inspectorate (2004) . [pdf] Available at: Payback time: Joint review of asset recovery since the Proceeds of Crime Act 2002〈https://www.justiceinspectorates.gov.uk/cjji/inspections/payback-time-joint-review-of-asset-recovery-since-the-proceeds-of-crime-act-2002/〉[Accessed 07 June 2024].

Her Majesty's Crown Prosecution Service Inspectorate (HMCPSI), Her Majesty's Inspectorate of Court Administration (HMICA) and Her Majesty's Inspectorate of Constabulary (HMIC) (2010) Joint Thematic Review of Asset Recovery: Restraint and Confiscation Casework. [pdf] Available at: 〈https://www.justiceinspectorates.gov.uk/hmic/media/joint-thematic-review-of-asset-recovery-restraint-and-confiscation-casework-full-report-20100324.pdf〉 [Accessed 10 August 2024].

HM Government(2023): , (2023), Chap 3. UK Home Office.No place to hide: Serious and organised crime strategy2023-2028.

Hoffman, D. & Rowe, J.J. (2013) Human rights in the UK an introduction to the Human Rights Act 1998. 4th ed. Chap 2. Harlow: Pearson Education.

Home Office (2022) Covert Human Intelligence Sources revised Code of Practice (accessible). Available at: 〈https://www.gov.uk/government/publications/covert-human-intelligence-sources-code-of-practice-2022/covert-human-intelligence-sources-revised-code-of-practice-accessible〉. [Accessed 15 August 2024].

Hughes, C. (2021) Financial Investigation: Establishing the principles of a generic and effective philosophy. PhD, unpublished.

Hughes, C., Brown, R., 2022. Financial investigation for routine policing in Australia. Trends and Issues in Crime and Criminal Justice. Australian Institute for Criminology, pp. 1–12.

Hughes, C., and Hicks, D. (2025) Financial Investigation and Financial Intelligence: A Critical Analysis. Abingdon, Oxon: Routledge. https://doi.org/10.4324/9781003438649 [Accessed 08 January 2025].

Merton, R.K., 1987. Three fragments from a sociologist's notebooks: establishing the phenomenon, specified ignorance, and strategic research materials. Annu. Rev. Sociol. 13, 1–29 Available online at: https://doi.org/10.1146/annurev.so.13.080187.000245 [Accessed 20 December 2024].

Moffet, L., Oxburgh, G., Desser, E., Watsdon, P., J, S., Gabbert, F., 2022. Inside the shadows: a survey of UK human source intelligence (HUMINT) practitioners, examining their considerations when handling a covert human intelligence source (CHIS. Psychiatry Psychol. Law 29 (4), 487–505 Available online at: 10.1080/13218719.2021.1926367 [Accessed 19 June 2024].

National Police Chiefs' Council (NPCC) Homicide Working Group (2021) Major Crime Investigation Manual. Available at: https//〈www.college.police.uk/app/major-investigation-and-public-protection/homicide〉 [Accessed 23rd August 2024].

Nunan, J., Stanier, I., Milne, R., Shawyer, A., Walsh, D., May, B., 2022. The impact of rapport on intelligence yield: police source handler telephone interactions with covert human intelligence sources (Available at:). Psychiatry Psychol. Law 29 (1), 1–19. https://doi.org/10.1080/13218719.2020.1784807. [Accessed 20 June 2024].

Parliament.UK (2008) Committee on European Union, Chapter 10: Summary of Conclusions and Recommendations. Available at: 〈https://publications.parliament.uk/pa/ld200708/ldselect/ldeucom/183/18313.htm〉 [Accessed 05 August 2024].

Ratcliffe, J., 2010. Intelligence-led policing and the problems of turning rhetoric into practice. Polic. Soc. 12 (1), 53–66 Available at: https://www.tandfonline.com/doi/abs/10.1080/10439460290006673?src=recsys [Accessed 05 August 2024].

Ratcliffe, J.H., 2016. Intelligence-Led Policing. Routledge: London.

Scott, P.F., 2022. Authorising crime: the covert human intelligence sources (Criminal Conduct) Act 2021. Mod. Law Rev. 85 (5), 1218–1244 Available at: https://onlinelibrary.wiley.com/doi/full/10.1111/1468-2230.12751 [Accessed 21 June 2024].

The Money Laundering Regulations (2007) (S.I. 2007/2157). London: The Stationery Office.

West Yorkshire Police website (2023) Freedom of Information Requests. Available at: https://foi.west-midlands.police.uk/chis-payments-994a-23/ [Accessed 27th August 2024].

Wood, H.(2017) Every Transaction Leaves a Trace. The Role of Financial Investigation in Serious and Organised Crime Policing. [pdf] London: Royal United Services Institute. Available at: .〈https://rusi.org/sites/default/files/201709_rusi_everytransactionleavesatrace_wood_web.pdf〉[Accessed 03 August 2024].