Journal of Financial Crime

Emerald Article: Winning the information wars: Collecting, sharing and analysing information in asset recovery investigations

Anthony Kennedy

Winning the information wars

Collecting, sharing and analysing information in asset recovery investigations

Anthony Kennedy
Northern Ireland for the Assets Recovery Agency, Belfast, UK

Abstract

Purpose – Recognising that financially related, personal information is the raw material of successful asset recovery investigations, the paper aims to examine the mechanisms which investigators may use to gather such information and the legal barriers to information gathering.

Design/methodology/approach – The paper draws on the author's own practical experience of involvement in criminal asset recovery proceedings in the UK.

Findings – It is the State's obligation to deliver criminal asset recovery in the most efficient and cost-effective way, consistent with privacy rights and obligations, providing value for money in what is delivered by law enforcement. Doing so will require making better use of financial information held by public sector agencies. There must be no form of financial information which is beyond the reach of an investigator in an appropriate case. If there is, criminals will utilize that weakness to place criminal assets where information in respect of those assets cannot be obtained. If asset recovery is to be successful, it is essential that – to use the metaphor of financial information as "dots" – investigators are able to collect the dots, connect the dots and share the dots.

Practical implications – The paper identifies: the need to keep the legal tools used to obtain information under regular review; eight core information skills which investigators must develop for effective asset recovery; and the importance of a multi-disciplinary approach in analysing financial information.

Originality/value – The paper explores UK criminal asset recovery from an informational perspective.

Keywords United Kingdom, Crimes, Financial control, Asset protection

Paper type General review

Introduction

> . . . it's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information. Fragments that can be retrieved and amplified . . . (Gibson, 1988).

Successful asset recovery requires the combination of these information fragments. An information-perspective on asset recovery recognises that financially related, personal information is the raw material of successful investigations[1]. While jurisdictions create rules to protect information pertaining to their citizens, criminals seek to benefit from those rules to prevent information regarding their criminal proceeds from falling into the possession of financial investigators. The result is: the information wars.

Financial investigations are information-intensive. They involve both public and private sector material, for example taxation records and bank-account information, which demonstrate money movements, together with any relevant information as to lifestyle. Any record that provides information concerning money may be significant. The investigator seeks to discover where money came from, who obtained it, when it

Journal of Financial Crime
Vol. 14 No. 4, 2007
pp. 372-404

1359-0790
DOI 10.1108/13590790710828136

was received and where it was stored, deposited, or transformed into other forms of property. Since, those who commit acquisitive crime continuously grow more sophisticated in their laundering activities, this requires investigators to acquire new and specialized financial investigation tools, designed to obtain and interpret information which criminals wish to hide. This paper examines financial investigators' need for information and how that information is obtained and analysed.

Financial investigations may be classified into two categories. Firstly, "follow the money" investigations, where investigators seek to discover the location of specific funds. This will take place, for example, where the proceeds of a fraud are being traced. Secondly, "net worth" investigations where investigators seek to identify all property owned by an individual. These will occur, for example, in a civil recovery or confiscation investigation. A "net worth" investigation may contain several "follow the money" investigations once specific sums of income have been identified and investigators attempt to trace their history.

Both types of investigation have similarities in terms of the tools that investigators use, but are different in that "net worth" investigations will be far more information-intensive. Conducting a "net worth" investigation consists of weaving together disconnected pieces of financial information to reveal broader patterns regarding someone's financial affairs. Seen from an information perspective (and using the metaphor of information as "dots") the role of a financial investigator is to "collect the dots" "connect the dots" and "share the dots" (and in a form where they are evidentially admissible) (Libicki and Pfleeger, 2004). A significant problem for investigators is that the dots may exist widely separated from each other. This is sometimes referred to as information being kept in separate "silos" or as "compartmentalisation" of information[2]. The key to the initial stage of investigation is bringing related but isolated facts into proximity with each other in order to help analysts detect significant patterns or connections. A conclusion only becomes possible once financial information from separate sources is combined.

Legal barriers to information gathering

While investigators will wish to obtain information, they must ensure that they do so in a lawful manner. There are a number of legal barriers which restrict the transmission of information, the principal of which are the duty of confidentiality, the Human Rights Act 1998, the Data Protection Act 1998 and the issue of *vires*. These are not matters to be considered sequentially, but rather impact on each other.

Duty of confidence

The law of confidence is a Common-Law concept. A duty of confidence arises when one person is provided with information by another in the expectation that the information will only be used or disclosed by the former in accordance with the wishes of the latter. The duty depends on the broad principle of equity that a person who has received information in confidence shall not take unfair advantage of it[3]. The tort of breach of confidence deals with unauthorised use or disclosure of certain types of confidential information and may protect it on the basis of an actual or deemed agreement to keep the information secret. For a duty of confidence to exist, two characteristics must be satisfied. Firstly, the information in question must have the necessary "quality of confidence". The nature of the information and the gravity of the circumstances are

relevant – the law will not intervene to protect trivial tittle-tattle, however confidential[4]. With regard to personal information, it should therefore not be in the public domain or readily available from another source and should have a certain degree of sensitivity. Secondly, the information must be communicated in circumstances giving rise to an obligation of confidence, although this may be implied from circumstances. An obligation of confidence is imposed by law if the circumstances are such that a person knew, or ought to have known, that the information was to be treated confidentially.

The duty of confidence owed by bankers is well established[5]. *Tournier* v. *National Provincial and Union Bank of England*[6] established that the bank owed its customer a legal, and not merely a moral, duty of confidentiality. However, *Tournier* recognised that the duty was qualified by four exceptions: where disclosure could properly be made under compulsion by law; where there was a duty to the public to disclose; where the interests of the bank required disclosure; and where the disclosure was made by the express or implied consent of the customer. In some jurisdictions, the confidentiality accorded to bank information exceeds that available under the usual duty of confidentiality. Such jurisdictions are described as bank secrecy jurisdictions. Bank secrecy laws have been criticised as "a criminally malevolent anachronism"[7] and as "a godsend for the criminal"[8] and there are international pressures against them.

Legal privilege is a particular form of confidentiality. It has been said that clients seeking advice must be able to speak freely to their lawyers secure in the knowledge that what they say will not be divulged without their consent and that, without this privilege, clients could never be candid and furnish all the relevant information that must be provided if lawyers are to advise their clients properly[9]. Privilege has been held to be a fundamental condition on which the administration of justice as a whole rests[10], a fundamental human right guaranteed by Article 8 of the European Convention on Human Rights[11], and a part of European Community law[12]. Of course, to extend privilege without limit to all solicitor and client communication upon matters within the ordinary business of a solicitor and referable to that relationship would be too wide[13]. Privilege therefore means that communications between a solicitor and his client relating to the transaction in which the solicitor has been instructed for the purpose of legal advice will be privileged, even if they do not contain advice on matters of law, provided that they are directly related to the performance by the solicitor of his professional duty as legal adviser of his client. Legal advice privilege covers communications between lawyers and their clients whereby legal advice is sought or given. It depends on there being a relationship of confidence between client and lawyer and on there existing the "relevant legal context" for the advice and confidentiality[14]. To try and ensure that legal privilege is not manipulated by a dishonest client, privilege does not exist where the communication has been made with a view to furthering a criminal purpose[15]. In *Francis and Francis* v. *Central Criminal Court*[16] the House of Lords held that, even where the intention to further a criminal purpose belonged to a third party, the communications were not privileged. The privilege may, of course, be waived by the client and a practice of the authorities requiring such a waiver has developed in certain US prosecutions[17].

From an asset recovery perspective, certain documents held by a legal adviser may not be covered by privilege. Importantly, this will include many conveyancing documents.

Solicitor's attendance notes, time sheets and fee records are also not privileged[18]. However, *R* v. *Crown Court at Inner London Sessions ex parte Baines and Baines*[19] held that, in a conveyancing transaction, documents containing advice from a solicitor to a client on factors serving to assist towards a successful completion, or the wisdom or otherwise of proceeding with the transaction, were privileged.

Duty of confidence is not a concept which applies only to information held in by persons in the private sector. Where information is obliged to be provided to a public authority, an obligation of confidence will generally arise. When a member of the public provides personal information to a public body, he expects that these details will be treated as confidential and will not be passed to persons other than the recipient – unless disclosure is necessary in the circumstances, or he has been told that disclosures may be made[20]. Whether a duty of confidentiality should be maintained has to be weighed against the powers and duties which the public body has to disclose the information (Cabinet Office, 2002, para. 3.45).

The Human Rights Act 1998

The Human Rights Act 1998 provides that public authorities are obliged to act in a way which is compatible with an individual's rights under the European Convention on Human Rights[21]. This impacts on the way public authorities may deal with information in their possession.

Article 8 of the ECHR enshrines a right to respect for individuals' private lives and prescribes the circumstances in which it is legitimate for a public authority to interfere with the enjoyment of this right[22]. It protects the individual from arbitrary interference by public authorities[23] and is wider than a right to privacy. It is a qualified right, as interference with its enjoyment is expressly foreseen in particular circumstances.

It has been held that the right secures to the individual a sphere within which he can freely pursue the development and fulfilment of his personality[24]. Protection of personal data has been recognised to be of fundamental importance to a person's enjoyment of his respect for private and family life as guaranteed by Article 8[25]. Any interference with that right must, firstly, be in accordance with law. This requires that the interference should have some basis in a domestic law which was accessible to the applicant allowing foresight of its consequences[26]. Secondly, any interference must pursue a legitimate aim. An investigator could undoubtedly argue that the aim of information gathering in asset recovery cases was the prevention of crime since such regimes are an important element in most jurisdictions' battle against organised crime and their effective functioning depends on having financial information available. Thirdly, an interference must be considered "necessary in a democratic society". "Necessity" implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued[27]. In determining whether an interference is necessary in a democratic society, the Court will take into account that a margin of appreciation is left to the Contracting States[28]. However, the margin of appreciation notwithstanding, the Court will look to ensure that there are adequate and effective safeguards against abuse.

In applying Article 8 to information, a compulsion by the tax authorities to divulge details of personal expenditure was ruled an interference, but one which could be justified in circumstances where the tax authorities legitimately required evidence

concerning the disposition of substantial personal assets. Nevertheless, broad use of such powers is likely to be considered disproportionate[29].

The State's ability to access financial information raises important human rights issues because an individual's financial transactions demonstrate his lifestyle, personal interests and even political beliefs. Nevertheless, appropriate privacy rights must co-exist with effective financial investigation into criminal proceeds[30].

The Data Protection Act 1998

The Data Protection Act 1998[31] regulates the processing and handling of personal data by "data controllers" a term which covers holders of information in both the private and public sectors. The main aims of the DPA are to protect individuals' rights to privacy and to ensure they have access to information held about them and can correct it. It protects against excessive and unreasonable retention of data and ensures compliance with ECHR Article 8 regards personal data, including sensitive personal data, by setting safeguards in accordance with the EC Directive to which it gives effect[32]. The DPA, described by the Court of Appeal as "a cumbersome and inelegant piece of legislation"[33] establishes eight Data Protection Principles[34], the most important of which, from an investigator's perspective, are that personal data must be, firstly, processed fairly and lawfully, and in particular must not be processed unless at least one of the conditions in Schedule 2 is met and, in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met[35]; and, secondly, obtained for specified and lawful purposes and not further processed in any manner incompatible with those purposes.

The DPA provides that, in determining whether any disclosure of personal data is compatible with the purpose for which the data were obtained, regard must be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed[36]. Therefore, unless the disclosure to third parties can properly be considered to be compatible with the purpose for which the data were obtained, the DPA effectively prohibits data-sharing. The Information Commissioner has a number of enforcement powers under the DPA and, if satisfied that a data controller has contravened any of the Data Protection Principles, may serve a preliminary enforcement notice raising issues of concern about the creation, retention or use of data and inviting a response.

Section 29 of the DPA empowers requests for personal data without the data subject's consent where the information is for one of the "crime and taxation purposes" namely:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; and
- the assessment or collection of any tax or duty

not having the information would prejudice one of these purposes.

Most investigators use a common form for requesting personal data for such purposes[37]. It gives details of the crime under investigation, why the data are needed, and how non-disclosure would be likely to prejudice the investigation. It is important to note that it is a request and not an order requiring the release of the information. Information required by an investigation for confiscation purposes clearly falls within Section 29. Given that the Director of the Assets Recovery Agency must exercise her

powers with a view to the "reduction of crime" it is also likely that civil recovery investigations fall within this exemption. However, even if it does not, Section 35 of DPA provides that personal data are exempt from the non-disclosure provisions where the disclosure is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. Since, civil-recovery proceedings are about establishing the director's rights to recoverable property, i.e. property obtained by unlawful conduct, it is clear that information may be released for that purpose[38].

The issue of vires

The powers possessed by a public body will depend on the category of body concerned. Statutory bodies derive their powers to act from their creating statute and have no vires to act outside their statutory functions. Government departments, however, have a broader scope of powers and may do anything that a natural person can, provided they are not forbidden from doing so[39]. According to well established principles of administrative law, a public authority must possess the power to carry out what it intends to do and may only act "within the four corners" of those powers[40]. If not, its action will be ultra vires and void. For public authorities considering the lawfulness of any proposed information-sharing with law enforcement agencies, a key question is therefore whether they have the power to process personal information in this way.

In addition to the necessity for a power to exist, it is also necessary that the power must be exercised for the purpose for which it was created. *Hazell* v. *Hammersmith and Fulham*[41] makes clear that an action will be ultra vires, notwithstanding the existence of a power, if a public authority uses a power to achieve a purpose that the power was not created to achieve. This issue underlay the Newton Committee's recognition that the information disclosure powers contained in The Anti-terrorism, Crime and Security Act (2001) were "a significant extension of the Government's power to use information obtained for one purpose, in some cases under compulsory powers, for a completely different purpose"[42]. As well as exercising specific powers provided, public authorities may also undertake tasks "reasonably incidental" to the defined purpose. At first glance, this might appear to create a broad power to permit public bodies to share information. However, it seems likely that the Human Rights Act 1998 militates against an interpretation that information-sharing may be too readily inferred, since it is apparent from the ECHR jurisprudence that the processing and disclosure to third parties of personal information falls within the scope of Article 8 (Cabinet Office, 2002, para. A.47-A.49).

Public authorities that wish to enter into information-sharing arrangements must therefore have an explicit power to do so. There is no universal statutory power permitting public authorities to disclose personal data to other such bodies even in limited circumstances. Government departments, agencies and other public bodies are each viewed as separate entities for the purpose of data-sharing and for privacy concerns (Cabinet Office, 2002, para. A0.5). In addition, it must also be recognised that there exist a large number of specific statutory provisions which prevent the disclosure of data or its use for purposes other than that for which it was collected (Cabinet Office, 2002, para. A.50-A.52).

The first Data Protection Principle's requirement that data processing must be lawful is also relevant here. Among other things, this means that there must be an underlying lawful basis upon which to conduct the processing, whether that is derived from statute, common law, implied powers, or by any other means. For this reason, information gateways have been established in a number of pieces of legislation to enable bodies to share data for the full range of purposes for which they are responsible (Cabinet Office, 2002, para. 3.50). The issue of gateways will be examined below.

Investigative orders under POCA

A principal mechanism for obtaining information in asset recovery investigations is the use of investigative court orders. Private sector companies are often unwilling, and sometimes legally unable, to disclose information in respect of their customers without some process which releases them from real or perceived client confidentiality and, usually, this will be a court order. In the UK, such orders will be obtained under Part 8 of The Proceeds of Crime Act 2002. Where an investigator seeks information by means of a court order, he is required to satisfy the evidential and other criteria set out in the Act. This will generally be feasible in respect of the principal defendant under investigation but it may often be difficult to convince a court that it ought to breach the privacy rights of the defendant's associates and family members in order to allow the investigators to discover whether the defendant has laundered money though them, unless the investigation can show financial transfers between the parties or that the associate holds more property than might reasonably be expected.

One can of course only analyse documentary information which exists. Police in Northern Ireland informed an Assembly Committee that the vast majority of criminals in Northern Ireland are what might be termed "spend as you go" criminals. In other words, they acquire money and it is quickly spent on alcohol, gambling, fast cars and holidays[43]. While this leaves little property for asset recovery, it may also provide fewer financial records for analysis, as much spending may have been in cash. Nevertheless, even evidence of cash expenditure can be useful to generate tax assessments in respect of criminal income.

Production Orders

Production Orders require individuals to produce documents and are frequently served on banks and other intermediaries to obtain financial records. However, they can be served on anyone who holds relevant material (including e-mails held on a computer) and might include, for example, bodies as diverse as the Student Loans Company if a person under investigation submitted information about income for the purpose of obtaining a student loan for a family member. The legislation specifically provides that Production Orders apply to information held by government departments[44]. Production Orders have effect in spite of any restriction on the disclosure of information, however imposed[45]. However, they do not enable the investigator to obtain privileged material[46] or excluded material[47].

Investigators should recognise that a court order may not result in all appropriate information being produced. An extreme example of this was demonstrated when a US Senate Subcommittee served a subpoena on Riggs Bank requiring financial documentation in respect of accounts held by former Chilean President General Pinochet. The bank initially produced material in respect of nine accounts covering

a period of eight years. Eventually, information regarding a further 19 accounts covering a period of 25 years was disclosed. When asked why the information was not disclosed earlier, bank officials identified a number of factors which had caused difficulties. Firstly, some of the accounts were over ten-years old. Secondly, other accounts had been in the name of an alias or a third party. Thirdly, relevant documents had been lost or destroyed. Fourthly, most of the individuals familiar with the accounts had left the bank. Fifthly, various Riggs Bank affiliates which opened the accounts had not fully communicated with each other. Sixthly, a senior Riggs official who was aware of many of the accounts did not identify the accounts when asked (an action which led to his subsequent dismissal)[48]. Where an investigator serves a Production Order on a financial institution, he should therefore recognise that similar factors may limit the information made available to him.

Search warrants

Inevitably, certain persons served with a Production Order would fail to comply and would conceal or destroy the material sought. Hence, there is a need to be able to execute search and seizure warrants[49]. While they will typically be executed on premises owned by defendants, they may also be used on any other premises where material might be located. This might include premises belonging to professional advisers if, for example, evidence suggested that the adviser had knowingly facilitated money laundering. Financial investigators also require the ability to obtain warrants which allow the seizure and subsequent sifting of material where the material is such that it cannot reasonably be sifted on the premises being searched. This is particularly true of computer hardrives where a decision as to whether they contain relevant material can only be made following forensic examination[50].

Customer Information Orders

Sometimes an investigator may not know which institution to serve a Production Order on. He needs to know where an individual holds an account. Customer Information Orders[51] give an investigator the ability to discover which institutions an individual holds accounts with. The order may require a bank to search for accounts held in a number of aliases or in a variety of spellings[52]. Such orders originated in Northern Ireland where police conducting proceeds of crime investigations discovered it was important to be able to trawl banks for information regarding hidden accounts[53]. Compliance with such orders is, of course, difficult for financial institutions if their records are not fully computerised. In such circumstances, a great deal of human intervention will be required to carry out a full review.

Account Monitoring Orders

Occasionally, an investigator may require not historical information of how an account has been operated, but rather future information as to how an account will be operated, allowing him to track money flows through the account to other destinations. Account Monitoring Orders require financial institutions to regularly inform the investigator as to transactions on the account, providing information which did not exist at the time the order was granted[54]. Such orders are sometimes more useful for money laundering investigations than asset recovery investigations.

Disclosure Orders

Not all financial investigations can be conducted by means of document examination. Information contained in IT systems or on paper records captures only a small proportion of the available information on an issue. Indeed, the most effective forms of money laundering are those which minimise the documentary information available to be discovered by an investigator. Sometimes, the relevant information resides in a person's mind and the investigator requires a method of compelling the individual to reveal it, hence the development of compulsory questioning powers to obtain oral information. This is particularly useful when dealing with organised crime cases, where members of the network will use threats, fear and corruption to keep information secret. Disclosure Orders enable an investigator to require an individual to attend for interview, answer questions and produce documents[55]. Failure to comply is a criminal offence[56]. The use of compulsory-questioning powers is not controversial. *Liberty* agrees that there is scope for compulsory-questioning powers to be used in organised crime cases and observes that it is common practice in the field of company law and when dealing with regulatory offences (*Liberty*, 2004b).

POCA contains two specific safeguards in respect of Disclosure Orders. Firstly, the power to seek orders is limited to civil recovery investigations being carried out by the Director of the Assets Recovery Agency. Secondly, the use of information obtained under compulsion is not available as evidence in criminal proceedings against those providing it, except in extremely limited circumstances[57].

It was anticipated that powers of compulsory disclosure would be extremely valuable in overcoming client confidentiality, concerns of professional advisers and other third parties required to provide financial information, a common block to financial investigation. This was expected to be particularly helpful in overcoming client confidentiality concerns of professional advisers and other third parties[58]. The experience has been that they are also useful in terms of obtaining information from family members of defendants and causing people to have to commit themselves to versions of events regarding the acquisition of assets early in an investigation. They also have the potential to be useful where nominee shareholders, nominee directors, shell companies and other such devices are used to conceal information of beneficial ownership. Undoubtedly, the use of compulsory questioning powers will become more sophisticated as time goes on. For example, their exercise by forensic accountants acting on behalf of the Director might have significant potential in complex cases.

There is now a definite trend towards the use of compulsory questioning powers for asset recovery and organised crime investigations in a number of jurisdictions. In Malaysia, corruption legislation provides compulsory-questioning powers in respect of excessive properties held by an individual[59]. In Ireland, a High-Court judge may order the release of information by trustees of a trust or by any other person in respect of information regarding any trust with which that person is connected[60]. This includes information into the settlor of the trust, the trustees or the beneficiaries. Such information includes documents or information held in a non-legible form. It is effectively a disclosure order limited to the field of trusts. In Australia, the Australian Crime Commission can compel production of documents and giving of evidence under oath. Only independent examiners can use these powers, subject to permission from the Commission's Board which oversees its work[61]. Such provisions are clearly being

introduced, *inter alia*, to create powers to compel individuals to reveal information which is held in their minds alone.

Other court-ordered provision of financial information

In addition to the investigative orders in POCA, there also exist other mechanisms whereby information may be ordered by the courts to be provided for asset recovery purposes[62].

Court Orders during confiscation hearings

During confiscation hearings the Crown Court has its own information-gathering power. For the purpose of obtaining information to assist it in carrying out its confiscation functions, the court may order a convicted defendant to give it information. If the defendant fails to comply with any such order, the court may draw such inference from that failure as it believes appropriate[63].

Disclosure affidavit at freezing stage

Where property has been frozen under a Restraint Order, the courts have the power to require a defendant to swear a disclosure affidavit providing information as to what assets he possesses and where these are located[64]. Although no authority on the matter yet exists, it can be anticipated that the courts will rule that there is a similar power to order a disclosure affidavit in connection with a Property Freezing Order[65]. Although the UK courts have held that they will not usually make an order directed against a UK branch of a foreign bank requiring it to produce documents held at the overseas head office relating to transactions which took place there[66], the same result may nevertheless be achieved by ordering a defendant to exhibit foreign bank statements to his disclosure affidavit[67].

There are limits as to what purposes such information may be put. In *Re O*[68] the Court of Appeal held that it would be sufficient protection of the defendant's right from self-incrimination for the prosecution to give an undertaking that no disclosure of information would be used as evidence in the prosecution of an offence alleged to have been committed by the defendant or his spouse. Thus, information disclosed can be used for asset recovery purposes but not to ground criminal proceedings for money laundering. This is because the right to a fair hearing in a criminal case has been interpreted as including a right to freedom from self-incrimination[69]. The European Court on Human Rights stated in *Saunders* v. *United Kingdom*[70] that, although not specifically mentioned in Article 6, the right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure. However, as the Northern Ireland Court of Appeal has emphasised, the European Court in *Saunders* was concerned with the use at the defendant's eventual trial of the information gained from him and was not casting doubt on the propriety of the use of compulsory powers at an earlier stage[71].

While it is true that defendants rarely provide information which investigators did not previously have, disclosure affidavits are still worth seeking. Firstly, if defendants omit assets, contempt proceedings may be brought. Secondly, some defendants do reveal previously unknown assets. Thirdly, when asked to identify the source of assets, defendants often commit themselves to a dishonest version of events which can later be disproved.

Orders on solicitors

While Customer Information Orders allow investigators to discover whether individuals hold an account with a financial institution (so that a Production Order may then be sought for relevant information) these do not apply to solicitors. However, investigators in Northern Ireland possess an additional investigation tool, currently not available elsewhere in the UK, which allows for the discovery of whether an individual is a client of a firm of solicitors. A court order can allow an investigator to serve a notice on a solicitor requiring him to provide the name, address and other information regarding any client of the solicitor in respect of any land or business; a company, firm, partnership or trust; a bank or other account; or any assets in the nature of investments[72].

The Law Society for Northern Ireland, unsurprisingly, was not in favour of this provision, saying that it was clear that the purpose of these provisions was to enable speculative trawls to obtain information about transactions conducted generally by solicitors for clients. It considered that the operation of the provisions would almost certainly involve infringements of confidentiality and privacy, not just of the person under investigation but of those persons with whom the person under suspicion had had legal dealings[73]. These arguments provided unfruitful and the power has subsequently been extended to investigators carrying out civil recovery investigations for the Assets Recovery Agency in Northern Ireland[74].

Financial Reporting Orders

The Serious Organised Crime and Police Act 2005[75] introduced Financial Reporting Orders which are available on conviction for a wide range of offences if the court is satisfied that the risk of offending is sufficiently high to justify the making of the order[76]. The normal maximum duration of this sentencing option is 15 years when imposed in the Crown Court[77]. The effect of the order is to require the offender to make reports containing specified particulars of his financial affairs. Failure to comply (or inclusion of false or misleading information) is a criminal offence punishable with up to a year's imprisonment[78]. The White Paper envisaged that these would be ancillary orders, taking effect after the offender's release from imprisonment and could constitute a requirement to file detailed six monthly returns setting out income, assets and expenditure. Released offenders might be obliged to report all bank accounts and credit cards being used, and be forbidden to carry out transactions using any other route (Home Office, 2004). In the event that an offender returned to crime, such returns might provide a vein of information for investigators. The majority of responses to the White Paper which mentioned this proposal supported it. JUSTICE regarded the use of tailored licence conditions post-release as a more creative response than simply seeking increased custodial penalties, but said that they should be imposed only where they were proportional to the offence and the risk of reoffending, given the potential infringement of the right to privacy that such financial reporting would involve, and the consequences of failing to do so. *Liberty* was more dismissive, doubting whether such a provision would be Human Rights Act compliant, and also doubting whether unrehabilitated prisoners would be likely to file returns stating their income from criminal activities. *Liberty*'s response noted that the requirements of a Financial Reporting Order could be onerous, would certainly engage Article 8 of the ECHR, and, to be justified, it would be necessary to show that the interference would serve a legitimate purpose and would be proportionate (*Liberty*, 2004c, paras 11 and 12).

Interim Receiving Orders

Under the civil recovery regime, the Director of the Assets Recovery Agency may apply to the High Court for an Interim Receiving Order[79]. Once appointed, the interim receiver performs an independent investigative function on behalf of the court. In carrying out this function, he has significant information-gathering powers. Amongst these are the power to obtain information or to require a person to answer any question. A requirement imposed in the exercise of this power has effect in spite of any restriction on the disclosure of information (however imposed)[80]. In effect, this is a free-standing power equivalent to, but more powerful than, a Disclosure Order, in that an interim receiver can require the handing over of journalistic material held in confidence[81]. Answers to compulsory questions may not generally be used against the speaker in criminal proceedings. The IRO may also empower the interim receiver to search property and remove or copy documents. In both instances, there is a protection for legally privileged material. An IRO may also require any person to whose property it applies to bring documents relating to the property which are within his possession or control within the jurisdiction[82].

Information gateways

Traditionally, the retention and use of government information is organised along departmental lines. The challenge is to overcome this fragmentation into separate "information silos" since silos create bottlenecks and delays for investigators, increasing the financial cost of investigations. The government recognises that there needs to be an efficient way of allowing access to information:

> The Government attaches high priority to protecting the rights of individuals, as its introduction of the Human Rights Act demonstrates. But an effective response to crime requires unnecessary barriers to information exchange between crime fighting agencies to be removed (Home Office, 2001, para. 3202).

Indeed, the cost of failing to share information can be high. The Bichard Inquiry Report into information-sharing in the Humberside and Cambridge Constabularies following Ian Huntley's conviction for the murders of Jessica Chapman and Holly Wells concluded that, where information is held, it must be used effectively and shared, where appropriate, with other agencies. Each part of the process must work well if the whole system is to be effective[83]. Bichard said that the lack of clear, understandable national standards and guidance on the subject of record creation, retention, review, deletion and information-sharing most likely contributed to the failure of record keeping in Humberside Police[84].

Government departments and agencies possess large amounts of information in respect of citizens and their financial affairs, and information gateways are an important mechanism permitting sharing of this. These enable sharing between two organisations where the administrative powers are not otherwise sufficient to permit the proposed sharing. They are created by legislation and generally specify the uses for which information obtained under their aegis must be used (Cabinet Office, 2002, para. 3.51). The advantage of gateways for investigators is that there is no necessity to apply for a court order and hence no need to satisfy any evidential threshold before the information is made available. Gateways represent the removal of "information firewalls" between separate government functions in circumstances where there are

legitimate reasons for this. There are, however, checks and balances. A "public authority" within the meaning of that term in the HRA, may not act in a way which is incompatible with a Convention right[85]. Thus, the exchange of information in any particular case needs to be ECHR-compliant:

> It is vital to ensure that the principles laid down in the Data Protection Act and the Human Rights Act are respected in order to safeguard the rights of individuals. But these provisions are there to prevent the unauthorised and unnecessary disclosure of information not to make it more difficult or impossible for agencies to share appropriate information. Data sharing is crucial to more effective, joined-up service provision[86].

Three sets of information gateways are noteworthy for financial investigators. Firstly, The Anti-terrorism, Crime and Security Act, 2001, passed in the wake of 9/11, opened a number of information gateways for specific purposes[87]. One gateway allowed Inland Revenue information to be shared for the purpose of assisting criminal investigations. (Since, taxation information raises particular sensitivities, this issue will be further dealt with below.) This gateway therefore enabled the usage of taxation information in confiscation investigations.

Secondly, Part 10 of POCA provides for information flows from a variety of law-enforcement bodies and government departments to the Assets Recovery Agency. Although there are a limited number of gateways specifically opened by POCA itself, the Act allows the opening of other gateways by statutory instrument[88]. One such statutory instrument has been made[89]. Information received can be used in connection with all the Director's functions[90]. These "inward" gateways provisions do not override the provisions of the DPA. They leave a discretion to the body which possesses the information and it is implicit that the provisions of the HRA need to be taken into account before the gateway is used[91]. However, criminal investigation bodies and prosecuting bodies have a statutory duty of co-operation with the Director and information provision needs to be viewed in this context[92]. The Act also recognises that the Director may need to pass information to other persons. The Director therefore has "outward" gateways to disclose information for specific purposes. These include criminal investigations and civil recovery investigations carried out overseas. The delicate nature of information relating to the tax affairs of individuals is recognised by the fact that it may only be further disclosed by the Director with the permission of the Commissioners of Inland Revenue[93]. The Parliamentary Joint Committee on Human Rights was comfortable with these gateways, commenting that they did not raise any issues relating to human rights which require to be drawn to the attention of either House[94].

Thirdly, information gateways exist under SOCPA[95]. The gateways were drawn widely to encourage "the proper and legitimate free flow of information" between the Serious Organised Crime Agency[96] and appropriate bodies, and were modelled on the gateways in POCA[97] (but are arguably wider).

The Joint Committee on Human Rights raised a number of concerns about the compatibility with Article 8 ECHR of SOCA powers in relation to the gathering, storage, use and disclosure of information. In particular, they expressed serious concerns about whether the provisions satisfied the requirement in Article 8 that interferences with private life be in accordance with the law, because the relevant provisions appeared drafted in terms too general to satisfy the requirement of foreseeability, whereby a person must be able to foresee the consequences for him of a law which potentially affects him.

The Government in its reply accepted that both SOCA's functions and the information gateway provisions were drawn widely, but argued that this was necessary "to encourage the proper and legitimate free flow of information between SOCA and appropriate bodies which will be the lifeblood for the effective and efficient functioning of SOCA". The Government therefore accepted that the powers conferred were wide, and designedly so. Its main response to the Joint Committee was that any additional safeguards would be "otiose" because both the DPA and the HRA would apply to any processing of information by SOCA. The Joint Committee commented on this argument in the context of the provisions authorising the use and disclosure of information in the Commissioners for Revenue and Customs Bill. They pointed out that, while it was legally correct to say that the duties under both the DPA and the HRA would apply, in practical terms this did not provide an answer to the lack of effective safeguards for the reasons pointed out by the Newton Committee in its review of The Anti-terrorism, Crime and Security Act, 2001. The Newton Committee had said:

> The protection offered by the Human Rights Act, 1998 and the Data Protection Act 1998 seems to us to be illusory since the burden will lie on the individual to complain about the disclosure of their confidential information in circumstances where, almost by definition, he or she will be unlikely to know that disclosure has occurred[98].

The Joint Committee also pointed out that the DPA contains significant exemptions from the Act's protections where personal data are processed for the purposes of the prevention or detection of crime, and the protection of the Common Law of confidentiality is expressly disapplied[99].

Gateways potentially represent the most powerful and effective mechanism for allowing the transfer of information between holders of it and asset recovery investigators[100].

Tax information

Sensitivities regarding disclosure of tax information means that this issue requires separate attention. Citizens are under an obligation to furnish the State with information as to income for tax purposes. It is difficult to argue, however, that, where a citizen is involved in acquisitive crime, that information should not be available to the State to provide a court with full details of the citizen's financial affairs.

The PIU Report recognised in 2000 that the Inland Revenue was heavily restricted in its ability to pass financial intelligence to other government departments and law enforcement agencies[101]. Historically, disclosures were made to other law enforcement bodies only in the event of murder or treason. Statutory provision also existed for the exchange of information with Customs and the DSS[102]. The report therefore recommended that the Revenue authorities should be allowed to disclose information to the police for criminal investigations and prosecutions. HMIC also believed this to be an effective way of tackling crime and recommended that the Scottish Executive, in consultation with law-enforcement agencies, considered how multi-agency working could be enhanced through the introduction of wider information gateways, including those with tax authorities[103]. Although the government incorporated this recommendation in the Criminal Justice and Police Bill 2001, the clauses were dropped "in the face of fierce criticism"[104] prior to the 2001 general election. Nevertheless, following the events of 9/11, the government

reintroduced the proposal. Although *Liberty* was unhappy with this, stating that it would allow the police to trawl through files held by other government departments simply on the basis that the information was useful in an investigation (*Liberty*, 2001), a tax gateway was incorporated in The Anti-terrorism, Crime and Security Act (2001).

Tax information is crucial for financial investigators who can compare information disclosed to the tax authorities with information regarding income revealed, for example, on mortgage application forms. Inconsistencies may be extremely important in demonstrating dishonesty. Ireland has also adopted a gateways solution to allow asset recovery investigators access to tax information[105]. Other jurisdictions have different mechanisms for making such information available. For example, in Grenada the Director of Public Prosecutions may, apply to a Judge for an order for disclosure of tax information[106].

Open source information

Open source information[107] is the easiest information for investigators to obtain, requiring no legal gateway or court order. Some of this information is available from public records such as the Land Registry or the Companies Registry on payment of a fee. Other information is available from commercial sources such as credit reference agencies or businesses such as 192.com.

For UK investigators to obtain open source personal information stored in private sector databases, they have to contact a variety of commercial database companies. In the USA, however, certain commercial data brokers tailor their services to law enforcement and provide comprehensive personal profiles. The US company MyPublicInfo offers a product called the Public Information Profile. For a fee, investigators can visit its website and examine all the public records about an individual from 5,000 US databases (*The Economist*, 2005). Law enforcement can thereby more quickly obtain a broad array of personal information (Hoofnagle, 2004). As more personal or property information becomes available through public records or public online access, the ability to access open-source information becomes more important to financial investigators.

Information from foreign jurisdictions

Since, defendants may try to hide assets overseas, crucial information may also reside overseas. The Courts recognise that there are attempts to evade their orders "by the manipulation of shadowy offshore trusts and companies found in jurisdictions where secrecy is highly prized and official regulation is at a low level"[108]. Investigators therefore require a means of obtaining information from overseas. However, sophisticated cross-border fraudsters attempt to use legal and organisational gaps and inadequate communication between national authorities to their advantage[109]. An example of such difficulties is that the courts in one jurisdiction are inevitably reluctant to enforce information-gathering orders issued by courts in another jurisdiction. In *Chase Manhattan Bank Na* v. *FDC Co Ltd*[110] the Hong Kong courts refused to construe "disclosure under compulsion of law" one of the *Tournier* exceptions, as including an order of a foreign court to produce documents which were in Hong Kong, since this was never within the contemplation of the judges in *Tournier*. Although the orders of the US courts were addressed to a bank in New York, they were aimed unashamedly at information held by a branch in Hong Kong and were therefore intended to have extra-territorial effect.

How do investigators seek to obtain information held abroad? Firstly, certain mechanisms which exist within POCA for obtaining information from foreign jurisdictions have been referred to earlier. Disclosure orders may require persons to bring to the UK documents which are held abroad. Interim receivers may require persons to bring to the UK documents which are held abroad. Those subject to restraint orders may be required to exhibit documents (for example bank statements from accounts held in foreign banks) to disclosure affidavits. Convicted defendants may be requested by the Crown Court to produce documentation concerning foreign held property for a confiscation hearing. However, each of these mechanisms is limited in that they require the compliance of the individual.

Secondly, there are mutual legal assistance arrangements for criminal investigations. The foundation for mutual legal assistance in Europe was laid by the 1959 Convention on Mutual Assistance in Criminal Matters and was further developed most notably through the 2000 Convention on Mutual Assistance in Criminal Matters. Information sought for use in criminal investigations, including confiscation investigations, may be sought by means of Letters of Request issued under the Crime (International Co-Operation) Act 2003 where the assistance requested relates to investigations or proceedings in respect of a criminal offence[111].

The European Judicial Network, set up by a Council Decision of 29 June 1998 with the aim of enhancing mutual legal assistance in criminal matters, consists of representatives of national judicial and prosecution authorities working on international judicial cooperation. They are designated by their governments as contact points for the exchange of information with the aim of dealing with certain serious forms of crime, mainly organised crime, in a fast and effective way.

Eurojust consists of judges and prosecutors, from each of the Member States, who assist national authorities in investigating and prosecuting serious cross-border criminal cases[112]. It does so by co-ordinating the activities of the national authorities responsible for a particular case and facilitating the collection of evidence under EU and other international mutual legal assistance arrangements (House of Lords European Union Committee, n.d., para. 11). Eurojust was established under the Third Pillar of the EU Treaty, which calls for common action among the Member States in the field of judicial co-operation in criminal matters. A Parliamentary Committee was in no doubt that Eurojust met a real and increasing need for assistance in facilitating the investigation and prosecution of complex cross border criminal cases (House of Lords European Union Committee, n.d., para. 105).

Nevertheless, mutual-legal assistance is not without its difficulties. It has previously been described as "time consuming and inefficient"[113]. Other jurisdictions have also experienced difficulties with one practitioner stating that "unless the U.S. Congress and other legislatures develop efficient means to gather admissible evidence in other countries, money laundering laws will continue barking more impressively than they bite" (Boersch, 2005).

Obtaining information for civil recovery investigations is an even more difficult task. This is because the international infrastructure for mutual legal assistance in criminal cases will not apply. Where evidence has been obtained under a Letter of Request for criminal proceedings, the issue may subsequently arise as to whether it may be used for civil recovery purposes. Although the Court of Appeal in *Barlow* held that it was admissible[114], admissibility is not the sole relevant issue. Future relationships with

the providing jurisdiction must also be considered. It is therefore desirable to seek the permission of the jurisdiction concerned.

Do other mechanisms for obtaining information exist? Firstly, the 1990 Council of Europe Strasbourg Convention was broadly drafted to enable it to cope with the confiscation of the proceeds from crime where they arose in a non-conviction environment, although that was obviously not its prime purpose[115]. The 1990 Strasbourg Convention was replaced by 2005 Convention, Article 15 of which, dealing with general principles and measures for international co-operation, clearly attempts to provide space for a new mutual assistance infrastructure to develop which will allow for assistance between States where a State is using civil recovery mechanisms for the investigation and ultimately forfeiture of criminal proceeds.

Secondly, the EU Judgments Regulation[116] and the Brussels[117] and Lugano[118] Conventions for mutual recognition and enforcement of judgments apply to judgements "in civil and commercial matters". However, where a claim is made by a public body, and is one which only a public body could make, it does not amount to a civil or commercial matter[119]. Accordingly, civil recovery rulings under POCA cannot be assisted by this means. The Harare Scheme relating to Mutual Assistance in Criminal Matters also defines "forfeiture proceedings" as being civil or criminal. However, its attempted use in civil recovery matters might nevertheless risk compromising the ECHR classification of civil recovery as civil proceedings.

Thirdly, an important development is direct agency to agency assistance. The Director of the Assets Recovery Agency may disclose information she possesses for a number of purposes, including the equivalent of civil recovery investigations and proceedings in other jurisdictions[120]. Ireland has amended its legislation to permit the Criminal Assets Bureau to assist authorities outside Ireland which have functions related to the recovery of proceeds of crime[121]. This approach may, in fact, represent the best hope for future developments.

Fourthly, the CARIN Network may be able to advise practitioners about how best to obtain information[122]. The objectives of the CARIN Network include establishing itself as a centre of expertise on all aspects of tackling criminal proceeds and promoting the exchange of information and good practice. CARIN members may exchange information with each other as far as their national legislation will allow and will advise on and facilitate mutual legal assistance which must be made through the appropriate formal legal channels.

Fifthly, information from foreign jurisdictions may be obtained through participation in Joint Investigation Teams[123]. The Convention on Mutual Assistance in Criminal Matters 2000 provides for Member States to set up JIT's for specific purposes and for limited periods. A JIT may, in particular, be set up where a Member State's investigations into criminal offences require difficult and demanding investigations having links with other Member States or where a number of Member States are conducting investigations into criminal offences in which the circumstances of the case necessitate coordinated, concerted action. Member States enter into an agreement determining the procedures to be followed by the team and will decide on its composition, purpose and duration. Article 13(10) of the Convention specifically addresses the issue of information sharing and provides that information lawfully obtained by a JIT member may be used for the number of purposes. Firstly, for the purposes for which the team has been set up. Secondly, subject to the prior consent of

the Member State where the information became available, for detecting, investigation and prosecuting other criminal offences. Such consent may be withheld only in cases where such use would endanger criminal investigations in the Member State concerned or in respect of which that Member State could refuse mutual assistance. Thirdly, for preventing an immediate and serious threat to public security. Fourthly, for other purposes to the extent that this is agreed between the Member States setting up the JIT.

Offshore data havens present a potentially even greater problem than foreign jurisdictions in that they may occupy a legal limbo which are beyond mutual legal assistance processes. An example of such is Sealand, a sea fort six miles off the English coast, which has declared statehood. The goal of HavenCo has been described as transforming Sealand into "a fat-pipe Internet server farm and global networking hub that combines the spicier elements of a Caribbean tax shelter, *Cryptonomicon,* and 007"(Garfinkel, 2000).

Financial intelligence

Some information comes to investigators as intelligence rather than in an evidentially admissible form[124]. This will often include intelligence provided by SOCA, the UK's national financial intelligence unit[125]. FIUs vary from country to country, but all of them share three core functions; they receive, analyze and disseminate information to combat money laundering and terrorist financing.

Typically, the starting point for financial intelligence is a suspicious activity report by a financial institution. Analysts then search their database to see if it contains information from other sources, including information provided by law enforcement, intelligence agencies, and foreign FIU's. Analysts also make use of publicly available information, commercial databases, and government databases maintained for the purpose of law enforcement (*Annual Report*, 2003, pp. 9-10). Using the "dots" metaphor, analysis is the stage where the dots are examined and connected. Information is put in context with other relevant data or events and meaning is derived. Analysis provides the basis for an inference or conclusion, which may lead to recommendations for action. However, the money laundering regulations generate "vast oceans of reports" leaving those responsible for reviewing those reports "drowning in data" (Gouvin, n.d.). To deal with such material, search and data-matching tools are being developed by FIU's (*Annual Report*, 2003, pp. 24-5). It has been recognised that sifting through, and making sense of, all the financial intelligence that comes to an FIU is a Herculean task and one which has not always been successfully executed in the past. Much depends on whether the FIU has the personnel and resources to rise to the challenge (Gouvin, n.d.; Fleming, 2005).

The issue for investigators is what use to make of intelligence provided to them. Firstly, intelligence can be used to identify the location of assets for confiscation or civil recovery purposes. Such assets may then be investigated using traditional means. Secondly, attempts can be made to turn intelligence into evidence. The most obvious way of doing so is to use intelligence as providing the basis for a reasonable suspicion that the individual has benefited from acquisitive crime[126]. Applications can then be made for search and seizure warrants, production orders and other investigative tools. In civil recovery cases it also may be possible to treat intelligence as hearsay evidence. A few individual pieces of intelligence may not be capable of being given evidential weight. However, if the intelligence is extensive then police may be able to swear

an affidavit setting out that there has been a flow of intelligence (for example that a particular person has been involved in drug trafficking), that this intelligence has come from a variety of sources over a prolonged period, and that it has led police to the firm belief that the individual is a drug trafficker. The court may be willing to put limited evidential weight on such an assessment. Nonetheless, this approach may lead to disclosure demands by the defence and it may be necessary to hold PII hearings in order to protect intelligence sources.

Social networks

Financial investigation is more than simply document examination and it requires an investigation into relationships between people. Beneficial owners of criminal assets often place them in others' names so as to conceal them. Social network analysis may therefore be important to discover in whose name a criminal might be hiding assets. Comprehensive financial investigation cannot however be done without a surveillance capability to discover who the target meets with and where he visits. The investigator may also require the ability to access whatever communication channels are being used, whether they be telephone, e-mail or personal meetings.

Information from telephone intercepts

A debate on the appropriate use of telephone intercept product in the UK has taken place in recent years[127]. The Regulation of Investigatory Powers Act 2000 prohibits the evidential use of UK intercept material in UK court proceedings[128]. This is unusual internationally. On the one hand, the evidential use of intercepts may hold out the prospect of prosecutions in some cases where they would not otherwise have been possible, and might encourage earlier guilty pleas. On the other hand, there is a concern that the evidential use of intercepts would reveal capabilities which could undermine the effectiveness of intercepts and damage the co-operation between intelligence and law-enforcement agencies in tackling terrorism and serious crime. The government has said that if it were satisfied that adequate safeguards could be designed to prevent the disclosure of sensitive capabilities, and that the benefits of this would clearly outweigh the costs, then it would bring forward legislation to allow the evidential use of intercept material (Home Office, 2004, para. 6.2.2).

If legislation is brought forward to allow the admission of intercept products as evidence, there would be distinct advantages in permitting it to be used in asset recovery proceedings and not just in a limited range of criminal cases.

Shared databases

In the past, public sector information was held on discrete databases which were effectively isolated from other sources of information, and had relatively small capacities for storing information. Advances in technology now mean that databases can hold much more information and it is much easier to link information between databases and to transfer data between them (Cabinet Office, 2002, para. 3.13). Developments such as digitization, exponential increases in information processing and concomitant increases in storage capacity, enormous growth in network bandwidth, and the common, decentralized architecture of the internet (Hurley, 2003) present the public sector with new opportunities that make using and sharing data much easier and more affordable (Cabinet Office, 2002, para. 1.05).

It has been recognised that better sharing of information between government departments can lead to the identification and reduction of fraud (Cabinet Office, 2002, para. 4.24). However, integrated law-enforcement computer databases (*Government Computing News*, 2002) raise a "big brother" concern for others (*Government Computing News*, 2001). Such persons fear a "dataveillance society"[129], in which privacy is routinely overridden by ever-more powerful systems of data collection, storage, exchange, matching and mining operating across private global networks (Perri 6, 1998). Nevertheless, privacy-enhancing technologies are advancing and evolving rapidly, and processes and safeguards can be built into system design from the outset to ensure that personal privacy is protected. These safeguards can restrict access to information to selected persons, restrict the information that each person can access and can keep a register of who has accessed what information and for what purpose (Cabinet Office, 2002, para. 3.14). The information which can be stored on individuals also raises civil liberties issues. The most serious concern would be the linking of distinct databases coupled with ever more powerful search engines. The individual pieces of information may not themselves be sensitive but the aggregation or joining together may give added value (*foresight*, 2000).

Such developments offer significant opportunities for law enforcement. However, some fear a deliberate decision to abandon a law enforcement paradigm for investigation of individuals and the substitution of an intelligence paradigm that seeks to secretly gather all information that might turn out to be useful (Gouvin, n.d.).

In order to optimise European law-enforcement co-operation, the Dublin Declaration[130] recommended that the effective collection, storage, analysis and exchange of data must be consistently promoted under the umbrella of a comprehensive EU law-enforcement information policy. It recognised the value of existing data would be enhanced by networking existing databases through data-mining and automated collection mechanisms and by using their contents as integral elements of high-performing data analysis strategies. Nevertheless, it acknowledged any future action in this area should take account of data protection in law-enforcement co-operation and so strike the appropriate balance between robust data protection and data security on the one hand and high performing use of law enforcement data at affordable costs on the other.

Shared databases may be of great potential for asset recovery investigators. Financial investigators need to be able to be make better use of emerging technologies as part of the wider strategy to deliver effective asset forfeiture.

Information offences and sanctions

Financial investigators are often concerned that assets will be dissipated. However, it may be that a greater risk is the dissipation of information, since once destroyed it may not be recoverable. Given this problem, sanctions are necessary in respect of those who actively seek to frustrate information-gathering by concealment, deletion or by creation of false information. There are three approaches to such sanctions.

Firstly, there are a range of criminal offences available to prosecutors depending on the facts. These include attempting to pervert the course of public justice[131] and false accounting[132]. Criminal offences also exist in respect of telling others that investigators are gathering information, for example by way of production order[133]. These are important since knowledge that an investigation is underway could enable a defendant to destroy or conceal documents which have not yet been seized or copied. Though proving the leakage of information regarding an investigation

may be difficult, nevertheless these are important offences which should be prosecuted where evidence exists, as there will usually be very strong public interests for doing so.

Secondly, there may be occasions where a defendant has refused to comply with a court order to provide information. While such non-compliance can be criminalised[134], the usual sanction to force compliance is contempt of court proceedings. However, the maximum penalty for contempt proceedings arguably requires review on the basis that concealment of information requires to be dealt with as severely as the concealment of assets. Comparing the two year maximum penalty for contempt with the maximum ten year default sentence for non-compliance with a confiscation order, the two penalties seem inconsistent. In proceeds of crime cases where action may be being taken against significant organised crime figures, there is an argument for concluding that the maximum contempt penalty ought to be significantly increased.

Thirdly, where there has been failure to comply with a court order concerning the provision of information, a court may be willing to draw an appropriate inference to the defendant's detriment either in civil[135] or criminal proceedings[136].

Developing legal tools

The legal tools used to obtain information require to be kept under review. The Australian Law Reform Commission, in its examination of asset forfeiture law, received a submission that law enforcement information gathering powers were, in general terms, too cumbersome, limited in scope and had too high a threshold (Canberra, 1999, para. 19.13). The Commission concluded that the effective use of the full range of asset forfeiture powers had been inhibited by the inability of law-enforcement agencies to obtain, by a simple, quick and effective process, information regarding the existence, nature and content of bank accounts kept by, or on behalf of, suspected persons and their associates (Canberra, 1999, para. 19.69).

Where weaknesses exist, new informational tools are created. For example, the US Patriot Act created a mechanism to enable the authorities to access foreign bank records. The Act requires foreign banks to appoint a person in the USA to accept service of legal process and gives the US authorities the power to issue a subpoena to any foreign bank which maintains a correspondent account in the USA and to request records relating to that account, including records maintained outside US borders[137]. This type of requirement on banks is only possible where jurisdictions possess considerable economic power. However, given the UK's significance as a major banking centre it would be open to the UK to impose such a requirement on foreign banks. It would also be possible for the EU as a whole to impose such a requirement on banks which desire a presence in the EU. Another example of new legal tools is a provision where, when a defendant in a US civil forfeiture case refuses to waive secrecy or produce records of financial accounts in a bank secrecy jurisdiction in response to a discovery request, this may result in the dismissal of his case with prejudice[138].

Legal tools may be necessary in some jurisdictions to cope with computer encryption. Much information can be held by an individual on his computer and the increased use of encryption has caused difficulties for investigators. Legislation currently allows for persons to be served with a notice requiring them to hand over encryption keys. It is a criminal offence to fail to do so[139]. However, the focus of attention in this context has been on indecent images and on terrorist activities (*The Times*, 2006).

It is inevitable that criminals are using encryption to conceal accounting records too and some foreign jurisdictions position such an offence in their criminal proceeds legislation[140]. An offence of failing to hand over encryption keys, backed by sufficiently tough penalties, is therefore an important legal sanction.

An interesting potential development is an administrative means of obtaining banking records rather than a court-ordered means. The Australian Law Reform Commission recommended a move to the former, exercisable only at a senior level (Canberra, 1999, para. 19-79). In the UK, the Newton Committee also suggested such a regime, arguing that "internal authorisation" could be justified for the disclosure of information in respect of terrorist or other types of serious crime[141].

Financial investigators need to have close interaction with policymakers to explain what financial information is difficult to obtain with currently available tools, so that policymakers can consider what new information-gathering tools need to be developed.

The need for training

The PIU Report recognised that financial investigation and asset recovery were seriously under-utilised in the UK. For asset recovery to be maximised, there was an evident need to train specialist investigators with appropriate levels of financial investigation skills. Since, then, there has been significant change. The National Policing Plan 2004/2007 provides that financial investigation should become an integral part of police work, with confiscation orders and money laundering prosecutions pursued as a matter of course wherever appropriate[142]. The National Policing Plan also provides that awareness of financial investigations should be promoted. The Asset Recovery Agency's Centre of Excellence has contributed significantly, building capacity in asset recovery through the development and delivery of financial investigator training[143].

There are eight core information skills which investigators and organisations must develop for effective asset recovery. Firstly, information planning skills: knowing what information is needed to support the delivery of asset recovery. Secondly, information searching and retrieval skills: knowing how to determine whether information exists, where it is available and how it can be accessed. Thirdly, information evaluation skills: understanding how to assess the value of information in terms of relevancy, accuracy and authenticity. The correct interpretation of the information obtained will depend on the knowledge that a financial investigator possesses. Fourthly, documentation and recordkeeping skills: knowing when and how to document activities, decisions and transactions adequately for legal needs. Fifthly, record management skills: being able to organise, file, and store paper-based and electronic information effectively. Sixthly, access and privacy management skills: knowing how to obtain authorised access and protect record-confidentiality. Seventhly, knowledge management skills: knowing how to capture and share the knowledge of colleagues and others to support creative problem solving. Eighthly, technology skills: being able to use new technologies to support these activities[144]. The effectiveness of financial investigation will depend on whether these skills have been acquired through the training provided.

A multi-disciplinary approach

Organised criminals often employ complex corporate and financial structures to launder their proceeds (Home Office, 2001, para. 3.193). Once information regarding

these has been obtained, investigators often need the specialist skills of others to analyse that information, as the skills necessary to gather such material will not always be the same as those necessary to analyse it. When criminals are relying on expert advice from accountants and lawyers (*Financial Times*, 2005), it is important that investigators have access to similar advice.

International best practice in asset recovery investigations is therefore characterised by a multi-disciplinary approach. An example of this can be seen in Canada where the Integrated Proceeds of Crime Units include lawyers, tax investigators, forensic accountants and police. The multi-disciplinary approach has been taken further in Ireland where a multi-agency approach has developed. The critical distinction between these is that, in the latter, each person brings with him the powers and rights of his parent agency, including rights of access to information. The Irish Criminal Assets Bureau has demonstrated significant success with its teamwork of police officers, Customs officers, Revenue officers, Social Welfare officers and forensic accountancy expertise. An informational perspective on multi-agency working suggests that a fundamental reason for the Bureau's effectiveness may be because of these rights to access information. Arguably, while a multi-disciplinary approach still leaves information in silos, the multi-agency approach brings those silos together.

Conclusion

Asset recovery investigation involves the obtaining and analysis of relevant financial information held by the public and private sectors. It has been said that "data sharing is a key to modernising government" (House of Lords Debates, 2000) and, similarly, it may be a key to modernising law enforcement. Ill-gotten gains can be hard to identify and it is important to have the necessary tools to attempt to do so[145]. Inadequate information-gathering powers will only result in ineffective recovery of criminal proceeds. The widening of financial investigation powers is a response to the money laundering techniques increasingly used by criminals. Investigation powers need to be kept under regular review to ensure they do not need to be enhanced.

In some jurisdictions, there is a fear that investigative powers are being strengthened while civil liberties weakened (*The Age*, 2004). Concern also exists about the potential loss of personal data and the misuse this might be put to (*New York Times*, 2005). *Liberty* has suggested that there has been a fundamental shift in the nature of the State's attitude to individual privacy and that we are moving from a position where information is not shared unless necessary, towards one where it will be shared unless there is a reason not to (*Liberty*, 2004a, para. 4). While there are those who argue that society is choosing between the invasion of privacy and the protection of privacy:

> ... the true choice may between a society altered by legislative and executive action to the extent necessary to hamper the misuse of civil privileges by criminals, or a society altered by the conditions created by those criminals and their activities[146].

The right to privacy and effective financial investigation are not mutually inconsistent goals. It is possible and desirable to achieve both objectives. Asset recovery is a public service and it is the State's obligation to deliver it in the most efficient and cost-effective way consistent with privacy rights and obligations, providing value for money in what is delivered by law enforcement. Doing so will require making better use of financial information held by public-sector agencies.

Revisiting the metaphor of information as "dots" inappropriate barriers to dot collection and sharing need to be identified and eliminated. It has been suggested that the fundamental barriers to this arise from the legal, policy, and cultural "rules" which exist[147]. It is hoped, however, that this paper demonstrates that, as far as UK asset recovery is concerned, legal rules do not generally cause significant difficulty. Problems are therefore more likely to stem from organisational cultures. In particular, two cultures prevent information-sharing. The first is a culture of fear and uncertainty. Organisations can adopt a safety-first approach, hiding behind the existing legal framework as the key barrier to data-sharing[148]. In reality, public servants fail to share information out of fear of being blamed for inappropriately releasing it. The second culture is a controlling one. Bureaucracies can possess a strong tendency to hoard information rather than share it[149]. A US Commission observed that the term information "sharing" suggested that the government entity that collects the information "owns" it and can decide whether or not to "share" it with others. The Commission rejected this concept, stating that information collected by any government agency belonged to the government and that officials were fiduciaries who held the information in trust for the nation. They did not have authority to withhold or distribute it except as provided for by law. There should be a move toward a culture of "stewardship" of information instead of ownership[150].

Just as managers of any manufacturing business must pay attention to the supply chain and ensure that suppliers provide raw materials in the most cost-effective manner, so too managers of organisations must ensure that the supply chain of information operates effectively and efficiently for asset recovery. There is an obligation on government to use available public-sector information in the most efficient and effective way possible to achieve legitimate goals (Cabinet Office, 2002, p. 5). This will involve strong leadership, holding accountable those who fail to share information appropriately. Information management responsibilities should therefore be incorporated into managers' performance evaluations[151]. Feedback might also be sought from those to whom information ought to be being supplied to ensure that appropriate stewardship is being exercised.

One area where the legal rules on information sharing are deficient is in terms of international sharing. Asset recovery in organised crime cases which cross national boundaries requires clear information sharing on an international basis. Arrangements for this need to be effective and efficient. A new global infrastructure needs to be developed to allow information-sharing assistance to be given for non-conviction based asset recovery proceedings.

Information is the lifeblood of a financial investigation. Since, all financial information is potentially useful, there needs to be no form of financial information which is beyond the reach of an investigator in an appropriate case. If there is, criminals will utilize that weakness to place criminal assets where information in respect of those assets cannot be obtained. If asset recovery is to be successful, it is essential that investigators are able to collect the dots, connect the dots, and share the dots.

Notes

1. Part 8 of the Proceeds of Crime Act 2002 categorises investigations into confiscation investigations, civil recovery investigations and money laundering investigations. For the purpose of this paper, the term "asset recovery investigations" will be used to refer to the first two categories.

2. The HM Crown Prosecution Service Inspectorate has stated: "Too many police forces keep financial intelligence in silos when it can play a part not only in asset recovery but also the investigation of murder and other serious crimes." Payback Time, the Report of the Joint Review of Asset Recovery Since, the Proceeds of Crime Act 2002, para. 19.
3. *A-G* v. *Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109.
4. *Coco* v. *A. N. Clark (Engineers) Ltd* [1969] RPC 41.
5. The operation of the duty of confidence can be seen in *Jackson and Another* v. *Royal Bank of Scotland* [2005] All ER (D) 280 (January).
6. [1924] 1 K. B. 461.
7. J. Moscow, New York District Attorney's Office, in a speech at a conference marking the first anniversary of Jersey's Financial Services Commission, 12 July 1999.
8. R. Wright, Director of the Serious Fraud Office, in a lecture entitled 'The Globalisation of Crime: The Electronic Dimension" to the 1997 Cambridge Symposium on Economic Crime.
9. *Jones* v. *Smith* [1999] 1 SCR 455.
10. *R* v. *Derby Magistrates Court ex parte B* [1996] 1 AC 487.
11. Hereafter referred to as "ECHR".
12. *R (MorganGrenfield & Co. Ltd)* v. *Special Commissioner for Income Tax* [2003] 1 AC 563.
13. *Balabel* v. *Air India* [1988] 1 Ch. 317.
14. *Three Rivers District Council and others v Governor and Company of the Bank of England (No. 6)* [2004] 3 WLR 1274.
15. *R* v. *Cox and Railton* [1884] 14QBD 153, citing with approval *Gartside* v. *Outram* (1857) 26 L.J. (Ch.) 113 in which Sir William Page-Wood stated "there is no confidence as to the disclosure of iniquity."
16. [1988] 3 All ER 775.
17. "The erosion of the attorney-client privilege and work product doctrine in federal criminal investigations: a report prepared by the American College of Trial Lawyers" (2003) 41 Duq. L. Rev. 307.
18. *R* v. *Manchester Crown Court, ex parte Rogers* [1999] 1 WLR 832.
19. [1987] 3 All ER 1025.
20. See for example *R* v. *Department of Health, ex parte Source Informatics Ltd* [2000] 1 All ER 786.
21. The ECHR is not the only human rights instrument which deals with privacy and information issues. Article 12 of the Universal Declaration of Human Rights provides that a person shall be free from "arbitrary interference with his privacy, family, home or correspondence." There are also international accords on privacy: the 1980 OECD Guidelines for the Protection of Privacy and Trans-border Flows of Personal Data and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.
22. Article 8 provides: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
23. *Belgian Linguistic Case*, (1968) 1 E.H.R.R. 252.

24. Application number 6959/75, decision of 12 July 1977.
25. *Z* v. *Finland*, (1998) 25 E.H.R.R. 371.
26. *Kruslin* v. *France*, (1990) 12 E.H.R.R. 297.
27. Investigators seeking court orders will have to satisfy courts that an infringement of a person's Article 8 rights is proportionate to the benefit to be gained from making an order or granting a warrant. Code of Practice issued under section 377 of the Proceeds of Crime Act 2002, para. 12.
28. *Olsson* v. *Sweden* (No. 1), (1989), 11 E.H.R.R. 259.
29. 9804/82 (December) 7 December 1982 31 DR 231.
30. The Code of Practice issued under section 377 of the Proceeds of Crime Act 2002 reminds financial investigators that they will have to satisfy a judge that any infringement of an individual's Article 8 Convention Rights is proportionate to the benefit to be gained from making an order or warrant.
31. Hereafter referred to as the "DPA".
32. Letter from Caroline Flint MP, Parliamentary under Secretary of State, Home Office, re Serious Organised Crime & Police Bill, set out in Joint Committee On Human Rights – Eighth Report, 23 February 2005, Appendix 2a.
33. *Campbell* v. *Mirror Group Newspapers Ltd*, [2003] QB 633.
34. Schedule 1 to the Act provides that data handlers must ensure that data are: (1) fairly and lawfully processed; (2) processed for limited purposes; (3) adequate, relevant and not excessive; (4) accurate; (5) not kept for longer than is necessary; (6) processed in line with individuals' rights; (7) secure; and (8) not transferred to countries without adequate protection.
35. The Schedule 2 conditions include (1) the data subject has given his consent to the processing; (2) the processing is necessary for compliance with any legal obligation to which the data controller is subject; (3) the processing is necessary for the administration of justice or for the exercise of any functions conferred on any person by any enactment or for the exercise of any functions of a government department and (4) the processing is necessary for the purposes of legitimate interests pursued by the data controller. The Schedule 3 conditions include (1) the data subject has given his explicit consent to the processing of the personal data; (2) the processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); (3) the processing is necessary for the exercise of any functions conferred on any person by any enactment or for the exercise of any functions of a government department.
36. Paragraph 6 of Part II of Schedule 1.
37. Often referred to as a "section 29(3) form".
38. The Green Paper "New powers against organised and financial crime" stated "There is a common perception in both the public and the private sector that data sharing is made almost impossible by the Data Protection Act. In reality, data protection will not create insuperable barriers to legitimate, proportionate data sharing – and it is difficult to see why this misperception has gained such common currency among policy makers and front line staff" Cm 6875, July 2006, p. 13.
39. This is the so-called "Ram doctrine" derived from advice by Sir Granville Ram, First Parliamentary Counsel 1937-1947. See Cabinet Office (2002, para. 3.46).
40. See, for example, *Associated Provincial Picture Houses* v. *Wednesbury Corporation* [1948] 1 KB 223, 233-234.
41. [1992] 2 AC 1.
42. Anti-terrorism, Crime and Security Act 2001 Review: Report, 2003, HC 100, para. 161.

43. Evidence of D/Supt Thompson to *Ad hoc* Committee – Financial Investigations (NI) Order 2001, para. 52.
44. Other jurisdictions provide an alternative mechanism for dealing with government departments, namely by providing for an order specific to such departments. For example, section 60 of Grenada's Proceeds of Crime Act 1992 provides: "Notwithstanding any provision in this or in any other law the Court may on the application by the Director of Public Prosecutions order the person in charge of any Government department or statutory body to produce or furnish to the Director of Public Prosecutions or any other person specified in the order any document or information which is in his possession or under his control or to which he may reasonably have access (not being a document readily available to the public) which the Court considers relevant to any investigation into, or proceedings relating to, a scheduled offence alleged or suspected to have been committed by any person."
45. POCA section 348(4).
46. POCA s 348(1).
47. POCA s 348(3). "Excluded material" is defined by sections 11-12 of the Police and Criminal Evidence Act 1984 as including personal records relating to an individual's physical or mental health or to counselling given to him; human tissue or tissue fluid taken for the purposes of diagnosis or medical treatment; and journalistic material held in confidence.
48. "Money laundering and foreign corruption: enforcement and effectiveness of the Patriot Act" Supplemental Staff Report on US Accounts used by Augusto Pinochet, US Senate Permanent Subcommittee on Investigations, March 2005, pp. 10-11.
49. POCA, s 353(3) and (4).
50. Seize and sift powers are available under sections 50-70 of the Criminal Justice Act 2001.
51. POCA, ss 363-364.
52. Minutes of Evidence of Power, D., NI Bankers' Association, to *Ad hoc* Committee – Financial Investigations. (NI) Order 2001, 9 January 2001, para. 194.
53. Evidence of D/Supt Thompson to *Ad hoc* Committee – Financial Investigations (NI) Order 2001, 8 January 2001, para. 25.
54. POCA, s 370(6).
55. POCA, s 357(4). A Disclosure Order does not confer the right to obtain privileged material or excluded material.
56. POCA, s 359.
57. POCA, s 360.
58. PIU Report, para. 7.47.
59. The Anti-Corruption Act 1997, s 22.
60. The Proceeds of Crime (Amendment) Act 2005, s 18.
61. Australian Crime Commission Act 2002, ss 24A – 36.
62. There are separate information-gathering powers in respect of terrorism investigations which also have asset forfeiture application but are outside the scope of this paper.
63. POCA, s 18.
64. Under previous legislation this was on the basis of the High Court's inherent jurisdiction: *Re O* [1991] 2 W.L.R. 475. POCA s 42(7) effectively gives a similar jurisdiction to the Crown Court.
65. POCA, s 245A.
66. *MacKinnon* v. *Donaldson, Lufkin and Jenrette Securities* [1986] Ch. 482.

67. The Northern Ireland High Court has made one such order in an unreported ruling. *In the matter of Paul Arthur Maye*, 2 July 1999, Kerr L.J.
68. The decision in *Re O* was approved by the House of Lords in *A T & T Istel and another* v. *Tully and others*, [1993] A.C. 45. However, the High Court accepted in *Re C* that the undertaking might not be wide enough to protect the defendant and varied the Restraint Order, adding to the usual undertaking: "and no use shall be made in any such prosecution against the defendant of evidence obtained as a direct result of such disclosure." Times Law Reports, 21 April 1995.
69. *Funke* v. *France* (1993) 16 E.H.R.R. 297 and *Murray* v. *United Kingdom* (1996) 22 E.H.R.R. 29.
70. [1998] 1 BCLC 362.
71. *Clinton* v. *Bradley*, Northern Ireland Court of Appeal, 12 April 2000, (Unreported).
72. Proceeds of Crime (Northern Ireland) Order 1996, Article 49(1).
73. Minutes of Evidence to the *Ad hoc* Committee on the Financial Investigations. (NI) Order 2001, Mr J. Neill, 9 January 2001, para. 352.
74. Criminal Justice (Northern Ireland) Order 2005, Article 15.
75. Hereafter referred to as "SOCPA".
76. The first such order was granted in the case of *R* v. *Abdullah Baybasin* on 19 June 2006 at Woolwich Crown Court.
77. Or 20 years if the offender is sentenced to life imprisonment: SOCPA, s 76.
78. Whether this potential penalty is sufficient to deter a convicted criminal who re-engages in acquisitive crime with a view to replacing those assets he has lost under a confiscation order and who therefore reports false information is debatable.
79. POCA, s 246 (hereafter referred to as "IRO").
80. POCA, Schedule 6, para. 2.
81. This is because Schedule 6 of POCA contains no exception for "excluded material" unlike the Disclosure Order power.
82. Proceeds of Crime Act 2002, s 250(2).
83. The Bichard Inquiry Report, HC 653, 2004, para. 4.39.
84. The Bichard Inquiry Report, HC 653, 2004, Introduction, para. 41.
85. Human Rights Act 1998, s 6(1).
86. "Criminal justice the way ahead" para. 254.
87. Sections 17-20 of, and Schedule 4 to, the 2001 Act.
88. POCA, s 438.
89. The Proceeds of Crime Act 2002 (Disclosure of Information) Order 2003. (SI 2003 No. 335.)
90. POCA, s 435.
91. Explanatory Notes: Proceeds of Crime Act 2002, Home Office, para. 578.
92. POCA, s 4.
93. POCA, s 437.
94. Joint Committee on Human Rights, Session 2001-2002, Third Report, HC 405, 26 November 2001, para. 53.
95. Serious Organised Crime Act 2005, ss 32-35. Any person may disclose information to Serious Organised Crime Agency if the disclosure is made for the purposes of the exercise by SOCA of any of its functions. A disclosure under this section does not breach – (1) any obligation of confidence owed by the person making the disclosure, or (2) any other restriction on the

disclosure of information (however imposed). But this does not authorise: (1) a disclosure, in contravention of any provisions of the DPA, of personal data which are not exempt from those provisions, or (2) a disclosure which is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000. Information obtained by SOCA in connection with the exercise of any of its functions may be disclosed by SOCA if the disclosure is for any permitted purposes, namely: (1) the prevention, detection, investigation or prosecution of criminal offences, whether in the UK or elsewhere; (2) the prevention, detection or investigation of conduct for which penalties other than criminal penalties are provided under the law of any part of the UK or of any country or territory outside the UK; (3) the exercise of any function conferred on SOCA by section 2, 3 or 5 of SOCPA; (4) the exercise of any functions of any intelligence service within the meaning of the Regulation of Investigatory Powers Act 2000; (5) the exercise of any functions under Part 2 of the Football Spectators Act 1989 (c. 37); and (6) the exercise of any function which appears to the Secretary of State to be a function of a public nature and which he designates by order.

96. Hereafter referred to as "SOCA".
97. Letter from Caroline Flint MP, Parliamentary Under Secretary of State, Home Office, to the Joint Committee on Human Rights regarding the Serious Organised Crime and Police Bill, Joint Committee On Human Rights, Eighth Report, 23 February 2005, Appendix 2a, para. 6.
98. Anti-terrorism, Crime and Security Act 2001 Review: Report, 2003, HC 100, para. 164.
99. Joint Human Rights Committee, Eighth Report, 23 February 2005, para. 2.7.
100. This assumes that there are no cultural and mindset barriers which prevent the gateways from operating effectively.
101. The Finance Act 1982, s 182(1) provided that a person who discloses any information which he holds or has held in the exercise of tax functions is guilty of an offence if it is information about any matter relevant, for the purposes of those functions, to tax or duty in the case of any identifiable person. Currently, confidentiality of tax information is governed by sections 17-23 of the Commissioners of Customs and Revenue Act 2005.
102. Finance Act 1972, s 127 and the Social Security Administration Fraud Act 1997, s 1.
103. "Making crime pay: confiscation of criminal assets in Scotland" Her Majesty's Inspectorate of Constabulary for Scotland, June 2000, para. 6.14-15.
104. "Parliamentary brief: anti-terrorism, crime and security bill – House of Commons, 19 November 2001" Law Society for England and Wales.
105. Disclosure Of Certain Information For Taxation And Other Purposes Act, 1996, s 1.
106. The Proceeds of Crime Act 1992, s 55.
107. This may be defined as information of potential value that is available from public sources.
108. *International Credit and Investment Co. Ltd* v. *Adnam* [1998] BCC 134, 136.
109. This is reportedly the conclusion of the Federal Audit Court in Germany: *The Financial Times* (2005).
110. [1985] 2 HKC 470.
111. If the Act were to be amended to allow the Director of the Assets Recovery Agency to issue Letters of Request in respect of civil recovery investigations, this might assist. While there would be no bilateral or multi-lateral instrument underlying this, and no guarantee that jurisdictions would respond co-operatively, its existence would represent another helpful step forward.
112. Eurojust was established by a Council Decision of 28 February 2002. *Official Journal*, L 63, 6.3.02, p. 1. Based in The Hague, it consists of one member for each Member State either a prosecutor, judge or police officer.

113. Memorandum by JUSTICE to the House of Lords Select Committee on the European Communities, 9 Report, 1998-99, "Prosecuting fraud on the communities' finances" HL Paper 62, p. 121.
114. *Barlow and Another* v. *BOC Ltd and Another*, Court of Appeal, 8 June 2001.
115. This is clear from the explanatory report (for example, para. 23 deals with the matter as does para. 15).
116. Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ 2001 L307/29.
117. The 1968 Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (as amended). For a consolidated text, see OJ C 27, 26.1.1998, p. 1.
118. Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, OJ L319, 25.11.88, p. 9.
119. *Netherlands* v. *Ruffer* [1980] ECR 3807 and *LTU* v. *Eurocontrol* [1976] ECH 1541.
120. POCA, s 438(1)(h). She may not, however, release information received from Commissioners of Customs and Excise or of Inland Revenue without their consent: POCA, s 437.
121. Proceeds of Crime (Amendment) Act 2005, s 15.
122. In October 2002 a proceeds of crime conference was held in Dublin co-hosted by the Criminal Assets Bureau and Europol. One of the recommendations arising was to consider the establishment of an informal network in the area of criminal asset identification and recovery. The name agreed for the group was "the Camden Assets Recovery Inter-Agency Network" (the Camden Court Hotel in Dublin being the original location of the workshops where the initiative started). The official launch of CARIN took place at the CARIN Establishment Congress in The Hague, 22-23 September 2004.
123. Hereafter referred to as "JIT's".
124. Hereafter referred to as an "FIU". Intelligence has been defined as "the considered and analysed product of systematic information gathering" "Blueprint for Policing in the 21st Century." Association of Chief Police Officers of England, Wales, and Northern Ireland. London, 2001.
125. Recommendation 26 of the Financial Action Task Force's 40 Recommendations states that "Countries should establish an FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of Suspicious Transaction Reports and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of Suspicious Transaction Reports." The global association of national FIU's is known as the Egmont Group. In an EU context there is a Council Decision concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. Council Decision 2000/642/JHA, 17 October 2000.
126. *O'Hara* v. *Chief Constable of The Royal Ulster Constabulary* [1997] AC 286.
127. A Private Members Bill, the Interception of Communications (Admissibility of Evidence) Bill, was introduced in the House of Lords by Lord Lloyd on 10 October 2005. In February 2006 the Home Secretary said the government was examining the issue "very actively and seriously" with a view to seeing how it can introduce an appropriate regime for the evidential use of intercept evidence. Hansard, House of Commons, 2 February 2006, col. 482. The Joint Coomitee on Human Rights recommended on 1 August 2006 that the ban on the use of intercept evidence in court should now be removed: 24th report, Counter-Terrorism Policy and Human Rights – Prosecution and Pre-charge Detention, HC 1576, para. 101.

128. *R* v. *P* [2002] 1 AC 146.
129. The term was introduced and popularised by Clark (1991).
130. The first European Congress on Developing Partnerships Between the Public and Private Sectors to identify, measure and prevent harm from organised crime, was held in Dublin on 20th and 21st November 2003. The purpose of the Declaration is to assist the further development of European and international co-operation across the private and public sectors and to strengthen measures, standards, best practices, and mechanisms to reduce and prevent harm from the activities of organised crime.
131. Contrary to Common Law.
132. Theft Act 1968, s 17.
133. Prejudicing a civil recovery investigation: POCA, s 342 and Tipping Off: POCA, s 333.
134. POCA, s 393.
135. POCA does not provide a statutory basis for suggesting that a court may draw an inference in recovery proceedings from a failure to answer questions, though this may be the result in practice.
136. POCA, s 18.
137. Article 319(b). Having a legal power and exercising that power are, however, different matters. It has been suggested that the US Justice Department "is often reluctant to authorize such subpoenas for fear of offending foreign sensibilities" (Boersch, 2005, p. 10).
138. Civil Asset Forfeiture Reform Act 2000, s.17.
139. Regulation of Investigatory Powers Act 2000, s 53.
140. Criminal Property Confiscation Act 2000, s. 76(1)(f). (Western Australia).
141. The Anti-terrorism, Crime and Security Act 2001 Review: Report, 2003, HC 100, para. 170-1.
142. Police Sector Skills Foresight 2004, Skills for Justice, para. 5.3.6.
143. Asset Recovery Agency, *Annual Report 2004-05*, pp. 24-9.
144. Speech by the Information Commissioner of Canada entitled "Information Management in the Government of Canada" Ottawa, 28 July 2004.
145. One blogger clearly fails to understand information-gathering powers: "There's a story on the BBC news site today about an ice cream salesman who has run into problems with the Assets Recovery Agency in Northern Ireland. The Agency claims his lifestyle could not possibly be sustained by the income from his fairly modest ice cream business and they have seized his assets including houses worth 1.5 million pounds... I would also love to know how the hell the Asset Recovery Agency has access to the sort of information that led them to this conclusion" www.dongxi.org/goblinblog/2005/06/long-way-round.html However, as criminals increasingly understand information-gathering powers, there will be a greater tendency to deal primarily in cash or through alternative remittance systems so as to avoid leaving a paper or electronic trail.
146. Corruption in Queensland Report, 1989, Fitzgerald QC 1987-89 Fitzgerald Commission of Inquiry into Police Corruption in Queensland.
147. Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 31 March 2005, p. 441.
148. See Cabinet Office (2002, para. 10.19). This view has been confirmed in the Green Paper "New powers against organised and financial crime" which stated " Some of this new data sharing might require legislative changes; in particular changes to the vires of agencies whose data sharing is governed by statutory provisions. Much should be achievable simply through a more robust approach to the use of existing powers . . . " Cm 6875, July 2006, p. 13.

149. Speech by the Information Commissioner of Canada entitled "Information Management in the Government of Canada" Ottawa, 28 July 2004.

150. Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 31 March 2005, pp. 430 and 444.

151. Speech by the Information Commissioner of Canada entitled "Information Management in the Government of Canada" Ottawa, 28 July 2004.

References

(The) Age (2004), "Revealed: the new police arsenal", *The Age*, 6 December.

Annual Report (2003) Financial Transactions and Reports Analysis Centre of Canada.

Boersch, M. (2005), "Global reach of U.S. laundering laws hindered by weak legal tools", *Money Laundering Alert*, February p. 10.

Cabinet Office (2002), *Privacy and Data-sharing, The Way Forward for Public Services*, The Mall, London, Annex A, Admiralty Arch.

Canberra (1999), "Canberra Confiscation that counts: a review of the Proceeds of Crime Act 1987", Australian Law Reform Commission Report No. 87.

Clark, R. (1991), "Information technology and dataveillance", in Dunlop, C. and Kling, R. (Eds), *Computerisation and controversy: value conflicts and social choices*, Academic Press, Boston, MA.

(The) Economist (2005), "A PIP of progress; identity theft", *The Economist*, 16 July.

Financial Times (2005), "Crime rings 'find Germany a haven for fraud'", *The Financial Times*, 2 August.

Fleming, M.H. (2005), *UK Law Enforcement Agency Use and Management of Suspicious Activity Reports: Towards Determining the Value of the Regime*, Jill Dando Institute of Crime Science, London.

foresight (2000), "Just around the corner: a consultation document", *foresight*, March.

Garfinkel, G. (2000), "Welcome to Sealand", *Now Bugger Off. Wired Magazine*, July, p. 230.

Gibson, W. (1988), "Johnny Mnemonic", *Burning Chrome*, HarperCollins, London.

Gouvin, E.J. (n.d.), "Bringing out the big guns: the USA patriot act, money laundering, and the war on terrorism", *Baylor L. Rev.*, Vol. 55, p. 955.

Government Computing News (2001), "Data sharing tightens net for the law", *Government Computing News*, Vol. 7 No. 7.

Government Computing News (2002), "Pennsylvania, FBI share crime data", *Government Computing News*, Vol. 21 No. 3.

Home Office (2001), "Criminal justice: the way ahead", CM5074, Home Office, London.

Home Office (2004), "One step ahead: a 21st century strategy to defeat organised crime", Cm6167, Home Office, London.

Hoofnagle, C.J. (2004), "Big brother's little helpers: how choicepoint and other commercial data brokers collect and package your data for law enforcement", *University of North Carolina Journal of International Law & Commercial Regulation*, Vol. 29, p. 595.

House of Lords Debates (2000)Vol. 196, p. 196, WA.

House of Lords European Union Committee (n.d.), "Judicial co-operation in the EU: the role of Eurojust", 23rd Report of Session 2003-04 HL Paper 138.

Hurley, D. (2003), *Human Rights in the Information Society*, International Centre for Human Rights and Democratic Development, Montreal.

Liberty (2001), "Anti-terrorism, crime and security bill 2001 – briefing for the second reading in the House of Commons", *Liberty*, November.

Liberty (2004a), "Identity cards bill: liberty's briefing for second reading in the House of Commons", *Liberty*, December.

Liberty (2004b), "Reconciling security and liberty in an open society", *Liberty*, August, p. 44.

Liberty (2004c), "Serious organised crime and police bill – liberty's briefing for the second reading in the house of commons", *Liberty*, December.

Libicki, M.C. and Pfleeger, S.L. (2004), "Collecting the dots: problem formulation and solution elements", Occasional Paper, Rand Corporation, Santa Monica, CA, January, p. 1.

New York Times (2005), "Another data broker reports a breach", *New York Times*, 10 March.

Perri 6 (1998), *The Future of Privacy: Private Life and Public Policy*,Vol. 1/2, Demos, London, pp. 179-80.

(The) Times (2006), "Paedophiles encrypting computer files to evade detection", *The Times*, 12 June.