"Les Uns et les autres – The role of personal and organisational circumstances in knowledge development and acquisition"

Author information

Ana Isabel Canhoto
London School of Economics, Houghton Street, London WC2A 2AE, England, a.i.canhoto@lse.ac.uk

James Backhouse
London School of Economics, Houghton Street, London WC2A 2AE, England, james.backhouse@lse.ac.uk

Submitted to OLKC 2006 Conference at the University of Warwick, Coventry on 20th - 22nd March 2006

Abstract

The collection and analysis of financial data, referred to as financial intelligence, is gaining recognition as a key tool in the war on crime in general and terrorism in particular, and there is a burgeoning industry providing sophisticated computer technology and complex mathematical models to mine financial data and single out unusual patterns of transactions. The process to develop financial intelligence has quantitative roots, yet it gives rise to critical cognitive issues. By treating financial intelligence development as a communication process, the paper examines the role of signs, affordances and norms in determining the emerging profile. The discussion highlights the growing role of “management of meaning” as organisations strive to comply with regulatory requirements. Important insights emerge regarding the social and pragmatic aspects of financial intelligence development, and how technology affects both the content of the profiles that can be developed and the variety of crimes that can be monitored at any stage.

Knowledge development and acquisition in organisations

The social constructionist approach to knowledge creation in organisations views organisations’ employees as social beings who construct their understanding of the world from social interaction with other employees (Gherardi and Nicolini 2000) within specific socio-cultural and material settings (Edmondson 1999). The individual members of the organisation contribute to the organisations’ knowledge structures by communicating their knowledge to other members of the organisation. In turn, the actions and the knowledge structure of the members of the organisation are also influenced by the organisation’s culture (Akgun, Lynn et al. 2003). Organisational knowledge is a combination of cognitive and social processes, and emerges as a result of the interaction of, among other factors, identities, rules, language, interests and artefacts (Easterby-Smith, Crossan et al. 2000).

One particular aspect of the organisational context that has the potential to frame knowledge is technology. Technology may play a supporting role in organisations by assisting in the collection, administration and communication of information available (McGrath and Berdhal 1998; Griffith, Sawyer et al. 2003), as well as linking employees in remote physical locations (Griffith and Neale 2001). Additionally, technology may provide information about the relationship between different tasks and pieces of data, this way creating information where it did not exist before (Zuboff 1988; Griffith, Sawyer et al. 2003). Research regarding the role of technology in knowledge creation and/or management, however, has mostly focused on technical aspects such as database design and data warehousing, with insufficient consideration being given, in the organisational learning and knowledge creation literature, to the social factors that may impair the effectiveness of technical implementations (Easterby-Smith, Crossan et al. 2000).

Financial intelligence, the systematic collection and analysis of data relating to financial transactions, makes extensive use of technology. Indeed, the use of automated monitoring systems is often seen as a powerful ally in the fight against money laundering and terrorist financing, justified by the increase in size of the typical transactional database, and by a desire to keep compliance costs under control (Canhoto and Backhouse 2004). As a result, there is a burgeoning industry providing sophisticated computer technology and complex mathematical models to mine financial data and single out unusual patterns of transactions. Yet, little has been written on the impacts of technology on the development and acquisition of financial intelligence in and by organisations. This paper addresses such gap, examining the role of technology in financial profiling and uncovering how the rich interplay between the organisational, individual and technological dimensions fundamentally impact on the outcomes of profiling, First, the paper provides a brief overview of the increasing importance of technology in financial intelligence. Next, it outlines the technique of developing profiles of financial behaviour, examining how cognition and cultural norms may impact on the profiling exercise. The article goes on to present a framework that treats the intelligence building process as an act of communication. The approach is applied to an empirical setting to investigate how the nature of the signs available, technology and task affordances and behavioural norms all affect the outcomes of profiling. The final section presents implications of these findings for organisations that rely on financial behaviour profiles for the prevention and detection of criminal activity.

Financial intelligence

While money laundering is not a new phenomenon, formal initiatives to detect and combat this criminal activity are relatively recent - the first international agreement making money laundering a criminal act was the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, also known as the Vienna Convention, signed in 1988. The international fight against money laundering gained further momentum in the wake of several high profile terrorist attacks worldwide, most notably, the attacks of September 11th 2001 in the USA. Indeed, some of the most important and far reaching provisions introduced by the Patriot Act were in the field of financial regulation and prosecution for money laundering (Goede 2004). Anti money laundering programmes aid in crime prevention by visibly removing the financial reward for those engaging in criminal activity. Additionally, the programmes aid in the detection of criminal activity directly, by triggering a criminal investigation, as well as indirectly by contributing to an existing investigation – e.g., by uncovering links between associates, by demonstrating the movement of money or goods, or by eliciting the modus operandi of a given criminal group.

In the UK, there is a regulatory requirement for financial institutions to observe *due diligence* with respect to the activity of their customers. The country's financial regulator puts forward two instruments for anti money laundering control: *know your customer* (KYC) – 'obtaining and using information about a customer over and above the basic identification information' - and *monitoring* - 'being alert to how a customer is using a firm's products and services and therefore to signs of money laundering' (FSA 2003). The requirement to detect suspicious activity consequently demands from financial institutions knowledge of the normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity (Basel 2001).

Nowadays, it is difficult for any person to manage his or her day-to-day activities without using the banking system. Having a bank account enables individuals to, among other things, pay bills, receive salary payments and store money securely, while also earning interest. The same applies to individuals engaged in criminal activity who may be interested in using the banking system to increase their wealth or move money between associates possibly in more than one country. It is also important to note that transactions are increasingly taking place in electronic form, which leaves an 'electronic trail' (Levi and Wall 2004) that is easy to monitor. It is, therefore, not surprising that anti money laundering initiatives worldwide place an enormous emphasis on the banking system's ability to detect and alert to potential money laundering activity.

The detection of suspicious activity is a complex and resource intensive task (Watkins, Reynolds et al. 2003), however, and many financial institutions have opted for automated monitoring solutions to fulfil the regulatory requirement (Veyder 2003). A survey of 1,337 UK financial companies shows that over 80% of UK banks with 1,000 or more members of staff have adopted automated transaction monitoring systems (Gill and Taylor 2003). The high adoption rate of such systems was also partly driven by the series of fines imposed by the financial regulator on several UK financial institutions that, arguably, breached anti money laundering requirements (Kitano 2005). The total amount of fines between 2002 and mid 2005 exceeded £6 million, with the highest single fine applied in 2003 and exceeding £2 million (FSA 2003; Kitano 2005).

The exact technological solution adopted by each bank varies, and includes vendor solutions, centrally developed intelligence used in a local context, employment of in-house data miners to develop ad-hoc queries and adoption of models developed by the relevant FIU (RSM 2002; Canhoto and Backhouse 2004). The automated monitoring systems process the large volume of financial transactions, using data mining technology that employs statistical analysis and artificial intelligence (Brenneman and DeLotto 2001; Complinet 2005) to flag non-obvious relationships between pieces of data in large input data sets or to look for unusual patterns of behaviour – for example, by flagging sudden cash movements in a previously dormant bank account (Kitano 2005). The following section provides a brief overview of the data mining, the technology underpinning the development of financial intelligence.

Cognitive issues in profile development

The study of patterns of behaviour and the grouping of users according to exhibited behaviour is called behaviour profiling. Behaviour profiling uses detailed records of the relationship between the organisation and the user, such as records on product usage, account balance or transaction history. Beyond just knowing that someone did something, behaviour profiling involves capturing records of events and actions over time and using these stored records of interactions to model typical behaviour and deviations from that behaviour (Lenzen 2004). Sometimes, this is augmented with data from outside databases, such as census data (Funsten 1998). The traditional method of turning data into knowledge relies on manual analysis and interpretation. The manual method, however, is becoming impractical as data volumes grow exponentially (table 1) and, nowadays, the process is highly automated and dependent in computer technology.

Table 1: The typical size of some databases

Types of Databases	1999	2004	Growth in size
Transactional	100 gigabytes	1 terabyte	9 times
Data warehouse	1 terabyte	100 terabytes	99 times
Data mart	20 gigabytes	1 terabyte	49 times
Mobile data	100 megabytes	10 gigabytes	99 times
Pervasive data	100 kilobytes	1 gigabyte	9,999 times

Source: (Hardy 2004)

The processing of the data includes several steps, ranging from data selection and preparation to the interpretation of the emerging results. A thorough review of the data mining process is beyond the scope of this paper. Rather, we wish to focus on the role of the profile developer in the data mining process, both in terms of the input for the data mining effort and in terms of analysing the output.

The input to the data mining process is a collection of data objects organised in a database, and the actual data interrogation process will usually start with the specification of the problem domain and an understanding of the goals of the project. Such specification is usually done by the business users who impart domain knowledge to the analyst (Kohavi, Rothleder et al. 2002). The following stage comprises an assessment of the existing knowledge, as well as of the data that needs to be collected. The target dataset resulting from this stage is pre-processed and, later, interrogated in order dig pieces of knowledge from the database (Bruha 2000). The choice of the model to interrogate the data is subject to human judgement and tends to be heavily influenced by the data miner’s experience, the model’s robustness and its interpretability, as well as the total cost of implementing the analytical solution (Fayyad, Piatetsky-Shapiro et al. 1996; Lenzen 2004). The final stage consists of examining the outcomes of the data mining process, and interpreting and using the resulting information. At this stage, it may happen that the volume of rules generated far exceeds the capacity to manually inspect them (Liu, Hu et al. 2000), in which case it is necessary to prioritise which patterns to analyse. The prioritisation criteria can be classified as objective when they depend solely on the structure of the pattern and the underlying data used in the data mining effort; and classified as subjective when they also depend on the users who examine the data mining output.

At the end of the data mining process, the analyst has to judge whether the outcomes are possible, internally consistent, and plausible (Chung and Grey 1999). The results typically raise further questions (Kohavi, Rothleder et al. 2002), sometimes in conflict with previously believed knowledge (Fayyad, Piatetsky-Shapiro et al. 1996), often leading to the generation of new hypotheses and the start of a new data mining cycle.

In summary, even though data mining is a largely quantitative and automated process, the analyst plays a crucial role in several steps. Human cognitive factors can affect the data mining exercise (Chung and Grey 1999; Pazzani 2000). Also, technology can affect the analyst’s work. For instance, it has been shown that technology impacts on cognition by preconditioning the characteristics of the stimuli available (Sund 2003). Additionally, the technical platform chosen to process the data may increase the salience of particular pieces of information which, in turn, cues attention and influences how a person thinks about a given problem (Potter and Balthazard 2004). This cuing effect seems to be bigger for those users of technology with lower levels of knowledge about the task or with less experience with problem solving (Mennecke, Crossland et al. 2000). Technology can also affect cognition by affecting how individuals communicate and, therefore, what is communicated (Te'eni 2001; Parsons 2002).

While some of the impacts of technology on organisations are intentional and planned and, therefore, predictable, others are more opportunistic and unanticipated. The possibility of unanticipated outcomes requires from the organisation immediate monitoring of emergent changes in ongoing practices (Orlikowski 1996; Orlikowski 1996). Given that the war on money laundering impacts on everyday financial life, transforming the relations between banks and their clients (Goede 2004), it is pertinent to ask, in the context of development of financial intelligence, how do the personal and organisational circumstances surrounding the analyst, including technological platforms, influence how specific intelligence is perceived and communicated?

We analyse this question by comparing the intelligence building process to an act of communication between three analytical levels that are very different in nature: 1) the technical level that captures and manipulates the data, 2) the informal level of human interactions in the process of giving meaning to the data provided by the technical level and acting upon this knowledge and 3) the formal level of the organisation where these agents participate. The communication metaphor is inspired by Smith, Blackman et al.'s (2003) study of the implementation of a customer relationship management system in a UK mapping agency. Looking at knowledge management has a communication issue, facilitates the individual analysis of each element in the system, thus leading to an '*incremental understanding within the system*' (Smith, Blackman et al. 2003).

In order to study the profiling activity as a communication process, we use semiotics, as well developed body of communication theory that has been used to analyse a wide range of artefacts and social practices (Pagel and Westerfelhaus 2005).

Semiotics

Semiotics, the theory of signs, draws on different disciplines to explain not only what words mean, but also the process by which meanings are made. A key concept in semiotics is the *sign*. A sign is 'everything that, on the grounds of a previously established social convention, can be taken as something standing for something else' (Eco 1976). For instance, a red rose is not only a flower but also a symbol of love in Greek mythology, a symbol of martyrdom in Christian iconography and the logo for the UK's Labour party. Furthermore, the red rose is not a sign in itself but only when, and if, it is recognised as so in a given social group. Charles Peirce (1931-58) suggested the word *representamen* to designate the material form of the sign which 'may embody any meaning' (2. 229), the word *object* to indicate that for which the representamen stands for, and the word *interpretant* to identify the convention linking the sign and the object together. The interpretant may be embodied in the person involved in reading or interpreting the sign, and to whom the signification makes sense (Liu 2000). Peirce emphasis that the sign exists in the intrinsic nature of the triadic correlation as a whole: 'A sign mediates between the interpretant… and its object' (Peirce 1977). That is, the sign is not a thing, rather it is a relation between three correlates (Nake 2002). Or, in other words, the sign is the meaning attributed to the representamen, such as the red rose, by the interpretant, and this meaning may differ depending on the context or time.

The process through which an agent attributes meaning to a sign is called *semiosis* (Morris, 1938/1970). Semiosis explains the creation and use of any type of sign processing activity, is capable of identifying anything present according to a specific norm, can make anything not present identifiable and is subject-dependent (Liu 2000). Semiosis can occur at several levels, and the result will depend on the point of view of the agent and on the knowledge available.

The fact that a sign requires a socially accepted convention in order to have meaning, and that meaning is subject-dependent, in turn, leads to two fundamental constructs: *affordance* and *norms*. The semiotic affordance is a natural extension of the theory of affordances developed by direct perception psychology (Gibson 1979) and refers to the patterns of behaviour made possible by some combined structure of organism and its environment. For example, a user and a web browser together afford surfing the web (DeMoor 2002). The semiotic norms are the social equivalent of the affordance in the sense that they provide the socially acceptable repertoire of behaviour. For example, the Hippocratic ideals, the health service concern with affordable medicine, political principles of equitability and practices of communication between medical hierarchies all guide the actions of members of a hospital (Liebenau and Harindranath 2002). Of particular importance to the study of behaviour in organisations is the distinction between informal, formal and technical norms. Informal norms are habits and unofficial conventions which may have been verbally agreed or even never verbally mentioned but that people will follow, nonetheless. For instance, the generally accepted convention that investment bankers may wear casual clothing on

Fridays but are not to do so on any other day of the week. Formal norms are those that have been officially documented, such as national laws, industry regulations or organisational policies. When formal norms are so exactly specified that they can be automated and executed by a computer, they become technical norms. The technical norms are embedded in the formal norms and these are interpreted through the prevalent informal norms. That is, two groups guided by different informal norms may react differently to the same formal or technical norm. So, the affordances refer to the possible meanings of the sign, whereas the norms refer to the accepted meanings of the sign.

The branch of semiotics that studies the creation of meaning in an organisational setting is usually referred to as *organisation semiotics*. Organisation semiotiocians adopt the subjectivist paradigm as its philosophical stance (Stamper 1973; Liebenau and Backhouse 1990), defending that meaning is created subjectively and socially, leading to subtle differences between groups of knowing agents. Different groups within an organisation typically have varying levels of access to information and, therefore, diverse, and eventually, conflicting perceptions.

Semiotics and organisational knowledge

Scholars working in such diverse disciplines as security, cultural studies or management have employed semiotic theory to study knowledge acquisition and dissemination in organisations, alternatively focusing on the characteristics of knowledge signs and on the process of interpreting such signs. Desouza and Awazu (2004) indicate that the organisation's 'knowledge space' is composed of knowledge objects that can be classified according to their granularity and context – data regarding sales of a particular book constitutes a knowledge object of low granularity and low context, whereas the book sales of a firm in relation to the sales of books in the industry are at the other end of the spectrum. Most importantly, the authors conclude that the knowledge objects that are context related are the ones that are most valuable for firms because they tend to be rare, inimitable and non-substitutable. The authors also mention that context-related knowledge is generated differently in different organisations, and requires different management approaches (Desouza and Awazu 2004).

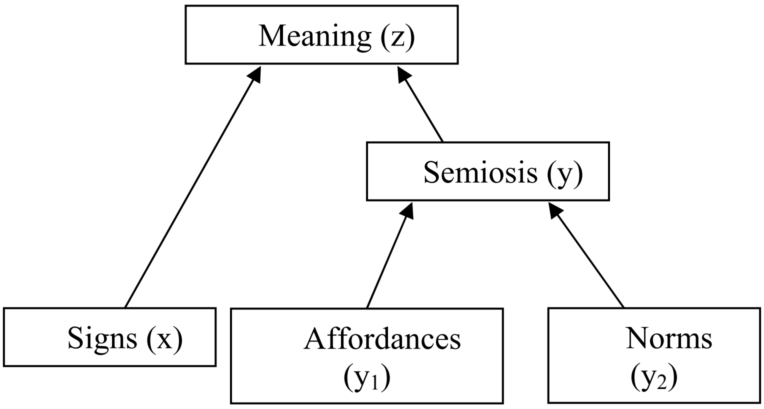
Pagel and Westerfelhaus (2005) also investigated the link between signs and context, looking specifically at the topic of written knowledge. The authors examined the reading habits of managers, analysing the interaction between text, reader and context. The study identified several rules governing the choice for particular types of texts, as well as the process of interacting with those signs or knowledge objects. The researchers concluded that the process of knowledge acquisition of the managers surveyed was influenced by three factors – time pressures, dissemination requirements and potential resistance from sceptical audiences. These three factors influenced the managers' preference towards texts that were succinct, simple and clear (Pagel and Westerfelhaus 2005). On a different line of investigation, Jahoda (2001) used semiotics to analyse the process of acquisition of knowledge about the 'other' and concluded that, since our psychological system is set up to make distinctions, one person's interpretations of signs about the 'other' are also based on distinctions. Moreover, such interpretations are value-laden regarding people's perceptions of, and beliefs about, 'others'. The author highlights that, even though the characterisation of the 'other' may be deliberate, in many circumstances it is quiet unwitting (Jahoda 2001).

The studies identified above highlight, alternatively, the role of different types of signs and of semiosis on knowledge acquisition and dissemination in organisations. Moreover, the studies emphasise the role of affordances and norms in such process. The present paper takes these insights further, exploring how technological, social and personal factors interplay and affect the knowledge emerging in the organisation. That is, how do artefacts, affordances and norms frame financial intelligence development?

Research framework

The research framework illustrated in figure 1 highlights the relevance of semiotics for understanding the emergence of organisational knowledge, and can be summarised as follows. Knowledge development is a process of attributing meaning (*variable z*) to specific signs (*variable x*) through semiosis (*variable y*). Different analysts may reach diverse conclusions because they focus on distinct signs or because they interpret the same sign differently as a result of disparities in what the analysts are afforded to do (*variable y_1*) or the norms that guide the analysts' behaviour (*variable y_2*).

Figure 1: Research framework



In the context of financial intelligence, the signs are the knowledge objects available to or in the organisation. Examples include identity data such as the customer's date of birth, name and address, as well as activity data such as the customer's spending patterns or product acquisition. The affordances are the possible actions that the organisation's technical artefacts and/or employees can perform such as manipulation of data and dissemination of information. Finally, the norms are the range of accepted actions at the technical level – for instance, which employees are given usernames and passwords that grant them access to particular databases – at the formal level – for instance, the organisation's policy for development of algorithms – or at the informal level – for instance, the ad-hoc discussion of relevant snippets of news among colleagues. In summary, the framework proposed enables the analyst not only to detect the directions of intelligence emerging in the organisation, but also how such knowledge is shaped by the attributes of the technical artefacts, the nature of the tasks or the prevalent technical, formal and informal norms.

Research methodology

The research framework depicted in figure 1 was applied in an interpretative, qualitative case study of the sources and content of financial intelligence in a UK bank to be referred to a BANK, and resulted in the development of a holistic, detailed and rich perspective of the phenomenon under scrutiny (Creswell 2003). The process of financial intelligence development at BANK mirrors that of similar institutions. It includes extensive brainstorming sessions, some very institutionalised and taking place at regular intervals, some on an ad-hoc basis, in order to gather the latest available information regarding the identity and the methods of money launderers. Such models of who money launderers are and what they do are then crystallised in rules which are later transformed into profiling algorithms that search through BANK's databases of identity and transaction records.

Data for this study was collected via interviews, observation and analysis of documents, in a financial organisation to be referred to as BANK, over a period several months in 2004 and 2005. Furthermore, the authors used two semiotic tools, semantic analysis and norm analysis. Semantic analysis enables the analyst to elicit and specify the elements that compose the information system, and the relations between them. The resulting semantic model, also called an ontology chart, represents the possible actions that the elements of an organisation can perform. These actions, the affordances, are ontologically dependent on the agent performing them. The affordances are linked by lines if there is an ontological dependency, with the antecedents on the left and the dependents to the right. The meaning of a sign is treated as a relationship between the sign and the appropriate actions, and the chart maps the vocabulary and the temporal relationships between the perceptions that those words represent (Stamper 1996). The second tool, norm analysis, enables the researcher to capture the various norms that condition the agent's behaviour. So, the ontology charts make it possible to elicit the beliefs afforded to the different roles in the organisation, while norm analysis explores the informal, formal and technical rules that shape the beliefs within those roles.

In order to protect the organisation's security and operational interests, all names and figures have been disguised.

Case study

Responsibility for the development of financial intelligence at BANK lies with a small team, herewith referred to as the financial intelligence (FI) team. The FI team is also in charge of developing algorithms to search through BANK's automated transaction monitoring system (ATMS). The specific technical solution in place uses a neural network system to monitor account transactions. Transaction data is fed into the ATMS from the organisation's various legacy systems overnight. The system was first implemented in 2003 and it is still undergoing developments, in particular regarding the process and the type of SQL rules used.

The inputs that the team considers for the intelligence building process are drawn from a pool of external and internal sources (table 2). Some sources are considered more valuable than others: The knowledge that another bank, widely regarded as a leader in anti money laundering monitoring, was targeting certain geographical areas and commercial organisations quickly prompted BANK to develop similar rules. By contrast, the information that one law enforcement unit is monitoring a specific age group did not prompt BANK to apply the same rule, which was justified by the fact that the given organisation faces ‘other type of money launderers’.

Table 2 – Signs considered in the intelligence building process

External to the organisation	Internal to the organisation	
	Outside of the FI team	In the FI team
Financial intelligence unit Law enforcement agencies Other banks Research bodies Press	Fraud department	Reports of success stories

Similarly, some signs are considered more relevant than others. In particular, BANK is interested in signs concerning the crimes that it considers more likely to be perpetrated by its client base. For instance, given that it has branches in areas where terrorist cells are suspected of being active, it has devoted considerable resources to the development of profiles of terrorist financing activity.

Some of the data obtained by the FI team has a factual, denotative nature, demonstrating that specific behaviour is or were pursued by known money launderers, as illustrated in the quote below:

> *“We had a couple of cases where we had good hits - for instance, a human trafficker that we helped to get arrested coming out of the branch. It was a*

> *huge success and it is good feedback to the team. Because we don't get a huge feedback…"*

Information of this nature is the most valued by the team because it clearly establishes the relationship between banking and criminal behaviour:

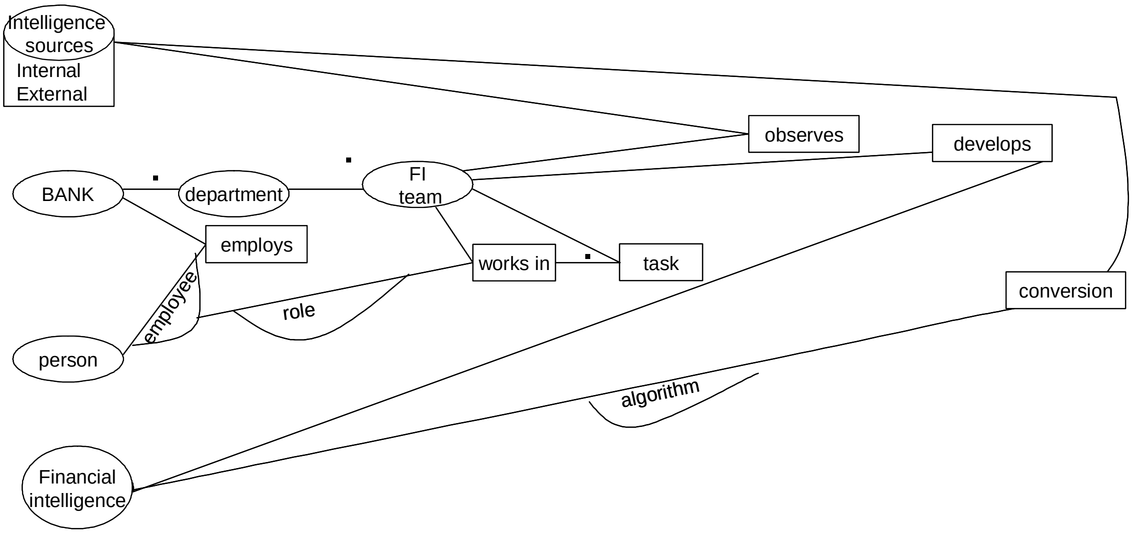
> *'I told them of the stolen vehicles that went to [country x] and other countries that [drive on] the left. I told them about the scam and the referral we had. When we investigated, it was a [specific type of commercial organisation], and the only thing that was happening was money coming into the account from [country x], and then going out. But there was nothing else: no salary payments, no bills…'*

However, instances of denotative information do not occur systematically. Moreover, they tend to deal with unique, unrepeatable events upon which a judgement must still be made regarding the application of that knowledge to other situations.

Most descriptive information available at BANK is of an affective nature, embodying value judgements of which transactions are likely to reflect money laundering activity, or which businesses or post codes are particularly risky. One example was the development of an algorithm to monitor the business accounts linked to a specific type of commercial organisation and whose postal code indicated that they were located along the border of two particular countries. Such rule was developed following news that a known terrorist group smuggled items traditionally traded by such organisations, in order to fund its terrorist activity. The accounts flagged by this rule were subsequently investigated by the analysts who, in the absence of intelligence regarding which commercial organisations were under the control of the terrorist group or which were the specific patterns of transactions of a 'legitimate' organisation of that type as opposed to one controlled by the terrorist group, could only but guess which outlets were engaged in suspicious activity.

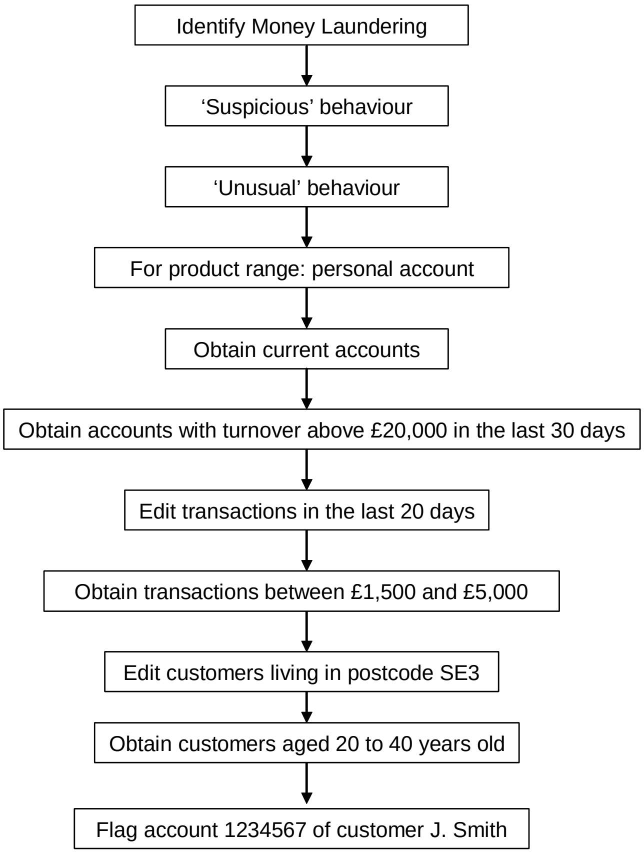
The allocation of meaning (variable *z* in figure 1) to the signs (variable *x*) just described, is performed by the FI team. That is, it is an affordance (variable y_1) of the individual members of the team, while employees of BANK (figure 2). The semantic analysis also identified affordances that are specific to each role in the team and that emerge from the team members' different ontological positions in the organisation. For instance, one of the team's members participates in several executive committees and steering groups which grants him a wide view of the operations of the organisation, but also exposes him directly to cost-control pressures. Another member assists marketing department colleagues in their profiling efforts and, hence, obtains insights regarding the typical revenue and spending patterns of particular types of business, or the socio-demographic profile of residents in selected postal codes.

Figure 2 – Semantic analysis



Having studied the behaviours afforded to the FI team members, the next step was to analyse the behaviours allowed to those same employees by force of the informal, formal and technical norms (y_2). For the purpose of this paper, we focus on the development and use of one specific algorithm to monitor possible tax evasion. The patterns of banking behaviour that are deemed suspicious of representing this crime are described at decreasing levels of abstraction and *translated* into the machine language, SQL, until specific unambiguous criteria are reached, as illustrated in Figure 3. The process aims to connect otherwise disparate pieces of personal, product and transaction data into a complex formula. The descent from the most abstract level to more concrete ones requires decisions between various possible alternative solutions, focusing the attention on a few specific concrete paths.

Figure 3 – Process of objectification of financial intelligence[1]


Identify Money Laundering
'Suspicious' behaviour
'Unusual' behaviour
For product range: personal account
Obtain current accounts
Obtain accounts with turnover above £20,000 in the last 30 days
Edit transactions in the last 20 days
Obtain transactions between £1,500 and £5,000
Edit customers living in postcode SE3
Obtain customers aged 20 to 40 years old
Flag account 1234567 of customer J. Smith

The decision between specific paths is determined by technical norms, such as the maximum number of algorithms that can run on the system at any moment. As a result, the system's administrator switches rules on and off according to external events (e.g., a terrorist attack), internal priorities (e.g., suspicion that BANK has been targeted by a fraud ring) or the lack of activity from a given rule (e.g., if the number of alerts from a rule falls below a given threshold). The choice between paths is also affected by formal norms such as the rule that personal accounts can not be used for business purposes. This is because of internal policies such as different fees charged for the two types of accounts, as well as external regulations. Finally, there are informal norms such as the desired level of output. In order to keep the number of alerts within a level that can be analysed by the team of analysts within a given period, the rules are often fine tuned and narrowed.

[1] The exact criteria have been disguised to protect the strategic and security interests of BANK

Discussion

The financial services' regulator points two pillars for an effective anti money laundering strategy: enhanced customer identification procedures and transaction monitoring. Yet, no concrete directions are given to the institutions regarding what constitutes suspicion. That is partly due to the very nature of the phenomenon – a secretive, illegal activity – and also due to the fact that there is no systematic procedure to feed back into the monitoring institutions which suspicions were eventually confirmed or not. The analysis of meaning developed in the previous section revealed that the process of creating and disseminating financial intelligence at BANK is not the discovery of an 'objective' truth, in which the 'methods' are neutral techniques (Punch 1998; Bisman and Hardcastle 1999) separated from the value system of the analyst. Rather, 'subjectivity matters' (Riessman 1994).

The abstract definition of what constitutes legitimate financial behaviour and what reflects suspicious criminal activity is achieved by way of 'definition by context'. Suspicious behaviour is not defined extensively because it is not known what all the possible criminal behaviours are. And it is not defined operationally because it is not possible to know, in the whole, all the properties of money laundering behaviour. Hence, the definition of suspicious behaviour is done in the context of normal behaviour of a given customer or usual utilisation of a given banking product. This enables the FI team to advance some general laws about how money laundering occurs, such as the use of large quantities of cash or the quick defunding[2] of an account.

Likewise, it is not possible to objectively measure the approximation of the definition adopted by the FI team and the 'reality' of money laundering behaviour. It is only possible to talk about the fit over a range of instances of money laundering processes and instances of banking behaviour. Hence the vast majority of information circulating in the organisation regarding what is or isn't money laundering is of an affective, rather than denotative, nature. That is, embodies more values than facts. That does not mean that the definition should be dismissed, but its nature and limitations must be recognised, namely the permeability to the cognitive and task

[2] Technical term referring to the withdrawal of over 75% of an account's balance over a very short period of time

constraints of those in charge of construing the definition. What is essential is that those involved in developing and applying financial intelligence is aware of the tensions herewith described, and periodically checks the quality of the information being circulated.

The analysis above also studied the impact of affordances on knowledge. It was revealed that while the FI team members have the same general affordance, their specific positions in the organisation gives them access to different pieces of information, and requests, thus possibly leading to varying profiles. The specific affordances of each member of the FI team are caused by unique ontological positions, and lead to differences in terms of point of view and knowledge. As Berger and Luckmann (1966) explained, a society's body of knowledge is structured in terms of relevance, and the areas of knowledge that are likely to be relevant to the members of a social group are determined by the members' pragmatic interests and situation in society. The member that participates in steering committees will be more sensitive to group-wide concerns with financial risk management, for instance. BANK's management may find it useful to look for ways to increase the relevance of these measures to the other FI team members, be it in their daily tasks, or as a component of their job evaluation.

The technical norms limit not only the content of the rules that can be developed, but also the variety of crimes that can be monitored at any time. BANK runs the risk of focusing on prototypes of high volume criminal behaviour, rather than what could be more damaging to the institution or more relevant to the country's anti money laundering objectives. In turn, the formal norms provide explicit guidance regarding the legitimate use of particular types of accounts. Finally, the use of specific formulas is determined by pragmatic interests. That is, individuals draw on a flexible set of tools or 'repertoire' of habits and techniques (Swidler, 1986, Swidler, 1997, Tilly, 1992) that are actively deployed by the individuals in order to pursuit valued ends. It is important for financial intelligence management to investigate the ways in which differing environmental cues situate particular cultural frames and, therefore, meanings.

Financial intelligence officers are catching up with criminality, an ever changing field marked by secretive behaviour, and the ever growing variety of possible avenues to disguise money laundering. While the FI team's management is aware that it is still in an early stage of its learning curve regarding how to develop effective financial intelligence, it is essential that the existing sources of bias be identified and corrected immediately, while the emerging profiles are not crystallised in the organisation's procedures.

Conclusion

There is a burgeoning industry providing sophisticated computer technology and complex mathematical models to mine financial data and single out unusual patterns of transactions. The process is largely quantitative and automated, but it is also one where the analyst plays a crucial role. We respond to Pazzani's (2000) call for further research into how cognitive factors can affect data mining. The paper used a semiotic framework to investigate how behaviour profiles are shaped by the existence of denotative and affective information, the nature of the tasks and the prevalent norms.

It was noted that the behaviours afforded to employees in different tasks impact on the individuals' exposure to information, as well as to that same individual's interpretation of commonly available information. Ensuring effectiveness of financial intelligence efforts demands from managers an understanding of the inputs available to each role in the organisation, and the specific context in which employees operate.

The paper highlighted that the emerging profile is narrower than the abstract definition of money laundering, and that this difference emerges because of technical limitations, internal and industry guidance, and pragmatic interests and situation in the organisation. Consequently, management needs to look for ways to align the relevance of anti money laundering objectives across the organisation. The paper also noted how informal norms dramatically cue meaning.

The study provided important insights into how task affordances and behavioural norms affect the success of technological initiatives. However, there are some important questions raised by the empirical study that could be pursued in future research exercises. The empirical work focused on one technological platform, only, but more artefacts used by the FI team could be considered. In particular, it would be interesting to investigate how visual analysis software, by increasing the salience of particular pieces of information, might cue the analyst's attention and, ultimately, influence the emerging profile.

Additionally, it was mentioned that the FI team draws on inputs from other units, inside and outside the organisation, in order to develop profiles of money laundering behaviour. It would have been interesting to extend the analysis to some or all of those units. In particular, further studies should investigate inter-organisational financial intelligence development. Indeed, it is possible to imagine that the output of the financial intelligence process would have been different if the analysis had centred on units with different views of the institution's customer, or driven by non-commercial objectives.

References

Akgun, A. E., G. S. Lynn, et al. (2003). "Organizational learning: a socio-cognitive framework." Human Relations **56**(7): 839.

Basel (2001). Customer due dilligence for banks. Basel, Basel Committee on Banking Supervision.

Bisman, C. D. and D. Hardcastle (1999). Integrating Research into Practice. Belmont, California, Wadsworth.

Brenneman, K. and R. DeLotto (2001). Vendors of Money Laundering Detection Tools Reviewed. Markets, Gartner Research. **M-13-5713:** 1-4.

Bruha, I. (2000). "From machine learning to knowledge discovery: survey of preprocessing and postprocessing." Intelligent Data Analysis **4**: 363-374.

Canhoto, A. I. and J. Backhouse (2004). Constructing Categories, Construing Signs: Analysing differences in suspicious transaction reporting practice. London, Information Systems Integrity Group, London School of Economics.

Chung, H. M. and P. Grey (1999). "Special edition: Data mining." Journal of Management Information Systems **16**(1): 11-16.

Complinet (2005). "Anti-money laundering systems review." Compliance & Technology Review **1**(4): 6-9.

Creswell, J. W. (2003). Research design: qualitative, quantitative, and mixed method approaches. London, SAGE.

Desouza, K. C. and Y. Awazu (2004). "Need to Know: Organizational knowledge and management perspective." Information Knowledge Systems Management **4**: 1-14.

Easterby-Smith, M., M. Crossan, et al. (2000). "Organizational learning: debates past, present and future." Journal of Management Studies **37**(6): 783-796.

Eco, U. (1976). A theory of semiotics. Bloomington, IN, Indiana University Press.

Edmondson, A. (1999). The view through a different lens: investigating organisational learning at the group level of analysis. 3rd Internation Conference on Organizational Learning, Lancaster.

Fayyad, U., G. Piatetsky-Shapiro, et al. (1996). "From data mining to knowledge discovery in databases." AI magazine **17**(3): 37-54.

Fayyad, U., G. Piatetsky-Shapiro, et al., Eds. (1996). Advances in knowledge discovery and data mining. Cambridge (Massachussets, USA), AAAI / MIT Press.

FSA. (2003, 21 March 2005). "FSA fines Abbey National companies 2,320,000." from http://www.fsa.gov.uk/pages/Library/Communication/PR/2003/132.shtml.

FSA (2003). Reducing money laundering risk - Know your customer and anti-money laundering monitoring. London, Financial Services Authority**:** 48.

Funsten, D. M. (1998). "Helping your customers behave themselves." Bank Marketing **30**(10): 22-27.

Gherardi, S. and D. Nicolini (2000). "To transfer is to transform: the circulation of safety knowledge." Organization **7**(2): 329-348.

Gibson, J. J. (1979). The ecological approach to visual perception. Boston, Houghton Mifflin Co.

Gill, M. and G. Taylor (2003). "Can Information Technology Help in the Search for Money Laundering? The Views of Financial Companies." Crime Prevention and Community Safety: An International Journal **5**(2): 39-47.

Goede, M. d. (2004). The risk of terrorist financing and practices of global governmentality. British International Studies Association, University of Warwick.

Griffith, T. L. and M. A. Neale (2001). Information processing in traditional, hybrid, and virtual teams: from nascent knowledge to transactive memory. Research in Organizational Behaviour. B. M. Staw and R. I. Sutton. Stamford, CT, JAI Press. **23:** 379-421.

Griffith, T. L., J. E. Sawyer, et al. (2003). "Virtualness and knowledge: managing the love triangle of organizations, individuals, and information technology." MIS Quarterly **27**(2): 265-287.

Hardy, Q. (2004). Data of reckoning. Forbes. **173:** 151-153.

Jahoda, G. (2001). "Beyond stereotypes." Culture & Psychology **7**(2): 181-197.

Kitano, T. (2005). The Adoption of Anti-Money Laundering Transaction Monitoring System in UK Banks: The Effect of Risk Perceptions. Department of Information Systems. London, London School of Economics. **MSC Analysis, Design and Management of Information Systems**.

Kohavi, R., N. J. Rothleder, et al. (2002). "Emerging trends in business analytics." Communications of the ACM **45**(8): 45-48.

Lenzen, R. (2004). Customer Analytics: It's all about behavior. DM Review.

Levi, M. and D. S. Wall (2004). "Technologies, Security, and Privacy in the Post-9/11 European Information Society." Journal of Law and Society **31**(2): 194-220.

Liebenau, J. and J. Backhouse (1990). Understanding information: An introduction. London, Macmillan.

Liebenau, J. and G. Harindranath (2002). "Organizational reconciliation and its implications for organizational decision support systems: a semiotic approach." Decision Support Systems **33**(Issue 4): 339-398.

Liu, B., M. Hu, et al. (2000). Multi-level organization and summarization of the discovered rules. Sixth ACM SIGKDD international conference on Knowledge discovery and data mining, Boston, Massachusetts, United States, ACM Press.

Liu, K. (2000). Semiotics in Information Systems Engineering. Cambridge, Cambridge University Press.

McGrath, J. E. and J. L. Berdhal (1998). Groups, Technology and Time: use of computersfor collaborative work. Applications of theory and researchon groups to social issues. R. S. Tyndale, L. Heath, J. Edwardset al. New York, Plenum Press. **4:** 205-228.

Mennecke, B. E., M. D. Crossland, et al. (2000). "Is a map more than a picture? The role of SDSS technology, subject characteristics, and problem complexity on map reading and problem solving." MIS Quarterly **24**(4): 601-629.

Nake, F. (2002). Data, Information, and Knowledge: a semiotic view of phenomena of organization. Organizational Semitiocs: evolving a science of information systems. K. Liu, R. J. Clarke, P. B. Andersen, R. Stamper and E.-S. Abou-Zeid. London, Kluwer academic publishers**:** 41-50.

Orlikowski, W. J. (1996). Evolving with Notes: organisational change around groupware technology. Groupware and Teamwork. C. Ciborra. London, John Wiley & Sons Ltd**:** 23-60.

Orlikowski, W. J. (1996). "Improving organisational transformation over time: a situated action perspective." Information Systems Research **7**(1): 63-92.

Pagel, S. and R. Westerfelhaus (2005). "Charting managerial reading preferences in relation to popular management theory books - A semiotic analysis." Journal of Business Communication **42**(4): 420-448.

Parsons, J. (2002). "Effects of local versus global schema diagrams on verification and communication in conceptual data modelling." Journal of Management Information Systems **19**(3): 155-183.

Pazzani, M. J. (2000). Knowledge discovery from data? IEEE Intelligent Systems**:** 10-13.

Peirce, C. S. (1931-58). Collected Writings. Cambridge, MA, Harvard University Press.

Peirce, C. S. (1977). Semiotic and Significs: the correspondence between Charles S. Peirce and Victoria Lady Welby. Bloomington, Indiana, Indiana University Press.

Potter, R. E. and P. Balthazard (2004). "The role of individual memory and attention processes during electronic brainstorming." MIS Quarterly **28**(4): 621-643.

Punch, K. (1998). Introduction to Social Research. London, Sage.

Riessman, C. K., Ed. (1994). Qualitative Studies in Social Work Research. Thousand Oaks, California, Sage.

RSM (2002). Clean sweep? Applying technology to money laundering detection, RSM Robson Rhodes**:** 34.

Smith, G., D. Blackman, et al. (2003). "Knowledge sharing and organisational learning: the impact of social architecture at Ordnance Survey." Journal of Knowledge Management Practice **4**(3): 18.

Stamper, R. (1973). Information in business and administrative systems. New York, John Wiley and Sons.

Stamper, R. (1996). Signs, information, norms and systems. Signs of work: Semiotics and information processing in organizations. P. Holmqvist, P. B. Andersen, H. K. Klein and R. Posner, Walter de Gruyter.

Sund, R. (2003). "Utilisation of administrative registers using scientific knowledge discovery." Intelligent Data Analysis **7**: 501-519.

Te'eni, D. (2001). "Review: a cognitive-affective model of organizational communication for designing IT." MIS Quarterly **25**(2): 251-312.

Veyder, F. (2003). "Case study: Where is the risk in transaction." Journal of Financial Regulation & Compliance **11**(4): 323-328.

Watkins, R. C., K. M. Reynolds, et al. (2003). "Tracking dirty proceeds: Exploring data mining technologies as tools to investigate money laundering." Police Practice and Research **4**(2): 163-178.

Zuboff, S. (1988). In the age of the smart machine. New York, Basic books.