Critical Perspectives on Accounting 50 (2018) 56–66

Contents lists available at ScienceDirect

Critical Perspectives on Accounting

journal homepage: www.elsevier.com/locate/cpa

Full length article

Suspicion of money laundering reporting obligations: Auditor compliance, or sceptical failure to engage?

Simon D. Norton

Cardiff Business School, Cardiff University, Colum Drive, Cardiff, CF10 3EU, UK

ARTICLE INFO

Article history:
Received 13 November 2014
Received in revised form 17 September 2017
Accepted 18 September 2017
Available online 5 October 2017

Keywords:
Money laundering
Auditors
Suspicious Activity Report
Surveillant assemblage

ABSTRACT

Money laundering has become of increasing concern to law makers in recent years, principally because of its associations with terrorism. Recent legislative changes in the United Kingdom mean that auditors risk becoming state law enforcement agents in the private sector. We examine this legislation from the perspective of the changing nature of the relationship between auditors and the state, and the surveillant assemblage within which this is located. Auditors are statutorily obliged to file Suspicious Activity Reports (SARs) into an online database, ELMER, but without much guidance regarding how suspicion is determined. Criminal rather than civil or regulatory sanctions apply to auditors' instances of non-compliance. This paper evaluates the surveillance implications of the legislation for auditors through lenses developed in the accounting and sociological literature by Brivot and Gendron, Neu and Heincke, Deleuze and Guattari, and Haggerty and Ericson. It finds that auditors are generating information flows which are subsequently reassembled into discrete and virtual 'data doubles' to be captured and utilised by authorised third parties for unknown purposes. The paper proposes that the surveillant assemblage has extended into the space of the auditor-client relationship, but this extension remains inhibited as a result of auditors' relatively weak level of engagement in providing SARs, thereby pointing to a degree of resistance in professional service firms regarding the deployment of regulation that compromises the foundations of this relationship.

1. Introduction

The state deploys numerous technologies to regulate and oversee the behaviours of individuals, populations, and professions, some of which are direct and transparent while others are concealed (McKinlay & Starkey, 1998; Rose and Miller, 1992). The concealed technologies include the gathering of information by individuals such as auditors and solicitors, institutions such as health authorities and welfare agencies, and its reporting to the state in fulfilment of legal obligations. The provider of the information may not know the precise purpose for which it will be used; this may be for statistical analysis, the allocation of tax resources (Miller & O'Leary, 1987), or, when criminality is suspected, to trigger further covert surveillance by other state actors. Neu and Heincke (2004, p.181) observe that:

> 'Technologies such as accounting, administration, and law serve to structure the conditions of possibility within a particular institutional field. These techniques not only frame potential problems within the field, but also construct possible solutions (Neu, 2000; Preston, Chua, & Neu, 1997). By mobilizing distant knowledges and by transmitting this

E-mail address: NortonSD@cardiff.ac.uk (S.D. Norton).

http://dx.doi.org/10.1016/j.cpa.2017.09.003

knowledge to centers of calculation, technologies of government facilitate the *efficient* exercise of government from a distance'.

Neu and Hencke suggested that historically, as the state became more remote from those it governed because of the increased complexity of economic affairs, its reliance upon constant flows of information increased. The direct punishment of offenders no longer sufficed, as those who facilitated criminality, directly or indirectly, also had to be sanctioned. The traditional 'touchstone' in the auditor-client relationship, the duty of confidentiality, also became subject to statutory incursion as the state extended its reporting obligations regarding known or suspected criminal behaviour. The difference between these two states of mind – knowledge and suspicion – challenges auditors when interacting with the on-line reporting system. The main applicable legislation, the Proceeds of Crime Act 2002 (POCA 2002 hereafter), imposes a reporting obligation when there is 'reasonable suspicion' of criminality, but without providing a statutory definition of what that means. Is suspicion to be determined objectively in relation to how an auditor's peers would view a client's series of transactions, or subjectively, by reference to the facts as directly perceived or interpreted? This dichotomy is embedded in the nomenclature of the reporting mechanism: the Suspicious Activity Report (SAR hereafter). POCA 2002 is principally aimed at the financial services sector where 'suspicion' tends to be triggered by single, specific transactions rather than by a 'piecing together' of a series of transactions which would be undertaken by a forensic accountant. For example, the transfer of a large sum of money from an overseas jurisdiction where bribery and corruption are prevalent will, *ceteris paribus*, trigger suspicion and the filing of a report. Similarly, multiple small deposits made by numerous individuals which accumu

late in one account (known as 'smurfing') will also generate suspicion. These so-called red flags, amongst others, were described in a report issued by the United Kingdom Financial Conduct Authority in July 2013. However, an accountant may witness or be party to a series of ostensibly innocent transactions by a client which, with the benefit of hindsight, can be viewed as suspicious, thereby leading to a questioning of the accountant not having originally filed a suspicious report.

The present paper extends the line of reasoning found in work by Brivot and Gendron (2011),Haggerty and Ericson (2000), and Giddens (1985), that surveillance in some aspects of the auditor-state relationship has evolved into a diverse, rhizoid structure (Hoskin, 1994). The networks of state agencies which have access to the database in which SARs are held, ELMER, have diverse purposes for which the information may be used, and reflect this evolving assemblage (the database was so named in honour of Elmer Lincoln Irey, the Director of the United States' Internal Revenue Service's lead investigation unit during the federal tax evasion prosecution of Al Capone in 1931).

The paper addresses three questions. First, how has the traditional auditor-client relationship been affected by the new statute-based surveillant assemblage? Second, what are the implications of the transformation of the traditional nexuses between auditor, client, and state into what Benjamin (1983), and later, Haggerty and Ericson (2000) identify as a 'multitude of organized surveillance systems'? Third, to what extent are auditors engaged with the new reporting regime? The paper's methodology is principally theoretical, evaluating the implications for auditors of evolving state surveillance as manifested in relevant provisions of POCA 2002. Its empirical dimension critiques the relevant sections of United Kingdom (UK hereafter) anti-money laundering law to comprehend the implications of reporting obligations placed upon auditors, and its apparent lack of clarity in how 'reasonable suspicion' is defined. Statistical data produced by the National Crime Agency (NCA hereafter) is utilised to explain the degree of reporting compliance by auditors.

The paper is organised as follows. The next section addresses a dichotomy: does the accounting profession facilitate criminality such as money laundering, or assist in its prevention or detection? Section 3 describes how information technologies create 'data doubles' of persons to be subsequently exchanged between and scrutinised by state agencies. The section draws upon theoretical work by Brivot and Gendron (2011) to demonstrate how Foucault's model of centralised surveillance as described in *Discipline and Punish: The birth of the prison* (1977) has been displaced by a more diverse, rhizoid surveillant assemblage, as discussed in the sociological work of Jessop (2007) and Deleuze and Guattari (1987). Section 4 critiques auditor reporting obligations under POCA 2002, describing technological failings and database inadequacies currently holding back development of the surveillant assemblage. Statistical data provided by the NCA is drawn upon to demonstrate how auditors have consistently and significantly underperformed, year on year, most other reporting sectors in terms of quantity of SARs filed. Section 5 provides the paper's conclusions.

2. Money laundering and the accounting profession: prevention or participation?

Money laundering may be defined as the attempt to disguise the origin and nature of income derived from illegal purposes and its subsequent integration into the financial system without attracting the attention of law enforcement or tax collection authorities (Compin, 2008; Lehman & Okcabol, 2005). The academic literature is rich regarding the interrelationship between the state and the accounting profession, and the reporting obligations imposed on the latter by the former (Gendron, 2002; Guenin-Paracini & Gendron, 2010; Hines, 1989; Humphrey & Owen, 2000; Power, 1997). The dichotomy in the auditor-state relationship relates to whether accounting is a means of detecting, preventing or deterring money laundering, or if it participates in the crime, enabling and hiding it. The dichotomy is important because if auditors facilitate the commission of a crime, then the ever-encroaching surveillance structures – the rhizoid assemblage – may be justifiable, even at the cost of undermining the traditional notion of client confidentiality. If, instead, auditors deter crime,

then this new strengthened surveillance is less justifiable, and allegations of unsubstantiated participation become a convenient tool in extending reporting obligations through the SARs system.

According to Morales, Gendron, and Gue Moore nin-Paracini (2014), a significant body of accounting literature examines the role of accountants in both detecting and preventing certain kinds of fraud. A dominant theme in this literature is that fraud invariably results from lack of control; the role of the accountant is to foster effective oversight and cultivate skills in its detection through forensic and internal auditing activities, and the introduction of systems by which opportunities to act dishonestly are reduced. An example of systemic failure is provided by the collapse of Barings Bank in February 1995. It was the notorious 'five 8′s account' which enabled Nick Leeson to circumvent internal control and audit safeguards to conceal his trading losses. Effective internal auditing activities combined with proper systems of oversight would have reduced the opportunity for his dishonest behaviour, and may have avoided the bank's subsequent demise. Training in fraud detection in accordance with criteria set out in the COSO framework of 2012 also reinforces, at least in principle, the capacity of accountants to address the risk of fraud (Hansen & Peterson, 2010). The framework explicitly includes a principle requiring companies to consider the potential for fraud in assessing the risks they face (COSO, 2012, p. 78; Morales et al., 2014, p. 189).

On the other hand, the role of accounting in facilitating financial crime, fraud, and corruption has been widely discussed in the literature (Arnold and Sikka, 2001; Compin, 2008; Neu, Everett, Rahaman, & Martinez, 2013). Mitchell, Sikka, and Willmott (1998) described the role of accountancy firms in facilitating the specific crime of money laundering. Formally speaking, accounting is principally concerned with the recording of transactions and with identifying, and thereby inhibiting, criminal behaviour. As Mitchell et al. (1998 p. 589) thus observe:

> '[A]ccountants routinely trade upon their claims of rationality, professionalism and "service of the public interest" to secure or extend their monopolies (e.g. external audits), privileges and status. In this way auditors have colonized both public and private sectors where their calculations routinely inform decisions about the allocation of goods and services, including employment health and education'.

The argument is that auditors create complex transactions which can make identifying the origins and destinations of illicit funds difficult since although tasked with detecting and reporting such activity, they have difficulty in discharging this obligation (Melnik, 2000). For Kerry and Brown (1992), money laundering is not generally conceived by 'wicked individuals'; 'Rather it is planned, executed, minuted and concealed in clean, respectable, warm and well-lit city centre offices' (1992 p.594). Neu et al. (2013) describe how the 'skilful use' of accounting practices and the social interactions around those practices enabled corruption (defined as the misuse of public office for private gain) to persist in the context of the Canadian government's Sponsorship Program (1994–2003), resulting in approximately $50 million being diverted into the bank accounts of political parties, program administrators, and their families and friends. Money laundering requires constant entries into and exits from the financial markets, and criminal organisations have at their disposal financial and accounting specialists able to find suitable fronts to circumvent national regulations and technical rules. Compin (2008) notes (p.594):

> 'Accounting provides sophisticated support to the criminal approach and serves as a risk minimization tool. The technique becomes the smokescreen, allowing financial communications to be given a positive spin to meet the required standards'.

The paradox is that accountants may, for example, build corporate structures with interlocking shareholdings on behalf of a client, perhaps across several jurisdictions, to present an entirely lawful series of transactions to revenue authorities, but through which criminal funds will subsequently flow in the form of intra group dividend payments, management charges, or inter-company loans at market interest rates. Recent UK legislation has required accountants to scrutinise these ostensibly lawful structures for evidence of criminality and to report any suspicions to the NCA. However, 'reasonable suspicion' exists across a wide mental horizon, from an intuition that 'something isn't quite right' to a near certainty that, based on objectively evaluated facts, crime of some sort is being committed. The raw materials upon which the effectiveness of surveillance depends are therefore derived from an array of sources, some of which may be more objectively certain, while others are likely to be vague and less factually based. Suspicion is not determined by application of a mathematical process; the surveillance assemblage must extract and process diverse information to construct a coherent, mineable database accessible by centres of control and oversight. The nature of this process of surveillance and its production of transferrable 'data doubles' are considered next.

3. Diverse surveillance and 'data doubles'

Surveillance exists in many forms from the direct and observable, for example cameras located at busy traffic junctions, to covert and unnoticed, where intelligence services tap phone calls, intercept mail, or scrutinise internet activity for evidence of criminality. Individuals can 'know' they have been watched: a speed camera captures the car registration plate of a speeding motorist, triggering a flash in the rear view mirror. Or they can 'suspect' that they are being watched: a vague intuition that a professional advisor has abrogated the confidentiality principle and reported a criminal client to the police, who are now monitoring through a host of technologies (Dandeker, 1990; Lyon, 2002). Finally, they may not contemplate the possibility that they have been subject to any scrutiny at all: for example, when a taxpayer's file is reviewed for evidence of 'red flags' of tax evasion which subsequently prove to be non-existent (Sikka & Hampton, 2005). The innocent taxpayer does not suspect that his or her financial affairs have been perused: why would they be? Scrutiny has been undertaken discretely

and unnoticed. In all of these contexts surveillance may be undertaken by single entities for a narrow purpose, or instead by multiple agencies for data for further review across a more extensive network. It may be centralised, focused and observable, mirroring Bentham's watchtower metaphor (Bentham, 1791, 1995), or it may be diverse, tacit, concealed and omnipresent. Haggerty and Ericson (2000) suggest that a convergence of previously discrete surveillance systems has occurred, so that they now constitute an emerging surveillant assemblage. They observe (p.606):

'This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct "data doubles" which can be scrutinized and targeted for intervention. In the process, we are witnessing a rhizomatic levelling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored'.

Effective surveillance requires an interface between technology and corporeality, and is comprised of those 'surfaces of contact or interfaces between organic and non-organic orders, between life forms and webs of information, or between organs/body parts and entry/projection systems (e.g. keyboards, screens)' (). It requires an extensive network of interconnected state agencies which constantly mine for, extract and exchange information derived from data filed by the multiple parties statutorily mandated to assist in this process. These networks have been likened by Deleuze and Guattari (1987) to rhizomes or plants which spread in a creeping horizontal fashion across surfaces through interconnected vertical root systems, in contrast to deep soil, single root plants which tend to develop vertically. In applying the rhizoid analogy to the social space, Latour (1987) sees evolving networks of state centres of oversight and control as 'scattered centres of calculation', in which information flowing into a surveillant assemblage is reassembled and scrutinised 'in the hope of developing strategies of governance, commerce and control' (). The person on whom information is reported now has a data double under constant scrutiny by multiple users. Haggerty and Ericson (2000 p.613) describe this situation:

'Data doubles circulate in a host of different centres of calculation and serve as markers for access to resources, services and power in ways which are often unknown to its referent'.

The purposes of data doubles remain undisclosed either to the 'data double original' or the filers of the information used to build them (Poster, 1990). In Foucault's panoptic model founded upon Bentham's watchtower metaphor, the nature of the relationship between overseer and overseen is transparent; information flows are homogenous, and the range of potential uses and users is limited and predictable. Central to the model is the notion of enclosure; there is surveillance exercised from a central point over a space bounded by physical parameters, for example bricks and mortar as would be the case for asylums, and mass production factories (Dandecker, 1990; Townley, 1994). The occupant of Bentham's watchtower surveilled prisoners walking in a courtyard for signs of breaches of prison rules, or secretive conversations preceding an anticipated escape attempt (Bentham, 1791, 1995; Foucault, 1977). In contrast, in the rhizoid assemblage the information flows are diverse, multi-directional, and complex; multiple overseers use the information for an array of undisclosed purposes. Information may be relevant in one context, for example suspected tax evasion, but irrelevant in another, depending on the statutorily defined purposes of the overseer. Ostensibly innocent tax avoidance via transactions between connected companies may lead to further investigation for criminal activity such as money laundering if passed to a policing agency. Relevance, and the way in which information is used, is in part determined by the nature and objectives of the agency extracting and scrutinising it. This rhizoid assemblage exhibits greater complexity than Foucault's hierarchical model, better reflecting the near-limitless capacities of new technologies to extract, store, process and share with third parties information drawn from across a fragmented landscape of overseers and reporters.

3.1. A rhizoid surveillance assemblage

Foucault's model has been complemented in the recent literature by more diverse and less centralised surveillant assemblages. Brivot and Gendron (2011) described the implications of new technology-based surveillance which followed the introduction of a computerised knowledge management system in a Parisian tax/law firm. For them, Foucault's panoptic metaphor weakens when spaces are permeated with contemporary information technologies. Technologies track a target's behaviour, whether through on-line purchases, the covert monitoring of websites visited, or the mapping of locations of mobile phone calls (Lyon, 2001). Overseers are 'invisible' in the sense that their locations, monitoring processes and capacities are unknown to those being watched. People being watched do not even know how many overseers have access to their online behaviour. For Poster (1997), digital databases result in a "superopticon" in which subjects constantly produce surveillance data through their interactions with technological interfaces such as e-mails and texts, generating a trackable digital footprint which, in some cases, is monitored by law enforcement agencies for evidence of criminal behaviour (for example, visiting illegal websites on the 'dark web') (Gandy, 1993). Blogs and social networking websites generate data on the profile and behaviour of users, which may be collected by various state agencies (Brivot & Gendron, 2011; Castells, 2001). The data has the advantage of permanence, and of difficulty of removal once 'posted on-line'. The targets of surveillance have also changed; the reduced cost associated with the mass storage of information means that everyone can now be surveilled, not just the deviant and abnormal as was the case in 18th and 19th century asylums and correction houses. This perspective chimes with Quessada's (2010, pp. 56–57) observation that surveillance has become '. . . light, discreet, immaterial and omnipresent'. Databases in which the mass storage of information takes place facilitate this expansion of surveillance.

The sources of data – the persons, corporate and otherwise, from which it is extracted – are largely oblivious as to how, and by whom, it will be later accessed and interpreted. Haggerty and Ericson (2000) discuss that police organisations routinely access non-police databases such as those held by insurance companies and financial institutions, and in the US, the Federal NCIC [National Crime Investigation Center] police database that is linked to Social Security, Internal Revenue, Passport, Securities and Exchange and the State Department (Stanley & Steindhardt, 2009). This process of consolidation of information flows and separate centres of information storage, alongside the widening classes of users and observers, manifests a deepening and extending of the surveillant assemblage as described by Deleuze and Guattari (1987) and Lyon (1994).

Information technologies mean that there is now no overtly central watching figure; instead, 'Modern technologies of surveillance are operated by an unstable collective of actors with a variety of agendas, each focusing on diverse targets of control' (Brivot & Gendron, 2011, p.140). For the surveillant assemblage to function effectively and efficiently in dispersing data across multiple centres of oversight, the transmission of information must be seamless and unobstructed, facilitated by compliant and statutorily bound providers of that information. New technologies make this transmission possible, unimpeded by physical or institutional boundaries.

3.2. Information flows across unenclosed spaces

For Martinez (2011), with the advent of new information technologies, disciplinary control is exercised not within institutional boundaries, but instead flows throughout the open landscape. Martinez draws upon the framework of a society of control by Deleuze (1992) which theorises that: (1) individuals do not necessarily move from confined systems of control to another, but instead across interconnected and continuous landscapes; (2) an emphasis is placed on communication and information technologies that facilitate instant and continuous tracking of individuals throughout the open environment; and (3) individuals are digitised and aggregated into large and multiple banks of information. Martinez argues that information and communication technologies target the individual throughout the open environment instantly, continuously and with heightened accuracy. Importantly, societies of control deconstruct boundaries so that information is extracted from surveilled targets as they proceed across a relatively borderless landscape. Martinez observes (p,205):

> 'In disciplinary societies, power is exercised across a network of heterogeneous institutional enclosures- each one possessing its own self-enclosed monitoring system that envelops the targeted population in a homogenous disciplinary effect. In contrast to this panoptic surveillance, it is proposed that contemporary systems of control are deployed from various angles, overlapping each other, forming interconnected networks of information spread throughout the social landscape. These networks are, moreover, composed of loosely connected modules and monitoring devices that facilitate mobility and surveillance across enclosures. The exercise of power is no longer confined to an institutional setting but exercised through the diffusion of previously enclosed logics of control across networks of information'.

Central to Deleuze's society of control and Martinez's targeting of individuals is the authority and legitimacy of state agencies to demand information.[1] Databases cannot exist in isolation, as they must be 'fed' by a multiplicity of statutorily mandated data gatherers who compile, retain, and file in standardised form information which can be subsequently mined by third parties with lawful authority (access) to do so. For Miller and Rose (1990, p. 8), laws are one of the principal technologies 'through which authorities of various sorts have sought to shape, normalize and instrumentalize the conduct, thought, decisions and aspirations of others in order to achieve the objectives they consider desirable'.

Neu and Heincke (2004, p. 181) propose that in prior historical periods, these technologies were associated primarily with the security needs of the state. In this earlier context laws against incitement, conspiracy, and corruption provided for criminal sanctions against those convicted of such offences. The authority of British 'spymasters' such as Queen Elizabeth I's Lord Walsingham was also rooted in laws, permitting any act deemed necessary for the protection of the state and the gathering of information, including through torture. However, Neu and Heincke note that over time technologies and experts were enlisted by the state to facilitate the governance of populations. This would have become necessary, for example, as the Industrial Revolution of the late Eighteenth Century got underway in the UK. The movement of peoples from rural areas into towns and cities made more complex the technologies used by the state to maintain social order, to gather statistical data to inform social policy, and to provide rudimentary support for the destitute, such as the Victorian Poor Laws. Now, technologies such as accounting, administration, and law serve to structure the conditions of possibility within a particular institutional field. These techniques not only frame potential problems within the field, but also construct possible solutions. For Neu and Heincke, by mobilising distant knowledges and by transmitting this knowledge to centres of calculation, technologies of government now facilitate the efficient exercise of government from a distance. Information is gathered from diverse centres by multiple, often unrelated agencies (in terms of statutory remits) possessed of the legal authority to demand it. It must then be easily and smoothly transmittable across networks of communication to other agencies which may then utilise it in furtherance of their own goals and agendas.

Accordingly, POCA 2002 authorises the extraction of information in the form of SARs and its transmission across a diverse surveillant assemblage, assisted by the storage, processing and mining capacities of the new technologies. The legislation has

[1] It needs to be recognized that a range of commercial actors, today, are also involved in monitoring web behaviour (Viale, Gendron & Suddaby, 2017).

attempted to redefine or reframe the traditional nexuses between auditor, client and the state; authorised third parties now have access to previously privileged information, whilst filers of SARs are protected, and their compliance with reporting obligations encouraged, through so-called 'safe harbour' provisions. The extent to which the dynamics of these relationships have been affected by the legislation is evaluated in the following section.

4. Auditor reporting obligations under POCA 2002: legality versus practicality

The three main UK money laundering offences are contained in sections 327, 328, and 329 of POCA 2002, and are punishable by a maximum prison sentence of 14 years and/or a fine. Under section 327, an offence is committed if a person 'conceals, disguises, converts, transfers or removes from the jurisdiction property which the person knows or suspects represents the proceeds of crime'. Section 328 states that an offence is committed when a person enters into, or becomes concerned in, an arrangement which they 'know or suspect' will facilitate another person to acquire, retain, use or control criminal property, and the person knows or suspects that the property is criminal property. Section 329 provides that an offence is committed when a person acquires, uses or has possession of property which they know or suspect represents the proceeds of crime. Auditors are now statutorily required to continuously review their relationships with clients for any evidence of 'suspicious activity' which, if identified, must be reported to the NCA through filing of a SAR. This newly established quasi-policing role is at odds with the traditional nature of the auditor-client relationship characterised thus by the ICAEW in its 'Response to Suspicious Activity Reports (SARs) Regime: Call for Information by the Home Office', 25th February 2015:

> 'With some notable exceptions, accountants do not generally have experience of law enforcement or forensic work. Whilst much of their work may well be investigatory, such investigations are rarely criminal. As such they may not always form suspicions in a given scenario where a law enforcement officer might. Greater access to data around typologies and red flags would help here, especially if law enforcement is to continue to rely on the private sector for intelligence'.

For the Institute of Chartered Accountants in England and Wales (ICAEW hereafter), auditors have become conscripted into the intelligence-gathering processes of the state without the necessary forensic tools or training.[2] If this is true, this lack of the appropriate skills-set represents a significant practical impediment to effective execution of legal obligations. Under the legislation, it is a criminal offence not to make a disclosure when a suspicion has formed but, as noted in a Report from the Information Commissioner to the UK Parliament ('The Serious Organised Crime Agency's operation and use of the ELMER database. Information Commissioner's Report to the House of Lords European Union Committee'), the legislation does not define 'suspicion', a task which is left to the courts. In the Court of Appeal case R v. Da Silva [2006] All ER 131, it was stated that there should be 'more than a fanciful possibility' that a person is handling criminal property or involving themselves in money laundering. A 'vague feeling of unease' would not suffice, but the law did not require the suspicion to be clear or firmly grounded, or based upon reasonable grounds. Ultimately, the legislation has resulted in the filing of reports on a scale which has overwhelmed the system (evidence in this respect is provided below), making the detection of crime less effective. The ICAEW further comments:

> 'The existing SARs report is primarily designed with banks and financial institutions in mind, not for accountants or in fact any section of the regulated sector where suspicions are formed based on patterns of behaviour rather than specific transactions. This is evident from sections of the SARs form requiring Credit/Debit information (the accountants understanding of these terms derives from an entirely different angle), account numbers and information as to the date the account was opened/closed. The report also assumes a single suspicious transaction is being reported rather than a pattern. An accountant may also have very little information about the intended recipient of a transfer. Currently accountants have to "shoehorn" their reports into this format'.

The legality of retention and mining of SARs has yet to be tested in court proceedings but in a Report by the Information Commissioner to the House of Lords European Union Committee in 2011 on the Serious Organised Crime Agency's operation and use of the ELMER database, concern was expressed that dissemination of information filed could be in breach of the Data Protection Act 1998, and the Human Rights Act 1998. Regarding the latter, a significant risk remains of breach of Article 8 of the European Convention on Human Rights, which gives every person the right to "respect for his private and family life, his home and his correspondence". This concern has yet to be addressed by the Government. The nature of the statutory reporting obligation as an instrument of bureaucratic control, and its displacement of professional judgement, is considered next.

4.1. Auditor reporting and bureaucratic control

In a Guidance Note issued by the NCA in September 2016, 'Submitting A Suspicious Activity Report (SAR) within the Regulated Sector', the following filing obligation is stipulated:

[2] Note that historically, financial auditors have changed their mind quite frequently regarding the extent to which they assume responsibility for detecting fraud (Humphrey, Moizer & Turley, 1992).

'Persons in the regulated sector are required under Part 7 of the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TACT) to submit a SAR in respect of information that comes to them in the course of their business if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing. A SAR must be submitted as soon as is practicable'.

The Guidance Note provides that according to section 7 (1) of the Crime and Courts Act 2013, the disclosure of information to the NCA will not breach any obligation of confidence the auditor may owe to a third party or any other restrictions (however they are imposed) on the disclosure of information. Section 29 of the Data Protection Act 1998 also provides protection against the disclosure of information covered by the Act when the disclosure is made to the NCA.

In 2017 the ICAEW provided on its website examples of SARs which have significantly contributed to successful prosecutions. These include the following. A SAR reported that a limited company was deliberately understating its business income on its VAT (value-added tax) returns. HMRC (Her Majesty's Revenue and Customs) confirmed that the information in the business records and that declared on its VAT returns did not match, resulting in a settlement of over £80,000. The estimated benefit was over £25,000. The VAT evasion was detected principally through information disclosed in the SAR. In a further example, a SAR reported that a business owner had been depositing large cheques and round sum amounts of cash into their personal savings account. The payments appeared to originate from the business but without formal recognition in the accounts. An HMRC investigation secured an admission by the trader that they had been under-declaring sales for several years, resulting in a settlement of just under £40,000. Information contained in the SAR secured this outcome. Finally, in the course of confiscation proceedings a defendant was attempting to thwart court processes by claiming that properties were the assets of his current partner and former partner and not his own. The SAR showed that the defendant was trying to sell a restrained property without seeking the permission of the court, confirming that it was in fact his own.

The NCA website (http://www.nationalcrimeagency.gov.uk/) 'About us- what we do' page states that upon receipt, SARs are logged onto the United Kingdom Financial Intelligence Unit (UKFIU) internal SARs database (ELMER). SARs can lead to the instigation of new investigations or enhance existing ones. There are approximately 1.5 million SARs on ELMER, which are retained for six years or until proven not to be linked to crime. The website also explains that a single SAR is often used several times by several different users for different purposes. For example, Her Majesty's Revenue and Customs may draw upon information contained in a SAR for evidence or leads relating to a tax investigation. Local police may use it in furtherance of a fraud or theft investigation, without necessarily disclosing or directly citing it should court proceedings follow. It is also unclear whether or not the SAR itself would be disclosed to a defendant's lawyers as part of the advanced disclosure procedural rules in preparation for a criminal trial. Finally, the NCA also indicates that SARs may be used by a government department for statistical analysis to inform policy.

The UK Home Office Circular 022/2015 titled 'Money laundering: the confidentiality of Suspicious Activity Reports (SARs) and the identity of those who make them' states that the exercise of law enforcement powers can lead to the disclosure of SARs in civil proceedings. This is more likely to arise in civil recovery proceedings undertaken by the NCA under matters assigned to it under POCA, and HM Revenue and Customs. If the cause for suspicion reported by the auditor proves unfounded, other relevant agencies with access to ELMER may take the investigation in a different direction from that initially envisaged by the filer, at which point the information passes across a wider surveillant assemblage.

Power (1997) and MacLullich (2003) identify the risk inherent in the increased use of auditing as a key mechanism of bureaucratic control in support of capitalist regimes of truth. MacLullich (p. 796) observes:

'Professional judgement is constructed as a largely technical task based on rationalised procedures where other forms of knowledge are subjugated and emotional expression suppressed'.

The point is that auditors may become fixated on generating indicators of best practice and bureaucratic compliance rather than focusing on exercising substantive judgement. As a result of the processes of filing and reporting as stipulated in the legislation, risk may become the main concern, prioritised over the actual exercise of informed discretion (Ponemon, 1990). The Home Office ran a Call for Information on the operation of the SARs regime in 2015, and noted in its Findings the following themes deduced from responses from the reporting sector:

'The reporting sector has concerns regarding the phrasing of the requirement to report suspicious transactions, as set out in POCA. This concern, and the penalties for failure to report, drive a significant level of defensive reporting, where reports are made more because of concerns regarding a failure to comply with POCA than because of genuine suspicion. This places a burden on the regime, and detracts from a focus on serious and organised crime'.

Processes of online reporting, the structure and mandatory fields of the SAR form, and filing time limits all affect auditors' daily work. As a profession they are 'watched' by the NCA via the monitoring of reporting compliance, and the compiling of statistics to inform future policy. The auditor's behaviour is affected because he or she will commit a criminal offence if information (that raises reasonable suspicion) relating to the client's confidential financial affairs is not filed in a SAR. The client is also 'watched' (or perhaps suspects that he or she is being watched, when in fact this may not be the case) because the professional advisor may have reported on their behaviour without first obtaining consent, such is the nature of safe harbour statutory protection. The report may be subsequently mined by agencies for purposes unknown to either the client or advisor after being filed in the database (Giddens, 1990; Gordon, 1987; Staples, 1997). Anti-money laundering legislation thus reflects state interposition into a nexus of relationships via a process of mandatory reporting and storage of data for later access by a multiplicity of agencies. Auditor reporting becomes a tool of bureaucratic control through which data is gathered

and offered up to the NCA but not necessarily with much prior reflection; professional judgement may be displaced by the need to comply with process. The SAR filing obligation in the UK, and its database, ELMER, represent the automation of this process, absented of human interaction at the web-based portal interface. However, several impediments exist to the extension of the surveillant assemblage into the auditor-client relationship, principally relating to technological failings and limited engagement with the reporting system as evidenced by declining numbers of annual SARs filed.

4.2. Technological failings and auditor non-engagement

Neu and Heincke (2004) describe how 'technologies' comprising laws and regulations as well as financial and monetary relations intersect with techniques of force, but tend to fail to achieve their stated objectives. The authors identify 'the eternally optimistic but perpetually failing nature' of such technologies. Miller and Rose observe (1990, p.11):

> 'Technologies produce unexpected problems, are utilized for their own ends by those who are supposed to merely operate them, are hampered by underfunding, professional rivalries, and the impossibility of producing the technical conditions that would make them work . . . '.

Technological effectiveness requires smooth interfaces between the system itself (i.e. the database) and the filers of information. Where practicable, the latter should provide information which is homogenous in form and substance. However, in the context of the accountancy profession generally, the NCA has stated that the sector is 'one of the most fractured in terms of membership of professional bodies, making compliance with the Money Laundering Regulations of 2007 more difficult to enforce' (NCA Report, National Strategic Assessment of Serious and Organised Crime 2015). This fragmentation causes problems in surveillance and with the enforcement of harmonised standards (Cooper & Robson, 2006). In a report produced by the House of Commons Home Affairs Committee, 'Proceeds of Crime. Fifth Report of Session 2016/17', the following criticism was made of the SARs system:

> 'We have become deeply concerned for some time that the ELMER system for Suspicious Activity Reports (SARs) is heavily overloaded and therefore rendered completely ineffective. The ELMER system currently processes 381,882 SARs [last year] despite being designed to manage only 20,000 [yearly] and, of this figure, only 15,000 looked at in detail. We have reminded the Government time and again that it must be replaced. The failure of ELMER has made the SARs system a futile and impotent weapon in the global fight against money laundering and corruption'.

Auditors now file information in order to be fully compliant with the law, however trivial and unsubstantiated that filing may be. Consequently, it has become very difficult for state agencies to follow up and investigate all the suspicions disclosed in SARs. The ICAEW noted that from October 2014 to September 2015, the NCA reported that 381,882 SARs were submitted, an increase of 7.82% on the previous year. The largest number of reports came from banks (83.39%), while accountants and tax advisors filed 1.21% of reports. The ICAEW observed in a comment in a newsletter dated 7th March 2016 titled 'National Crime Agency publishes Suspicious Activity Reports (SARs) annual report':

> 'The report does note specifically though that of the 4618 SARs made by accountants and tax advisors, these were submitted by a total of 1487 individual entity reporters. Simple maths then gives an average of just over 3 reports per reporter. However, these numbers have to be taken in context. In the UK, taking all the accounting and tax bodies together and adding in all the other accounting service providers who are supervised by default by HMRC, there are probably in the region of 25,000 entities in the sector. The number of SARs made therefore represents about 1 per annum for every 6 [accounting] firms or, alternatively, almost 95% of firms do not make any reports'.

The ICAEW suggests that there may be several reasons for the low level of filing, including excellent risk assessment, client engagement and other firm procedures to avoid finding itself having to submit a SAR. Equally, it may be due to a lack of diligence among principals and staff, or a failure to keep up to date with training in the area of money laundering legislation. According to NCA statistics issued in its Annual Reports for 2012–2015, of all the SARs submitted by sectors including credit institutions (by far the largest filers), independent legal advisors, estate agents and trust or company service providers, accountants filed 2.06% in 2012, 1.71% in 2013, 1.39% in 2014, and 1.21% in 2015. Between October 2013 and September 2014 the number of SARs submitted by accountants and tax advisors fell by 18.7% in comparison to 2012–2013, when most other sectors reported on by the NCA showed positive increases. Similarly, between October 2014 and September 2015, there was a decline in SAR submissions of 12.9%, when most other sectors showed increases.

These statistics bear out the ICAEW's observation that accountants do not appear to be wholeheartedly embracing the reporting system established by POCA 2002. This leads to a further paradox: while the total number of SARs filed and reported in annual NCA reports has increased dramatically during these years (278,665 in 2012, 316,527 in 2013, 354,186 in 2014, and 381,882 in 2015), overwhelming the ELMER database according to the House of Commons Home Affairs Committee Report of 2015, reporting by the accountancy profession has remained almost static and at a significantly lower level than other sectors. This in spite of the fact that, according to the UK's National Risk Assessment of Money Laundering and Terrorist Financing published by the Home Office in late 2015, the profession was listed as high risk, second only to banks in terms of facilitating criminality. Evidence produced in statements to the House of Commons Home Affairs Committee also suggests that even this minimal level of reporting relates more to token compliance and the avoidance of criminal sanctions rather to real suspicions of criminal activity. The Committee cited in its Report (at p12, para 22) concerns expressed by Laurence Sacker, Partner, Corporate Finance and Money Laundering Reporting Officer at UHY Hacker Young LLP that his

perception was that many firms were submitting SARs simply so that the reporting officers were "in the clear" in terms of having met their statutory requirement and that investigators "probably only look in detail at the consent SARs that go to them, which is about 15,000 in a year. The others are just recorded somewhere and may get passed on eventually". Fundamental problems remain in the legalistic interpretation of 'suspicion', a concept not defined in the legislation, and a reporting system which seems to focus on individual transactions (bank-centric) rather than the series of transactions approach with which accountants are familiar. This difference may be exacerbated by a standardised online form with fields which fail to reflect these nuances between different reporting sectors. Another possible reason for the relatively low level of filing is accountants' well-known propensity to align with their clients' interests, in order not to compromise the influx of professional service fees. This has been described by Malsch and Gendron (2013) who identified an ongoing dialectic, in terms of prioritisation, between professionalism and commercialism. They cite Moore, Tetlock, Tanlu, and Bazerman (2006 p. 10) who maintain: 'Accounting firms have incentives to avoid providing negative auditing opinions to the managers who hire them and pay their auditing fee'. Audit can generate a conflict of interest between social service professionalism on the one hand, and the influence of mercantilism on the other. The filing of a SAR represents a prioritising of the former over the latter, and accordingly will be approached with caution if a consequence may be the loss of a client's trust who suspects that information has been passed on to a third party. Commercial self-interest sometimes outweighs a wider sense of professionalism. This view corresponds with that of Picard et al. (2014) who examined the relative cultural shift from social service professionalism to mercantilism or commercialism in the accounting profession, based upon consideration of the promotional brochures used by the *Ordre des comptables agréés du Québec* (Institute of Chartered Accountants of Québec), over the last 40 years, to attract new members.

5. Conclusion

As this paper has discussed, at first glance the extension of auditor reporting obligations under POCA 2002 reflects an evolving rhizoid surveillance assemblage comparable to that described in sociological literature by Deleuze and Guattari (1987), Deleuze and Foucault (1977), Haggerty and Ericson (2000), and Giddens (1990). The concern has arisen that data mining of ELMER by 'authorised end users' may result in the information filed by auditors emerging in entirely different and unforeseen locations and juridical contexts, for example in tax evasion court proceedings against a client or disputed welfare claims, or in police prosecutions. The ongoing compilation of ELMER evidences elements of the architecture of the surveillant state described by Lyon (1994), Nock (1993), Gordon (1987), and, of course, Orwell (1949); auditors now file information through SARs which then becomes available to unknown users and for unpredictable uses. If a client is notified by third parties with access to ELMER of pending investigations which only information known to the auditor could have triggered, then they will know (or suspect) that the auditor provided the information, without authorisation or notification. Consequently, the trust and confidentiality implicit in the professional relationship risks being compromised. The link between money laundering and terrorist activity is, and will remain, of concern to legislators, and POCA 2002 represents an attempt to dissuade auditors, through fear of criminal sanction, from participation in processes and structures which make these crimes possible (Davis, 2003). However, in practical terms, the reporting regime ushered in by the Act has significant shortcomings. The technology underpinning the regime received significant criticism in the Proceeds of Crime Report issued by the House of Commons Home Affairs Committee, Fifth Report of Session 2016–17:

> 'To repair the damage to the reputation of the SARs regime caused by the failure of ELMER, we recommend that the Government involves those who actually use the SARs system to make reports- as well as those charged with investigating at the other end- in designing the replacement to ELMER. Only by doing so can the Government rebuild industry's trust in the regime and ensure that the next generation of SARs does not suffer the same fate'.

The existing database technology lacks the capacity or capability to deliver on the development of the rhizoid surveillant assemblage envisaged by Brivot and Gendron (2011), Haggerty and Ericson (2000), and Giddens (1985). Annual empirical evidence from the NCA also strongly suggests that auditors are not engaged with the reporting system as the quantity of SARs they file appears to be either static or declining, unlike that of other reporting sectors such as banks and legal advisors. Several reasons have been suggested for this shortfall, but the statistical indicators might have been expected to indicate an increase in the number of SARs filed given the 'high risk' status of the profession *vis a vis* other reporting sectors (Lehman and Thorne, 2015; Mitchell et al., 1998; Neu, Everett, & Rahaman, 2015; Reinstein, Moehrle, & Reynolds-Moehrle, 2006).

The evidence suggests that auditors have not been 'caught up' in the surveillance assemblage to the extent which might otherwise have been envisioned, given the wide reporting obligations of POCA 2002. The ELMER database, which was originally intended to handle a significantly smaller quantity of SARs, also appears to be struggling with 'information overload'. The Act does not have a *de minimis* rule, as even where there is a low level of suspicion, and even if that suspicion relates to possible commission of a trivial criminal offence, auditors are still obliged to file a SAR. The recommendation by the Information Commissioner to the House of Lords European Union Committee in 2011 that consideration should be given to amending POCA 2002 to include a *de minimis* exclusion was rejected by the Government on the grounds that it would be unworkable. The wider legal architecture within which ELMER and the SARs filing obligation operates, particularly regarding human rights and data protection, will continue to present challenges to auditors when considering the extent of their reporting obligations and 'squaring' these with the traditional duty of client confidentiality as well as pressures not to compromise the firm's fee generation.

The implications of this paper's findings are threefold. First, the failure of POCA 2002 to define 'suspicion' in the context of 'suspicious activity' has resulted in a low reporting threshold, exacerbated by an absence of a *de minimis* rule. This has overloaded the ELMER database, and anecdotal evidence in responses to Parliamentary enquiries indicates that a significant proportion of SARs are not investigated. Minor legislative amendment, or more realistically, detailed and specific guidance by the professional bodies to their members, is therefore necessary to clearly define terms, thereby reducing the deluge of filings which is blocking up the system. The introduction of a *de minimis* rule should also be revisited. Second, the annual statistical evidence provided by the NCA evidences a limited engagement on the part of the accountancy profession with the SARs reporting system. The on-line filing process comprises a standardised form which must be completed by bank officials, estate agents, legal advisors, and of course auditors, but with fields which do not account for nuanced differences between grounds for suspicion. Importantly, some professions are 'event' focused, such as banking where, as an example, money may pass into an account from an offshore location; but in others, such as audit and legal, suspicion sometimes only arises when a series of transactions has been executed. In this latter context it is the whole, and not the individual parts, which triggers suspicion. Reformulation of the fields of the SAR form to reflect nuanced differences between reporting sectors regarding grounds for 'suspicion' may make filed data more specific, more relevant, and more readily minable by authorised third parties. Finally, by linking failure to report suspicious transactions, however trivial, with serious criminal repercussions, legislators have demonstrated a scepticism of the ability of auditors to exercise professional judgement. They therefore deem that a 'big stick' in the form of the threat of imprisonment is required to encourage compliance. This approach appears to have failed, however, as evidenced by NCA statistics as well as in responses to Parliamentary enquiries into the effectiveness of ELMER. This points to important limitations in regulatory capacities to impact human agency.

Acknowledgements

I am grateful to the Editor, Yves Gendron, for his guidance, advice, support and insightfulness throughout the revision process for this paper. I am also grateful to Hugh Willmott and Kevin Holland, both of Cardiff Business School, Cardiff University, for constructive critique of an earlier version. I also thank the Reviewers for their recommendations regarding practical and empirical focuses, and thematic priorities.

References

Arnold, P., & Sikka, P. (2001). Globalization and the state-profession relationship: The case of the Bank of Credit and Commerce International Accounting. *Organizations and Society*, *26*(6), 475–499.
Benjamin, W. (1983). *Charles Baudelaire: A Lyric Poet in the Era of High Capitalism*. London: Verso.
Bentham, J. (1791). *Panopticon: Postscript; Part II: Containing A Plan of Management for A Panopticon Penitentiary-House*. London: T. Payne. 2 vols.
Bentham, J. (1995). *The panopticon writings*. London: Verso.
Brivot, M., & Gendron, Y. (2011). Beyond Panopticism: On the ramifications of surveillance in a contemporary professional setting, Accounting. *Organizations and Society*, *36*, 135–155.
Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012). *Internal control- integrated framework, exposure draft- framework and appendices*. [2012, September].
Castells, M. (2001). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford: Oxford University Press.
Compin, F. (2008). The role of accounting in money laundering and money dirtying. *Critical Perspectives on Accounting*, *19*(5), 591–602.
Cooper, D. J., & Robson, K. (2006). Accounting, professions and regulation: Locating the sites of professionalization. *Accounting Organizations and Society*, *31* (4/5), 415–444.
Dandecker, C. (1990). *Surveillance, power and modernity: Bureaucracy and discipline from to the present day*. Cambridge: Polity..
Davis, K. (2003). Legislating against the financing of terrorism: Pitfalls and prospects. *Journal of Financial Crime*, *10*(3), 269–274.
Deleuze, G., & Foucault, M. (1977). Intellectuals and power. In D. Bouchard (Ed.), *M. foucault language, counter-Memory, practice: Selected essays and interviews*, New York: Cornell University Press. [translated by D. Bouchard & S. Simon].
Deleuze, G., & Guattari, F. (1987). *A thousand plateaus*. Minneapolis: University of Minnesota Press.
Deleuze, G. (1992). Postscript on the societies of control. *Winter*, *59*, 3–7. [October 1992].
Financial Conduct Authority (2013). *Banks' control of financial crime risks in trade finance*. [Thematic Review. TR13/3].
Foucault, M. (1977). *Discipline and punish: The birth of the prison*. London: Penguin.
Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder: Westview.
Gendron, Y. (2002). On the role of the organization in auditors' client-acceptance decisions. *Accounting, Organizations and Society*, *27*(7), 659–684.
Giddens, A. (1985). *The nation-state and violence*. Cambridge: Polity Press.
Giddens, A. (1990). *The consequences of modernity*. Stanford: Stanford University Press.
Gordon, D. (1987). The electronic panopticon: A case study of the development of the National Crime Records System. *Politics and Society*, *15*(4), 483–511.
Guenin-Paracini, H., & Gendron, Y. (2010). Auditors as modern pharmakoi: Legitimacy paradoxes and the production of economic order. *Critical Perspectives on Accounting*, *21*, 34–158.
Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622.
Hansen, J. D., & Peterson, N. D. (2010). A comparison of auditors' and accounting students' ability to identify fraud risk. *Journal of Forensic Studies in Accounting and Business*, *2*(1), 11–19.
Hines, R. D. (1989). Financial accounting knowledge, conceptual framework projects and the social construction of the accounting profession. *Accounting, Organizations and Society*, *2*(2), 72–92.
Hoskin, K. W. (1994). Boxing clever: For, against and beyond Foucault in the battle for accounting theory. *Critical Perspectives on Accounting*, *5*(1), 57–85.
Humphrey, C., & Owen, D. (2000). Debating the power of audit. *International Journal of Auditing*, *4*(1), 29–50.
Humphrey, C., Moizer, P., & Turley, S. (1992). The audit expectations gap—plus ça change, plus c'est la même chose? *Critical Perspectives on Accounting*, *3*(2), 137–161.
Institute of Chartered Accountants for Englandand Wales (2017). *SARs case studies*. https://www.icaew.com/en/technical/legal-and-regulatory/money-laundering/uk-law-and-guidance/sars-case-studies.
Jessop, B. (2007). From micro-powers to governmentality: Foucault's work on statehood state formation, statecraft and state power. *Political Geography*, *26*, 34–40.
Kerry, J., & Brown, H. (1992). *The BCCI affair*. Washington DC: US Government Printing Office.

Latour, B. (1987). *Science in action*. Cambridge, Mass: Harvard University Press.
Lehman, C. R., & Okcabol, F. (2005). Accounting for crime. *Critical Perspectives on Accounting*, *16*, 613–639.
Lehman, G., & Thorne, K. (2015). Corruption: Criminality and the privatised state: The implications for accounting. *Accounting Forum*, *39*, 366–370.
Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.
Lyon, D. (2001). *Surveillance society: Monitoring everyday life. buckingham*. England: Open University Press.
Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. *Information, Communication and Society*, 5, 242–257, MacLullich, K.K. (2003). The emperor's 'new' clothes? New audit regimes: Insights from Foucault's technologies of the self. *Critical Perspectives on Accounting*, *14*, 791–811.
Malsch, B., & Gendron, Y. (2013). Re-theorizing change: Institutional experimentation and the struggle for domination in the field of public accounting. *Journal of Management Studies*, *50*(5), 870–899.
Martinez, D. E. (2011). Beyond disciplinary enclosures: Management control in the society of control. *Critical Perspectives on Accounting*, *22*, 200–211.
McKinlay, A., & Starkey, K. (Eds.). (1998). *Foucault, management and organization theory: From panopticon to technologies of self*. London: Sage.
Melnik, S. V. (2000). The inadequate utilization of the accounting profession in the United States Government's fight against money laundering. *Legislation and Public Policy*, *4*(143), 143–173.
Miller, P., & O'Leary, T. (1987). Accounting and the construction of the governable person Accounting. *Organizations and Society*, *12*(3), 235–265.
Miller, P., & Rose, N. (1990). Governing economic life. *Economy Society*, *19*(1), 1–31.
Mitchell, A., Sikka, P., & Willmott, H. (1998). Sweeping it under the carpet: The role of accountancy firms in money laundering. *Accounting Organizations and Society*, *23*(5/6), 589–607.
Moore, D., Tetlock, P., Tanlu, L., & Bazerman, M. (2006). 'Conflicts of interest and the case of auditor independence: Moral seduction and strategic issue cycling'. *Academy of Management Review*, *31*, 1–20.
Morales, J., Gendron, Y., & Guenin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. Accounting. *Organizations and Society*, *39*, 170–194.
Neu, D., & Heincke, M. (2004). The subaltern speaks: Financial relations and the limits of governmentality. *Critical Perspectives on Accounting*, *15*(1), 179–206.
Neu, D., Everett, J., Rahaman, A. S., & Martinez, D. (2013). Accounting and networks of corruption. *Accounting Organizations and Society*, *38*, 505–524.
Neu, D., Everett, J., & Rahaman, A. S. (2015). Preventing corruption within government procurement: Constructing the disciplined and ethical subject. *Critical Perspectives on Accounting*, *28*(1), 49–61.
Nock, S. (1993). *The costs of privacy: Surveillance and reputation in america*. New York: Aldine De Gruyter.
Orwell, G. (1949). *Nineteen eighty-four*. New York: Penguin.
Picard, C.-F., Durocher, S., & Gendron, Y. (2014). From meticulous professionals to superheroes of the business world. *Accounting, Auditing & Accountability Journal*, *27*, 73–118. [!].
Ponemon, L. A. (1990). Ethical judgments in accounting: A cognitive-developmental perspective. *Critical Perspectives on Accounting*, *1*(2), 191–215.
Poster, M. (1990). *The mode of information*. Chicago: University of Chicago Press.
Poster, M. (1997). *The second media age*. Cambridge, Massachusetts: Polity Press.
Power, M. (1997). Expertise and construction of relevance: Auditors and the environmental audit. *Accounting Organizations and Society*, *22*, 123–146.
Quessada, D. (2010). De la sousveillance. La surveillance globale, un nouveau mode de gouvernementalite. *Multitudes*, *40*(1), 54–59.
Reinstein, A., Moehrle, S. R., & Reynolds-Moehrle, J. (2006). Crime and punishment in the marketplace: Accountants and business executives repeating history. *Managerial Auditing Journal*, *21*(4), 420–435.
Rose, N., & Miller, P. (1992). Political power beyond the state: Problematics of government. *British Journal of Sociology*, *43*(2), 173–205.
Sikka, P., & Hampton, M. P. (2005). The role of accountancy firms in tax avoidance: Some evidence and issues. *Accounting Forum*, *29*(3), 325–343.
Stanley, J., & Steindhardt, B. (2009). Bigger monster, weaker chains: The growth of an american surveillance society. In D. M. Kaplan (Ed.), *Readings in the philosophy of technology*, Rowman and Littlefield.
Staples, W. (1997). *The culture of surveillance: Discipline and social control in the United States*. New York: St. Martin's Press.
Townley, B. (1994). *Reframing human resource management: Power, ethics and the subject at work*. Thousand Oaks, California: Sage Publications.
Viale, T., Gendron, Y., & Suddaby, R. (2017). From mad men to math men: The rise of expertise in digital measurement and the shaping of online consumer freedom Accounting. *Auditing & Accountability Journal*, *30*(2), 270–305.