Organizational tensions arising from mandatory data exchange between the private and public sector: The case of financial services

Ball, K., Canhoto, A., Daniel, E., Dibb, S., Meadows, M. & Spiller, K.

Original citation & hyperlink:
Ball, K, Canhoto, A, Daniel, E, Dibb, S, Meadows, M & Spiller, K 2020, 'Organizational tensions arising from mandatory data exchange between the private and public sector: The case of financial services' Technological Forecasting and Social Change, vol. 155, 119996. https://dx.doi.org/10.1016/j.techfore.2020.119996

DOI 10.1016/j.techfore.2020.119996
ISSN 0040-1625

Publisher: Elsevier

Organizational tensions arising from mandatory data exchange between the private and public sector: The case of financial services

Kirstie Ball
School of Management, University of St Andrews

Ana Canhoto*
Brunel Business School, Brunel University London

Elizabeth Daniel
The Open University Business School

Sally Dibb
Centre for Business in Society, Coventry University

Maureen Meadows
Centre for Business in Society, Coventry University

Keith Spiller
School of Social Sciences, Birmingham City University

* Corresponding author

Brunel Business School, Brunel University London, Kingston Lane, Uxbridge, UB8 3PH
Ana.canhoto@brunel.ac.uk

Abstract

This paper examines the organizational tensions arising from mandatory data exchange initiatives between private and public organizations. The focus is the UK financial services sector, which is required to monitor and report on customer identities and transactions under the country's Anti-Money Laundering/Counter-Terrorist Finance (AML/CTF) regulations. The transferred data are generated from existing organizational activities, systems, processes and working patterns; we examine how government demands for such data affect commercial priorities, customer relationships and working patterns in the sector. We adopt an exploratory approach to investigate this phenomenon, consisting of 16 in-depth interviews, analysis of documents and two case studies. Three contributions are made. First, we use remediation theory to show that existing organizational arrangements are reconfigured at multiple analytical levels, creating tensions between the organizations' commercial and compliance roles. Second, we establish the information flow as an appropriate unit of analysis in the study of data exchange mechanisms and reveal the flows that characterise AML/CTF compliance for financial services organizations. Finally, we adopt a 'set theoretic' perspective on multi-level organizational research, to argue that the multi-level effects of this regulation can be examined in parallel.

Keywords: Data exchange mechanisms, information flows; financial services; anti-money laundering; counter-terrorist finance; remediation; multi-level analysis.

Acknowledgements

The research featured in this paper was funded by a Leverhulme Trust Project Grant, no F/00269/X

1.0 Introduction

Since the terrorist attacks of 9/11 and the first use of the term 'War on Terror'[1], the growing prevalence and intensity of surveillance regimes on civilian populations has been under increasing scrutiny. The Proceeds of Crime Act 2002 and the Immigration, Asylum and Nationality Act 2006 are just two examples of UK legislation that mandates the private sector to collect and transfer communications, financial, identification and travel data about the general population to government. These and other laws place individuals' data at the heart of national security policy. The private sector is thus enlisted in collecting and processing such data; constituting what Loader and Walker (2010) identify as a hybrid, networked security landscape, within a new political economy of surveillance (Ball and Snider, 2013).

Given the transferred data are generated from existing organizational activities, systems, processes and working patterns (Bergström et al., 2011), concerns emerge about how these new government demands for customer data align with the activities of private sector organizations. The limited evidence available (e.g. Dibb et al., 2014) suggests that tensions are created because the forced participation of commercial organizations in national security programs leads to a dramatic reorganization of work practices. For example, in the travel sector, the likely negative consequences of the UK's e-Borders initiative have led travel firms to seek "to return their commercial interests (and those of their customers) to the fore, and to restore equilibrium to the disrupted system" (Dibb et al., 2014, p. 58). With regard to military and security services, Godfrey et al. (2014, p. 119) argue that "the absence of clear and robust forms of accountability, oversight and regulation makes is extremely difficult to grasp either the activities or the true scale" of the private security industry. Yet very little research has addressed how governments' demands for customer data affect commercial priorities, customer relationships and working patterns in other industry sectors.

[1] https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html

Crucially, a new discourse is giving "senior management in financial institutions a new public responsibility beyond the direct interest of shareholders" (Power, 2013, p. 538).

This paper examines how organizations in the UK financial services sector have adapted to the data exchange demands arising from the Anti-Money Laundering/Counter-Terrorist Finance (AML/CTF) regulations. Three contributions are made. First, drawing on remediation theory (Bolter and Grusin, 2000), we show how the capture and transfer of commercial, transaction data for national security purposes starts to reconfigure the context in which that information is collected. Specifically, we highlight how the AML/CTF data capture and transfer activities prompt reconfigurations of existing organizational arrangements at multiple levels of analysis, creating tensions in terms of the financial organizations' commercial priorities, customer relationships and working patterns. Second, we show that such programs rely on the establishment of an information flow between the private and public organizations. We argue that the information flow is the appropriate unit of analysis for the study of national security programs which, like AML/CTF regimes, are based on the analysis of individuals' behavioral data. Third, drawing on Lacey and Fiss (2009), we adopt a 'set theoretic' as opposed to a 'nested' perspective on multi-level organizational research, to argue that the multi-level effects of inter-organizational data exchanges can be examined in parallel. This approach allows the application of multiple analytical lenses to the problem, enabling the development of a rounded understanding of the impact of large scale private-public data transfer programs.

The AML/CTF phenomenon extends beyond the UK to other countries around the world (Lepoutre and Oguntoye, 2018; Meifang et al., 2018; Dey et al., 2019). Likewise, large scale data transfer programs are not confined to the financial services sector. Rather, they are part of the ever-growing expansion of generalised surveillance practices powered by big data, cloud services and other technological developments, which are performed by commercial

organizations (Zuboff, 2015) and governments alike. For example, the mass surveillance of its citizens by the Chinese government has been widely discussed[2][3][4]. Therefore, the contributions from this paper extend beyond its empirical scope.

The paper is organized as follows. In Section 2, we set out the conceptual background of the study, outlining the flows of customer data and information that are part of AML/CTF regimes, exploring the information flow as the most appropriate level of analysis and establishing remediation as a valuable theoretical lens. Section 3 explains our approach to data collection and data analysis. Section 4 presents our multi-level findings: at the individual and task level; the intra-organizational level; and the organizational and inter-organizational level. Section 5 highlights and discusses the study's main contributions to the understanding of the impact of information flows in financial services between private firms and the public sectors. In Section 6 the paper concludes with comments concerning a future research agenda.

2.0 Conceptual background

2.1. The role of transaction data

Money laundering "describes the process through which illicit profits are hidden from authorities, often by using a combination of complex financial transactions and financial secrecy; and re-introduced into the financial system under the guise of legitimate transactions" (Sica, 2000: 47). Since most criminal activity is considered to be financially motivated (Byrne, 2011), hindering the movement of criminal funds is believed to reduce all

[2] https://www.spectator.co.uk/2019/07/chinas-surveillance-technology-is-terrifying-and-on-show-in-london/

[3] https://www.nybooks.com/daily/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state/

[4] https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/

forms of crime, from small scale tax evasion to international terrorism, or the proliferation of weapons of mass destruction (FAFT, 2019).

Financial transactions leave electronic traces, which can be pursued and connected to individuals and their networks (DeGoede, 2012). Thus financial intelligence has become a key component of modern national security (DeRosa, 2004), with governments around the world exploring how they can harness and utilize big data (e.g. Amankwah-Amoah, 2016; LaBrie et al., 2018; Jun et al., 2018). In particular, there is growing interest in exploring the potential of big data analytics (BDA) and artificial intelligence (AI) in the international fight against money laundering and terrorism financing (Kaminski & Schonert, 2018). Other technologies, such as machine learning/artificial intelligence, natural language processing and distributed ledger technology are also considered essential to support the processing and analysis of ever-growing databases of transaction data (Grint et al., 2017).

2.2. Information flow

National security programs, such as AML/CTF, are reliant on having access to the records of financial transactions carried out by suspect individuals. Financial services organizations operate as points of entry for cash into the financial system and as major facilitators of moving money globally. They also have a history of collecting and analyzing financial transaction data for commercial purposes, such as customer relationship management programs (Canhoto et al., 2017). Customer information is now so central to the way financial services organizations operate, that customer data has been described as the currency of financial institutions (Kuljis, Macredie and Paul (1998). That is, these private organizations typically have both the opportunity and the means to collect financial transaction data. Governments worldwide have therefore passed legislation ordering financial service providers to proactively detect and prevent the movement of money to or from

criminal agents, in order to curtail ‘money laundering through the front door’ (Zdanowicz, 2004).

In the UK, the Proceeds of Crime Act (2002) that governs AML/CTF applies to banks, building societies, insurance companies and any other organization dealing in financial transactions. Professional services firms, such as solicitors and accountants, estate agents and dealers in high value goods such as jewellery, boats and luxury cars, are all included.

There are two pillars to the AML/CTF regulations (e.g. Ball et al., 2015). First, financial services institutions should ‘know your customer’ (KYC). This means that firms are required to conduct appropriate identity checks when an account is opened. Further, they must perform ‘customer due diligence’ (CDD), by monitoring all transactions to identify any unusual or suspicious activity based on recognised patterns of behavior (Backhouse et al., 2005; Ball et al., 2015).

The financial institution is required to report any suspicions to the National Crime Agency (NCA), which will investigate and take appropriate action (Backhouse et al., 2005). Failure to disclose suspicious transactions is a criminal offence (JMLSG, 2006), with institutions facing heavy fines and staff risking prosecution if they are seen to fail in their duty to prevent money laundering and terrorism financing. For example, in 2012 HSBC was ordered to pay a fine of $1.9bn for failing to report the financial transactions of a Mexican drugs baron (Arnold, 2018). The reputational, commercial and legal costs of failing to comply have resulted in an exponential increase in reporting levels, from 5,000 reports per year in 1995, to 463,938 in 2018[5]; with most reports being made by the big four UK banks – National Westminster Bank, Lloyds, Barclays and HSBC.

In summary, as an intermediary in the AML/CTF regime, the financial services

[5] https://nationalcrimeagency.gov.uk/who-we-are/publications/256-2018-sars-annual-report/file

organization's primary role is to pass data concerning suspicious transaction activity of their customers to the NCA for further investigation. The financial institutions' organizational systems, processes, employees and resources are mobilised to produce a flow of information from the customer to the government. In this process, as data are transferred from one agent to the other, their purpose and nature changes. These changes are illustrated in Table 1 and unpacked in the next section.

Stage	**Cash enters the financial system**	**Financial organization conducts KYC and CDD**	**NCA conducts further investigations**
Data	Transaction records	Suspicious transactions	ML suspects
Generated by	Customer	Financial organization	NCA
Generated via	Financial behavior	Analysis of transaction records	Analysis of suspicious transactions reports
Transferred to	Financial organization	NCA	Law enforcement agencies
Transferred for the purpose of	Completing commercial transaction	Regulation compliance	Criminal investigation

Table 1. Information flows in Anti-Money Laundering/Counter-Terrorist Finance

2.3 Remediation and the information flow

We draw on remediation theory (Bolter and Grusin, 2000), to examine what happens in the AML/CTF information flow and the impact it has on the financial services organization at the centre of this data collection and transfer exercise. Remediation refers to the incorporation of one medium into another. The concept was originally employed to analyze the significance of new forms of digital media, such as how changing the format of commercially available literature from paper to e-book, impacted on the publishing industry.

Remediation is also at the heart of AML/CTF. Transaction data are not only transformed in terms of their format, but also in terms of their meaning, the practices to which they are subject and their route through the organization. Remediation theory also states that the act of re-mediation refashions the networks of actors, resources and other media that produce it (Bowker and Star, 1999). Accordingly, in our examination of information flows in AML/CTF, we specifically investigate the networks of actors involved, the resources used and the media produced in the process.

In terms of actors, AML/ CTF regulations and guidance have an individuating focus on the employee and their morality (Morales et al., 2014). However, organizational elements such as size, structure and culture can also shape responses to the regulations (Gabbioneta et al., 2013). Financial institutions are required to respond to the regulations but each needs to identify the riskiest products, customers and territories on which to focus their AML monitoring efforts. In AML/CTF, the organization and its employees become the means by which external criminal and terrorist wrongdoing are detected. As regulatory requirement becomes embedded within organizational processes, the ongoing work of various employees is re-oriented to balance the reporting and the commercial demands (e.g. Dibb et al., 2014).

In terms of the resources used, AML/CTF has become embedded in the systems and practices of UK retail banks. Even though there is scepticism regarding AML's effectiveness to detect and prevent crime (Grint et al., 2017), UK financial services providers have invested

heavily in customer profiling and transaction monitoring technology to assist in these efforts; circa £5m a year according to the latest estimates by the regulator (Arnold 2018). A clash of priorities and transparency problems arises between the commercial processes and national security (Amicelle and Favarel-Garrigues, 2012; Amicelle, 2011). Balani (2019) notes that firms find the training requirements and financial burden of AML/CTF regulations to be high, while Ryder (2008) suggests that AML/CTF presents organizations with little to gain but much to lose.

Regarding new media forms, transaction records that were initially captured as part of an ongoing commercial relationship, once analyzed through a compliance lens, re-emerge as records of suspicious transactions to be included in suspicious transaction reports. Furthermore, once those reports and the associated data records are exchanged with the NCA and subject to further analysis, they assume yet a different form; namely records of money laundering suspects, to be subjected to criminal investigation. By ensuring that data about customers are captured and transferred, the organization remediates the customer, their behavior and data about their transactions as the consumer of a financial services product, into a data-subject with potential to threaten national security. In turn, the banking customer relationship is transformed from one of privacy and protection into one which incorporates suspicion and surveillance (Backhouse et al, 2005). Reporting customers runs against the traditional strategic objectives of banks, the culture of privacy (Donaghy, 2002) between a bank and its customer, and how performance is assessed and rewarded (Canhoto, 2008). Criminal activities involving data are also highly varied and can sometimes be difficult to distinguish from legitimate activities (e.g. FATF 2018). The technical limitations arising from the lack of reliable profiles mean that financial intelligence is a ‘speculative endeavour’ (de Goede, 2012, p. 58); especially because money laundering evolves as criminals attempt to take advantage of new financial products or trading strategies, such as using mobile payments

(Whisker & Lokanan, 2019) or virtual currencies (Vandezande, 2017). Concerns are raised regarding how financial services organizations adapt to this intermediary role and how this phenomenon might be studied.

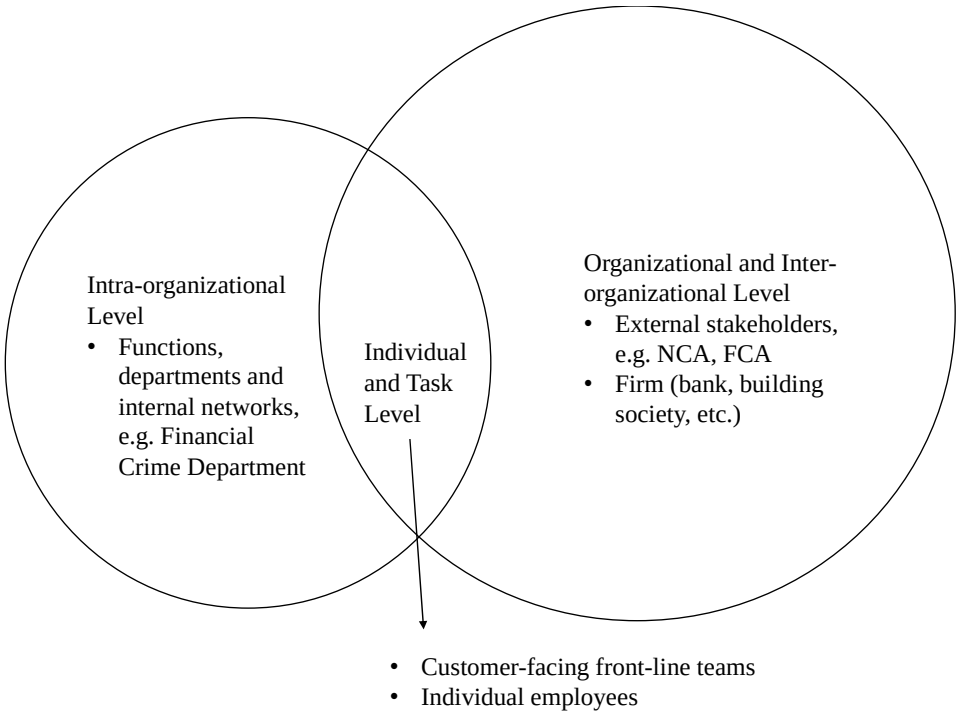
The remediation of customer data into suspicious money laundering activity has the potential to reconfigure local social, political and material orders within the organization, which we investigate empirically, as detailed in the next section.

Empirically exploring the AML/CTF regime involves examining how this remediated information flow comes into contact with different organizational elements. The selection of remediated information flow as a unit of analysis is a deliberate theoretical move which highlights these multi-level effects (Chen, Mathieu, and Bliese, 2004; Mathieu and Chen, 2011). There are, however, some conceptual issues with the parallel treatment of different levels of analysis within one analysis. A common conceptual approach to an organization's hierarchical and analytical levels is to think of them as nested within each other. This approach has been adopted in the study of organizational fraud regulation (Shadnam and Lawrence, 2011) but is identified elsewhere as inhibiting multi-level analyses (Lopes Costa, 2013).

Reflecting these concerns, we adopt a networked-style 'set logic' to identify connections in our dataset (Lacey and Fiss, 2009). Our approach is illustrated in Figure 1, where we highlight the multiple and overlapping 'sets' in our analysis: we explore remediation points at the individual and task level; at the intra-organizational level; and at the organizational and inter-organizational level. Set logic moves away from the use of analytical levels as de facto groupings of data in a research problem-space. Instead, it views organizational problem spaces as overlapping multidimensional groupings of phenomena occurring at different analytical levels. This approach does not structure the problem space *a priori* as nested approaches tend to. Accordingly, membership of the multidimensional

AML/CTF ‘set’ of phenomena features organizational elements, which might be different in analytical level, but similar in that they are reconfigured and drawn together by the thread of information flow. A nested approach is also not appropriate because AML/CTF, as a set of external regulations, is not necessarily aligned with an organization’s core commercial activities and interests. It only directly affects the parts of the organization which come into contact with the customer and take part in risk assessing their behavior, identity and transaction patterns. The entire organization is not nested within the remit of these regulations, only parts of it interact, adapt and change as a result. For example, certain departments of the financial services organization will interact with law enforcement agencies to assist in cases not related to AML/CTF, such as helping to trace the last movements of a missing person. Furthermore, as those in charge of AML/CTF within the organization are not in a hierarchical management relationship with the front line workers and managers who are looking for suspicious activity, hierarchical nesting is not present either. Hence, we view the boundaries between regulatory activity and customer focused activity as permeable, not necessarily hierarchical and as connected by information flow, forming the AML/CTF ‘set’.

Figure 1. Analytical levels in Anti-Money Laundering/Counter-Terrorist Finance information flows



3.0 Method

3.1 Data Collection

This paper pursues a fine-grained thematic analysis of interview data to explore the remediation processes and information flows which constitute AML/CTF compliance data exchange schemes. The study is distinctive in its use of primary qualitative data. Most AML/CTF research tends to rely on *post hoc* analysis of secondary sources such as court reports, official enquiry reports and historical documents (e.g., Compin, 2008; Mitchell et al., 1998; Sathye and Islam, 2011). Where contemporary primary empirical data are used, the emphasis is usually on survey-based methodologies (e.g., Pok, Omar and Sathye, 2014). Only a few studies draw on interview-based accounts (e.g., Canhoto, 2008).

An exploratory research method was followed, with data collection unfolding in two phases. During the first phase, detailed insights were gathered into the research context through an in-depth review of the AML/CTF practitioner literature, attendance at financial

service industry events devoted to crime detection[6], and key informant interviews. Specifically, 16 interviews were conducted with senior staff from regulatory bodies and industry associations, as well as senior executives and MLROs from investment banks, retail banks, insurance companies and building societies. Analysis of these interviews, together with notes taken at several industry events, generated vital information about the institutional and regulatory context of AML/CTF, as well as the strategic and operational issues facing financial services institutions responding to the regulations. The insights gained from this phase also helped the researchers to decide which specific organizational (inter as well as intra), individual and task elements to focus on in the second phase of data collection (in accordance with the set-theory perspective), to refine the terminology to be used in that phase, and to interpret the case study data gathered.

The second data collection phase explored the operational impacts of the regulations in two case organizations: a bank (Company A) and a building society (Company B) which had recently merged, generating a further ten interviews from which the data within this paper are drawn. Due to the sensitive nature of AML/CTF operations, it was extremely difficult to secure access: many avenues were tried with many different organizations until a personal recommendation secured access to the case organizations. The recent merger placed Company A in control of the AML/CTF operation with Company B reporting to Company A. One MLRO covered both companies. In each company, financial crime managers and staff were interviewed (two from Companies A and B respectively) and customer facing staff in high street branches or call centres (four from Company A and two from Company B).
The interview guide for the case study interviews reflected the three levels of remediation described in section 2.3: the **actors** involved, specifically the individuals and organizational

[6] Events were run by the Institute of Money Laundering Protection Officers (IMPLO)

units; the **resources** implicated, to examine the impact of the regime on the organization; and the **media**, to capture the operational adaptations made as a result of the regulations.

Where permission was granted, interviews were recorded, otherwise contemporaneous notes were taken. The majority of interviews were undertaken by at least two researchers, allowing comparison of notes to ensure understanding and completeness.

3.2 Data Analysis

This paper explores the multi-level adaptations which take place in financial services organizations' actors, resources and media, as they comply with AML/CTF. The analytical approach follows Neu et al.'s (2013: 510) study of accounting and networks of corruption in which they describe "follow[ing] the flow of money through a complex web of financial transactions". In this study, rather than focusing on flows of money, we focus on the flows of data and information between private and public organizations. The following aspects were considered: (i) the impact of the regime on financial services institutions; (ii) the flow of data and information about suspicious customers and transactions through and beyond each of the organizational elements of the AML/CTF set identified in Figure 1; and (iii) how information is remediated as it moves across the AML/CTF set (Bolter and Grusin, 2000; Lee, 2012).

Data were ordered using a fine grained and iterative thematic analysis (Boyatzis, 1998). Patterns in explanation and reasoning were inductively explored by cross-referencing verbatim coded extracts of interviewee data to construct the AML/CTF compliance process. By progressively refocusing the thematic analysis, more detailed codes were produced. The resultant record linked the situated fieldwork, the texts which represented it and the ideas which underpinned interviewees' accounts. Data were coded in N-Vivo; with 189 coded extracts of interview data identified which featured information flow as a theme. These 189 extracts were sub-coded to reflect six different areas of AML/CTF practice. The fine-grained

reading of the codes emerged in a coding workshop in which the researchers worked together to identify the information flows and remediation processes in each extract. Inter-coder reliability was high, but where differences occurred these could be resolved by looking at the text in its fuller context (Miles and Huberman, 1994). By combining data from multiple interviewees with differing roles in the process, and augmenting with the additional data sources from phase 1 of the data collection, a detailed picture of the AML/CTF compliance process across the different organizational elements and at the different levels of analysis of the AML/CTF set, began to emerge.

Insight and opportunities for reflection during the data analysis were provided by referring to information gathered from the key informant interviews, corporate and media documents, and the industry events. Guidance on AML/CTF practice provided by the Basel Committee, the UK National Crime Agency and the Financial Conduct Authority was also consulted, while a workshop for research participants at the conclusion of the project provided a further opportunity to reflect on the findings.

4.0 Findings

The findings are organized into four parts. We begin with an overview of the organizational elements that enable the data exchange, in order to provide the context in which the information flows take place, and to explain how the financial crime department is positioned as the hub of the AML/CTF operation. We then present the findings regarding the three types of remediation (namely actors, resources and media) occurring in each of the three levels of analysis of the AML/CTF 'set'. The individual and task level focuses on front line staff. The intra-organizational level reveals how the financial crime departments bring together different information sources to be remediated into evidence for suspicious activity reports. The organizational and inter-organizational level draws on strategic issues, such as competition

and corporate reputation in relation to external stakeholders like government and industry associations. Table 2 summarises the findings. The quotes presented in the section are representative, chosen collectively by the researchers.

	Actors	**Resources**	**Media**
Individual and task level	New roles (e.g., financial crime manager) and performance goals (e.g., compliant sale)	New skill sets (e.g., keeping one eye on service and another on suspicion) and systems (e.g., Money Laundering Detection Systems)	Customer (e.g., nationality, credit score, age) and context (e.g., use of a translator, car parked outside the branch)
Intra-organizational level	CRM system used for AML/CTF purposes, with asymmetrical communication between departments	Transaction Monitoring System, financial crime analysts, and the emergence of new expertise	Evidence files based on tacit knowledge about 'normal' behavior; adjustable search parameters; and watch lists
Organizational and inter-organizational level	Good citizenship role vs. commercial obligations	Expenditure on AML/CTF vs sales	Decision to close accounts; profit vs. dirty money

Table 2. Summary of findings

4.1 Organizational Elements

The organizational arrangements for managing data flow in the banks reflected those described in the literature, as captured in Table 1. Employees, customers, financial crime departments and strategic organizational actors were enrolled into producing the information flow. Front line customer facing staff, financial crime departments and the companies' MLRO – a strategic level role – each remediated information about suspicious transactions towards the NCA. Front line customer facing staff, in branches and call centres, initiated information flows by implementing 'Know Your Customer', gathering and validating information from identity documents when a customer opens an account, and 'Customer Due Diligence' by monitoring customer behavior during transactions and reporting anything unusual to the financial crime department.

The organization's financial crime department was the hub of AML/CTF, receiving information about AML/CTF from all directions. It received reports from staff via the money laundering detection system, which were investigated using in-house investigators and outsourced service providers, if appropriate. A decision was then taken on whether to act upon these suspicions and submit a Suspicious Activity Report (SAR) to the National Crime Agency (NCA). The NCA was the ultimate recipient of the SAR. Upon investigation, the NCA decided if and how to pursue customers directly, finishing the information flow between customers, financial services organizations and government. The next section examines these remediation points in more detail. In each case, the data remediated and the organizational elements which were reconfigured as a consequence, are explored.

4.2. Individual and task level: Customer facing front line

The first set of remediations occurred at the customer facing front line. Front line staff were responsible for identifying suspicious behavior in customers and reporting it to the financial crime department, alongside performing their usual customer service functions such

as opening accounts, accepting deposits or providing financial advice. According to one financial crime manager, front line staff bore the burden of the vigilance required to initiate information flows about customers:

> *Anti-money laundering, partly because of our size and partly because of the nature of our business, it's not an easy thing to fully automate …. and so we have a mixture of system support, which probably only forms 30% or 40% of our controls, and the rest of it is due diligence by the staff*. (Financial Crime Manager, Company A)

Various pieces of information became remediated into the front line employees' decision about whether to report an incident using the company's Money Laundering Detection System. First, staff used information from existing information systems they were able to access. For instance, credit scoring systems enabled the employee to evaluate a customer's identity and creditworthiness. Judgements were also partly informed by the customer management system, which displayed all account transactions and other customer details during the customer interaction. Using this system, staff in both companies were able to decide whether customer behavior was 'unusual' compared to their previous account usage. Employees also used their knowledge of the AML/CTF regulations, which warned about very young or very old customers. These customers' lack of financial independence afforded them greater scrutiny in case they were being manipulated by another party (JMLSG, 2006). Information gleaned from employees' previous experience also sensitised them to nationality[7]. For example, a customer from a country associated with organized crime or terrorism, and/or presenting with very poor language skills, might be sources of suspicion. This branch manager described a situation where a newly arrived immigrant who could not speak English was trying to open an account. Eventually the obvious language barriers

[7]In early 2014 BBC Radio 4's 'Money Box' detailed a court case brought by nine innocent Iranian citizens living in the UK whose bank accounts had been frozen using the money laundering regulations http://news.bbc.co.uk/1/shared/spl/hi/programmes/money_box/transcripts/money_box_04_jan_14.pdf accessed 5th June 2019.

caused the manager to become suspicious:

> *…he can't speak English so how can I physically open …him an account? That's difficult because you might have his brother sat next to him who has brought in four people in one week – this has happened before – and he's trying to open an account for these people because he is doing the translation for his family. How do you know that he's telling that person what you're telling him?* (Senior Branch Advisor, Company A)

Contextual factors in the branch and customer appearance also informed their judgement:

> *…the customer has come in, he's drawn £4,000 and what he's said it's for is a new car. However, outside … he went back outside and got in a Mercedes that was 2011, brand new, it was like this was the registration plate, the customer had a tattoo on his left arm…* (Senior Branch Advisor, Company A)

With multiple information sources remediated into their decision, front line staff described three ways in which the nature of their work had changed because of AML/CTF. First, at the individual level of analysis, staff skillsets had been reconfigured. Staff described how the tacit AML/CTF knowledge they had developed caused them to approach the customer interaction with one eye on service and another on suspicion. Such tacit knowledge enabled staff to distinguish between suspicious behavior or otherwise. Front line staff made judgements about the customer's demeanour, their comportment and attire, the circumstances of their arrival and departure from a branch, or whether 'things added up' about them or not, based on their tacit knowledge and experience of working in a customer-facing role, while possibly also drawing on their 'instincts' or 'stereotypes' of what might constitute suspicious activity.

Second, customer handling skills became reconfigured. Sales-like performativities were mobilised around security to ensure remediation occurred: putting the customers off, keeping them at ease, listening, analyzing and verifying what the customer was saying all

featured (see also Ericson and Doyle, 2004). A bank call centre employee described the process of keeping the customer comfortably in suspense:

> *You don't let on in any way that you're suspicious. You just process as normal. Say, okay, that's fine, here's your application number. One of three things, it'll either decline, it will either go through accepted, which means it's agreed, so just around formalities, or it will refer, needing the further information … Let's say they come back in a couple of days to get a decision, it could be that there are notes from fraud on there, from AML, because they're checking things. And we'll say, you just have to wait a couple of days, it's still coming through, we're still waiting for the result from the team. Not letting on in any way that we're checking into them, basically.* (Call Centre Employee, Company B)

A bank branch employee noted that *'dealing with people 24/7 means actually you're quite good and quite adept at having those kinds of conversations'* (Senior Branch Advisor, Company A). The regulations were an added motivator. As a result of having to report any suspicions they had about the customer without 'tipping them off'[8], front line retail finance employees were required by law to maintain a veneer of service in the face of suspicion. 'Tipping off' involves letting a potential suspect know they are under suspicion, which would compromise any future criminal investigation. Staff could receive at best a fine, or at worst, a five year prison sentence if found guilty of such offences.

Finally, at the task level of analysis, sales work and its performance management had been reconfigured to incorporate notions of AML/CTF compliance. The 'compliant sale' emerged as a performance ideal: one which incorporates both commercial and regulatory priorities; and against which employees were performance managed. This branch manager succinctly explains how the performance rating system picks up compliance problems in

[8] Proceeds of Crime Act (2002) Section 333A (1)

sales transactions, reflecting how performance management processes have institutionalised compliance alongside sales:

> *...we are salespeople ... however it doesn't matter how good your sales are, your sales could be 200%, if you're not managing your compliance ... again you would not get 'achieving' [reference to internal performance rating system], because you're not doing your job, regardless as to how good the sales are.* (Branch Manager, Company B)

In summary, at the front line remediation point, different forms of information were used by the employee to judge whether customer behavior was suspicious or not. If so, it was remediated into a report to the financial crime department. Information from existing systems, the customer's characteristics and observed behavior as well as their knowledge of normal behavior on different accounts, were remediated. Reconfigurations also occurred in terms of the employees' tacit knowledge and skills, as well as in terms of the nature of their task and its performance management.

4.3 Intra-organizational level: Financial crime department

The second remediation point occurred in the financial crime departments of the case organizations. The work of the financial crime departments primarily involved the remediation of new information into evidence files on potential wrongdoers. This information came from different sources. Information received from the front line was investigated and remediated to produce new insight and intelligence about the crime and risk-based aspects of the organization's operations. In addition, the department monitored all transactions in real time and screened them on a daily basis using a Transaction Monitoring System (TMS). Outputs from the TMS were investigated and added to files if they indicated suspicious behaviour. The search parameters within the TMS were defined for each kind of financial

services product provided by the bank. To assist in setting their search parameters, the departments remediated information from organizational Customer Relationship Management (CRM) software relating to consumer profiles. The profiles indicated an acceptable range of product use, beyond which customer activity would be deemed unusual or suspicious. Financial crime department employees highlighted how different types of account attract different rules:

> *I think we've got about nine rules with regard to the savings accounts and five on mortgage accounts, and we'll go and look … For example, one of the rules could be a large cash deposit or large cash withdrawal. If it happens on a customer's account, we would get an alert. That comes in every morning.* (Financial Crime Employee, Company B)

Finally, as with front line staff, financial crime staff also had tacit knowledge as to what a particular kind of consumer using a particular product would 'normally' do with it. Whether a customer appeared to be conforming to that lifestyle and the range of financial transactions that accompanies it was enough to raise questions:

> *…it's all about lifestyles, and obviously different accounts are for different lifestyles. Because obviously a very basic account would be for someone who may not be earning that much, hasn't got enough of a credit report to get a higher level account. So really, although you can't use it as law, really, though, looking at one account can let us know or give us an idea of what we shall be seeing going through that account, as compared to someone else.* (Financial Crime Employee, Company A)

Tacit knowledge also influenced the sensitivity of the search parameters used, so that a manageable amount of positive identifications resulted, as this MLRO explains:

> *…the trick is making sure you don't produce so many false positives that you're just blinding your analyst … Because the risk is if you're sitting there just trailing through*

thousands of payments … you're going to miss something because you're going to be blinded by the one that is a match. (MLRO, Company A*)*

As well as monitoring the transactions of their customers, they were required to run TMS searches in response to new watch lists released from NCA, HM Treasury, Department of Work and Pensions, local authorities or the police. Such requests would concern finding evidence of persons suspected of being involved in organized crime or terror, or who were politically exposed. Once enough evidence had been amassed, the department would make a recommendation to the MLRO that a SAR should be submitted.

The activities of the financial crime departments studied reconfigured elements at the intra-organizational level of analysis: organizational communication patterns and internal boundaries. First, interesting communication patterns emerged from the vast upward flow of information to financial crime. The financial crime departments did not feed back to front line staff on their reports, to avoid influencing how they then dealt with the customer. Chains of secrecy, based on the AML/CTF regulations concerning tipping off, began to characterize interactions between financial crime departments and the rest of the organization, as this branch manager explains:

…they said you won't get feedback; there's two reasons you won't get feedback. One, because if you do get feedback you might treat that customer differently, and that's classed as tipping off, and if the customer gets in tune with that obviously then you're again tipping him off when you might have not meant to. (Senior Branch Advisor, Company A)

The amassing of evidence was also important in financial crime employees' descriptions of their expertise. This had the effect of legitimating new internal boundaries based on this expertise and with whom they shared information. This financial crime employee explains that their sight of the 'bigger picture' afforded them a privileged position:

…we understand a lot more than the front line people will, we still have to make our own decision as to whether it is suspicious; whether we feel that that could do with looking at in a bit more detail in a couple of months' time after we've got a bit more of an idea, their account use, or it's just not suspicious and we can close it off and just wait. It might crop up again, and then we can take the bigger picture. (Financial Crime Employee, Company A)

The insight gained by AML/CTF processes was only rarely shared with other departments or functions because of customer privacy and internal fraud concerns. Where any sharing of information took place, it was done on a 'need to know' basis, as illustrated by this member of the financial crime team:

The only team that our work sometimes feeds into is we have obviously our internal security and risk management teams. Now they deal with, sometimes it could be internal matters, or it could be external matters where maybe we feel a customer is being scammed, so we can then feed that information on to them and say what we think: you need to look at this. But as regards any other department, we don't feed it to anyone. (Financial Crime Employee, Company A)

In summary, at the financial crime department remediation point, different types and sources of information were brought together to be remediated into evidence upon which a legitimate suspicious activity report could be based. Reports from the wider organization, evidence generated by transaction monitoring and the screening of watch lists, were investigated as appropriate. Tacit knowledge developed from CRM systems guided employee judgement and helped to set search parameters. As a result, financial crime evidence and expertise were built to legitimate the work of the department and to influence communication patterns. Information was shared on a highly selective basis but not with the wider organization. Both of these phenomena occur at the intra-organizational level of analysis.

4.4 Organizational and inter-organizational level: Strategic issues

With many different organizational resources being mobilised to meet the AML/CTF regulatory requirements, and with the MLROs occupying a strategic role which covered both case organizations, strategic organizational elements began to reconfigure. In this section, we draw upon insights from key informants working at strategic levels, from industry associations and from government, to focus on perceptions of how AML/CTF changes a firm's ability to compete and its corporate reputation.

In relation to competition, AML/CTF exerted pressure on organizational resources and priorities. One interviewee claimed *"Ultimately banks are not interested in the good citizen role. There are no obvious benefits to the organization of applying AML measures*" (Senior Executive, Retail Bank) and another: *"There is more time and money being spent on overheads, such as regulation and AML, than on sales*" (MLRO, Investment Bank). An additional aggravating factor was the global financial crisis which had put the financial institutions under even greater scrutiny. Each described how AML/CTF issues were given even higher priority than before the crisis, since they did not want to be seen to make further mistakes. As such there was some recognition, as one interviewee suggested, of "*turning a negative into a positive*" and exploring the commercial benefits offered by AML/CTF. This MLRO outlined how pragmatism was necessary:

> *It's just, there's no point in fighting it because it's not … we internally cannot influence the law in the short-term and in the current climate we're just lucky to be able to keep going, sort of thing, so you just make do. And the more time you waste on questioning and all, then the less time you have to actually address the clients' needs I guess*. (MLRO, Retail Bank)

This pragmatism was underpinned by deep tensions between commercial and regulatory priorities, which also surfaced in relation to AML/CTF and corporate reputation. There are strong financial reasons for banks to ignore their obligations under AML/CTF:

> *…if an account is laundering ill-gotten gains, the likelihood is it's going to be quite a good income earner for the bank – that's the reality of it… and this goes right up to senior management… but if we say we've got concerns about this customer and these customers are x y and z, we'll get it closed down.* (Financial Crime Manager, Company A)

It was acknowledged, however, that AML/CTF compliance can make or destroy a bank's reputation:

> *A bank in the US was brought down because of their lax in AML controls – it literally brought them down … the bank doesn't want to be, well, we want to do business, want to make money…but we don't want to make; we don't want to be making the money from dirty money. Or even have that perception that we're doing that.* (Financial Crime Manager, Company A)

In summary, at the point where remediated AML/CTF information flowed out of the organization and was visible at a strategic level, effects at both organizational and inter-organizational levels were observed. Strategic actors identified the ways in which reporting potentially reconfigured both tangible and intangible corporate assets. Resources and reputation were mobilised into compliance rationales, which highlighted that while these regulations intersected transversally with commercial priorities, they nevertheless had the potential to compromise business priorities.

5.0 Discussion

This paper considers how government demands for customer data under the AML/CTF regulations intertwine with the organizational processes and priorities of the financial services organizations in charge of collecting and transferring such data. In this section, we summarise the tensions arising at the three analytical levels and draw out the main contributions of the study. The AML/CTF regulations' requirements position financial services organizations as intermediaries with systems that both enable the transfer of funds and are used to compile and transmit data that evidences wrongdoing (Canhoto et al., 2017). This dual role created tensions between the activities required for the delivery of the original (commercial) service to its customers on the one hand, and those required for the performance of the new (AML/CTF) service to law enforcement on the other. Consistent with previous AML/CTF research (e.g., Amicelle and Favarel-Garrigues, 2012; Ryder 2008), we detected across all levels of analysis a clash between commercial priorities and practices and this security imperative.

5.1 Tensions at multiple analytical levels

At the individual level, this tension was manifested in the way individuals balanced conflicting demands, such as serving versus reporting on the customer; and selling products versus protecting the organization from being involved in AML/CTF. We witnessed attempts to start addressing these tensions and to find common ground between the two conflicting goals, as in the case of the compliant sale. Ball et al (2013) report a similar phenomenon in their study of front line employees in the airline industry, in which they describe attempts to bridge infrastructural gaps, as a coping mechanism in the face of changing workloads and shifting professional identities.

At the intra-organizational level, this tension manifested itself in the creation within the larger commercial organization of a unit with the sole purpose of meeting customer

surveillance obligations imposed by AML/CTF regulations. This unit used financial and technical resources that might otherwise have been directed to achieve commercial goals, and used communication in an asymmetrical way to give primacy to the AML/CTF role over the commercial one. Our observations echo Zuboff's (2015) analysis of the phenomenon of surveillance capitalism, where the accumulation of data results in the creation of asymmetries in terms of knowledge and power. Zuboff (2015) suggests this asymmetry is manifested between the owners of a data driven service (e.g., Google) and the service users. In our analysis, such asymmetry is also manifested between different parts of the same organization.

At the inter-organizational level, the tension was felt in the competing demands on time and other resources resulting from the power struggle between institutionalised corporate and state interests. The AML/CTF information flows placed these firms in double jeopardy. On the one hand, meeting the AML/CTF requirements goes against the fiduciary duty of financial services organizations towards their customers (Canhoto, 2008), and could limit their ability to meet day-to-day business goals. On the other, a failure to meet AML/CTF compliance requirements could potentially damage the commercial survival of the firms, as well as national security interests (Huysmans, 2014).

5.2 Key contributions of the study

Several theoretical and practical contributions emerge from the findings. Our first contribution is largely theoretical and concerns the utility of remediation theory as an analytical lens to provide deeper evidence about how AML/CTF reconfigures the different elements within the organization. Remediation theory (Bolter and Grusin, 2000) highlights that social, political and material reconfigurations occur when information is gathered and transformed into new digitally mobile forms. Our findings also show that the AML/CTF requirements created new roles and expertise, demanded new skills and work practices,

required new investment, and instilled new ways of viewing the financial organization's role and profit in society. Remediation is at the heart of AML/CTF because of its imperative to gather and electronically transfer evidence of wrongdoing among customers' transaction records. By analytically identifying three different remediation points – at the front line, in the interactions with the financial crime department and through the relationship with external shareholders and entities – the findings reveal how organizational elements were reconfigured to accommodate AML/CTF requirements.

We demonstrate how multiple data points were combined to produce evidence of suspicious activity. Front line staff used information from credit scoring information systems, customer management systems, their knowledge of the regulations and their instincts about customer behavior, to inform their assessments. This process began reconfiguring staff's tacit knowledge, customer handling skills, the task and its performance management. The financial crime department used reports from the front line but also generated insight using TMS searches, the CRM system and tacit knowledge about customer lifestyles and normal account use. Organizational communication patterns unique to AML/CTF processes emerged, with new organizational boundaries based on the specialist expertise and interests of the financial crime department. As the organization's MLROs submitted SARs to the NCA, strategic level actors questioned the regulation's effect on tangible and intangible assets. Space limitations prevented an in-depth analysis of the organizational meaning systems surrounding these activities. However, the data identified struggles for organizational legitimacy by the financial crime departments and front line staff being made responsible for crime prevention. Employees worked hard to formulate their reasoning for suspicion to render it 'reportable' in AML/CTF systems, using available data and their customer experience to tease that out.

The paper's second contribution concerns the use of information flow as a unit of analysis. Taking this conceptual stance had methodological consequences for how the

research was conducted, which resulted in a range of practical insights being generated. In order to understand how an organization can act as an intermediary in a national security regime, we adopted Neu et al.'s 2013 approach, and focused on what and how information was exchanged between the various parties. Information about suspicious activities connected the banks and the NCA, as the data flowed from the customer to the government via the financial organization. However, tracing this passage through the organization demonstrates that information has different viscosities, so that it does not flow automatically and freely. The extent to which information about suspicious activities flowed depended on factors that included the vigilance and decisions of human beings, available resources, the weight of existing evidence about a particular case, information to hand, tacit knowledge, system search parameters, labor, time and expediency. At times, these factors were in conflict with each other. The findings further show that information did not flow both up and down the organization. Front line staff identified an almost Kafkaesque upward information flow created by the law of 'tipping off'. Although these staff perceived that they needed feedback on the quality of their reporting, none was forthcoming. We believe this unit of analysis is useful for understanding how staff manage the multiple requirements on their labor and expertise, given such limited feedback. A similar approach could be useful for future studies of private sector involvement in national data exchange programs where organizations are intermediaries between the general public and the government.

Our final contribution, which concerns the multi-level nature of the study, is both conceptual and methodological. By examining three remediation points, a reconfiguration of organizational elements at three different analytical levels was revealed (see Table 3 below), resulting in some rich practical insights. In organization theory terms, multi-level effects were observed. For the organization theorist, there are conceptual issues with the parallel treatment of different levels of analysis within one analytical piece. The fact that the organization

requires consideration as a whole problem space, as well as a set of interlinked parts, may help explain why organization theorists have been silent on the use of the private sector in national security arrangements: As Lopes Costa (2009, p. 4) comments, due to diverse disciplinary backgrounds "organizational researchers are likely to highlight either a micro- or a macro- perspective. What is, perhaps, lacking is the operationalization of that multilevel thinking in more research that actually converts an encompassing vision of organizations in empirical studies".

One of the ideas we drew upon was a 'set logic' to define the relationship between different organizational levels of analysis that occurred simultaneously in one study (Lacey and Fiss, 2009). This approach is in different to a 'nested' logic, in which each level would be embedded within the other, making a complete picture difficult to describe. Table 3 shows the multi-level effects which result from information flow as part of the AML/CTF 'set' of phenomena.

Level	**Organizational element reconfigured**
Individual and Task:	Changes in tacit knowledge of front line employees about suspicious behavior. Changes in customer handling skills of front line employees. Changes in the content of sales work to include compliance. Changes in the performance management of sales work.
Intra organizational:	Emergence of chains of secrecy in organizational communication patterns. Changes to internal organizational boundaries as financial crime

	departments reinforce their expertise.
Organizational and Inter-organizational:	Recognised pressure on organizational resource distribution towards regulatory compliance. Changes to ability of organizations to compete on a level playing field because of investments required in AML/CTF. Perceived centrality of AML/CTF to corporate reputation.

Table 3: Multi-level effects of the AML/CTF data exchange program

5.3 Reshaping organizational elements at multiple levels by new information flows

Within each level of analysis, one or more organizational elements is transformed by AML/CTF information flows. Some of these elements inter-relate and influence one another. For instance, the (KYC) requirements led to changes in the customer data routinely captured when opening an account, and instigated a heightened contextual awareness among staff, as highlighted in our findings and summarised in Table 2. This observation echoes the findings from research examining the impact of e-Borders regulation on the travel sector, where the need to monitor travellers shaped how customers were dealt with, marketing related activities or even the user interface of booking systems (Dibb et al., 2014).

Changes in knowledge and skillsets necessarily altered the shape and nature of tasks, which needed in turn, to be performance managed. The establishment of a dedicated financial crime department redrew internal boundaries and communication patterns. Patterns of reporting SARs to the NCA caused senior managers to reflect on how resources were distributed, the competitive playing field and corporate reputation.

Poor performance in AML/CTF potentially undermined corporate reputation, which affected the firm's ability to compete in the marketplace. Similarly, optimum resource distribution between commercial and regulatory activities was also a challenge. As

information regarding suspicious transactions was generated for every transaction and sometimes acted upon, these processes were in a constant state of flux. Simultaneously, skills and knowledge became honed, roles became shaped, internal boundaries became redrawn, resources were distributed in new ways and reputations were made or destroyed by virtue of AML/CTF. In the next section, we identify some of the opportunities for future research to extend such insights.

6.0 Conclusion

A panoply of newly enacted laws in the UK and worldwide positions the private sector as a data source for national security, imbuing these organizations with the surveillance powers of the sovereign state. This activity reflects governments' attempts to tap into the big data capabilities of corporations (e.g. Amankwah-Amoah, 2016; LaBrie et al., 2018; Jun et al., 2018) and is part of the ever-growing surveillance economy (Zuboff, 2015). An organizational treatment of the phenomenon of mandatory data exchanges between private and public organizations has been long overdue. Business disciplines have strong contributions to make to debates about the operationalisation of national security.

Our study has highlighted how strategy, systems, the customer relationship and employees are impacted. Many of the observed phenomena occurred because they are mandated by this regulation. Reporting suspicions, not tipping off, investigating unusual transactions, responding to watch lists and submitting SARS, are all examples of regulatory compliance in action. However, our data show that skill, effort, resources and intangible assets are deployed; and organizational processes are reshaped to create and maintain an information flow to government. This is the political economy of involving the private sector in actioning public programs, with destabilisation and change from dealing with mandatory security regulations, shown to impact core organizational elements in multiple ways. We also

reveal the potential for different business disciplines to study these areas in more detail. Critical accounting, marketing, strategy, policy studies academics, consumer behavior experts, employee relations academics and organization theorists could each use this analysis to develop a research agenda based on their own unique perspectives.

Our first contribution concerns the utility of remediation theory in exploring the information flows in the financial services sector. We show that the mandatory data capture and exchange activities reconfigure existing organizational arrangements at multiple analytical levels, creating tensions between the commercial and compliance roles of financial services firms. Specifically, we find tensions in terms of commercial priorities, customer relationships and working patterns. Future research is required to gain a deeper understanding of the tensions - such as around the reshaping of roles and work practices - that emerge in these circumstances, and how they can best be addressed.

Our second contribution relates to the information flow as a unit of analysis. In an era when personal data is increasingly at the heart of national security policy and the private sector is required to share and to process such data, further research is needed to explore how such information flows can best be studied. The contributions of such research to future policy and practice also warrants further attention.

Our third contribution arises from the multi-level nature of the study and the potential insights from adopting a ‘set logic’ at three levels: individual/task, intra-organizational and organizational/ inter-organizational. Future research could use perspectives from any one of these levels of analysis and explore, for example, the intersection between AML/CTF and commercial priorities through a single analytical lens. In turn, this would result in a deeper understanding of the tensions between different priorities and influencing processes at that level.

Our study has practical implications for the stakeholders involved, at all three levels

of analysis. At the individual/task level, we suggest that organizations put training in place to specifically guide front line staff to help them navigate the new tensions they face. This training could develop staff to balance the conflicts they face in making judgements about the legality of financial transaction behaviours, while protecting the organization's customer service ethos and commercial priorities. The role that incentives play in reinforcing or ameliorating these tensions should also be considered. For instance, a bonus system that puts too much emphasis on customer acquisition or sales may undermine efforts to avoid exposing the organization to risky customers. Similarly, an overemphasis on speed of processing may limit the ability to collect additional customer or transaction information, which could result in staff under or over reporting suspicion (Eisenhardt, 1989).

At the intra-organizational level, we note that firms encountering these requirements for the first time might consider models adopted by other organizations to manage these tensions, such as setting up a separate financial crime department or carefully considering the changes in expertise, skills and communication patterns needed in other areas of the business. At the organizational/inter-organizational level, organizations may need to respond to these new tensions by re-evaluating the appropriate level of resource allocation to regulatory compliance. Regulation and AML/CTF also need to be fully considered when managing external reputation, to minimize risks to the corporate brand and image.

To overcome the tensions arising from AML/CTF, the UK regulator could consider adopting features of AML/CTF systems from other jurisdictions. In Italy, financial services providers are required only to collect the data, which is then transferred to the central financial intelligence unit for analysis and action. Consequently, the onus of detection and the conflicts associated with it, are removed from the financial services organizations. Such a system was previously adopted by the UK government in the travel industry. In the now abandoned e-Borders programme, travel operators had to collect and electronically transmit

passenger data to the UK Border Agency, which was then responsible for flagging suspicious behaviour. While this centralised intelligence model would overcome some of the issues discussed in this paper, it would suffer from several disadvantages. First, a costly, secure infrastructure would be needed to transmit highly personal and sensitive data, which could create a point of vulnerability for cyber-attacks. Second, such a system would require organizations to adopt standard data collection and transfer formats. As has been shown in the travel sector (Ball, Spiller, Canhoto, Daniel, Dibb and Meadows, 2014), due to the variety of legacy systems in place, this would be highly technically complex and financial burdensome to organizations. Third, at a time of heightened sensitivities concerning surveillance and privacy, such a move would probably prove highly unpopular with the UK population.

As the travel sector example indicates, although our study was concerned with the financial services organizations, similar conflicts may be witnessed in other sectors. For instance, the hospitality industry is expected to be alert to people trafficking; social network providers are expected to contain the spreading of extremist content and attempts at radicalisation; higher education institutions are penalized if they are deemed to not do enough to stop visa fraud, and they also need to monitor and report on students that are at risk of being radicalised; and private firms with CCTV systems (e.g. banks and hotels) are required to share images from private security systems with law enforcement to assist with criminal investigations.

While our research concerned the data and information flow from private to public organisations, it is also possible for information to flow in the other direction. For instance, several NHS trusts in the UK have shared patient data with Deep Mind, an organisation that is part of the Alphabet Inc. (which also owns Google), in order to train Deep Mind's machine learning algorithms. It has also been suggested that the law enforcement agencies fighting

child sexual exploitation could make their cache of images available to YouTube and Facebook, to help them develop algorithms to detect the presence of such content in their networks. While the tensions identified in our research may apply to this type of information flow, new ones may also arise. Further research is needed regarding the specific organizational elements included in such public-private information flow sets, as well as the associated organizational tensions.

Turning to the limitations of our study, we note that our data are drawn from two case studies, in a single industry sector in the UK. While the financial services sector is an important research site, we hope that our insights may inspire others to investigate the experiences of firms in other sectors of industry, such as information and communication services providers. These organizations will likely increasingly be subject to mass surveillance legislation, with many already engaged in a struggle with governmental surveillance agencies over access to their customers' data.

7.0 References

Amankwah-Amoah, J. (2016). Emerging economies, emerging challenges: Mobilising and capturing value from big data, *Technological Forecasting and Social Change*, 110, 167–174.

Amicelle, A. and Favarel-Garrigues, G. (2012). Financial surveillance: Who cares? *Journal of Cultural Economy*, 5(1), 105–124.

Amicelle, A. (2011). Towards a 'new' political economy of financial surveillance. *Security Dialogue*, 42(2), 161–178.

Arnold, M. (2018). *HSBC brings in AI to help spot money laundering*. Financial Times. London. Retrieved 28 April, 2019 from https://www.ft.com/content/b9d7daa6-3983-11e8-8b98-2f31af407cc8

Backhouse, J., Demetis, D., Dye, R., Canhoto, A. and Nardo, M. (2005). *Spotlight: New approaches to fighting money-laundering* (4 volumes); AGIS programme JAI/2004/AGIS/182.

Balani, H. (2019). Assessing the introduction of Anti-Money Laundering regulations on bank stock valuation: an empirical analysis. *Journal of Money Laundering Control*, 22(1), 76–88 DOI: 10.1108/JMLC-03-2018-0021

Ball, K. and Snider, L. (eds.) (2013). *The surveillance-Industrial Complex: Towards a Political Economy of Surveillance*. London: Routledge.

Ball, K., Spiller, K., Canhoto, A., Daniel, E., Dibb, S. and Meadows, M.. (2014). Living on the edge: Re-medial work in the UK travel sector", *Journal of Work, Employment and Society*, 28(2), 305–322.

Ball, K., Canhoto, A.I., Daniel, E., Dibb, S., Meadows, M. and Spiller, K. (2015). *The Private Security State? Surveillance, Consumer Data and the War on Terror*. Copenhagen, Copenhagen Business School Press. ISBN: 8763003325.

Bebbington, J., Kirk, E.A. and Larrinaga, C. (2012). The production of normativity: A comparison of reporting regimes in Spain and the UK *Accounting, Organizations and Society,* 37, 78–94

Bergström, M., Helgesson, K., Svedberg, K. and Mörth, U. (2011). A new role for for-profit actors? The case of anti-money laundering and risk management. *Journal of Common Market Studies,* 49(5) 1043–1064

Bolter, J. and Grusin, R. (2000). *Remediation: Understanding New Media*. Cambridge, MA: MIT Press.

Bowker, G.C. and Star, S.L. (1999). *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press.

Byrne, E. (2011). Business Ethics Should Study Illicit Businesses: To Advance Respect for Human Rights. *Journal of Business Ethics*, 103(4), 497-509. DOI: 10.1007/s10551-011-0885-y.

Canhoto, A. (2008). Barriers to segmentation implementation in money laundering detection. *Marketing Review* 8(2), 163–181.

Canhoto, A., Meadows, M., Ball, K., Daniel, E.M., Dibb, S. and Spiller, K. (2017) 'The role of customer management capabilities in public-private partnerships', *Journal of Strategic Marketing*, 25(5/6), 384-404.

Chen, G., Mathieu, J.E. and Bliese, P.D. (2004). A framework for conducting multilevel construct validation. In F.J. Dansereau, and Yammarino, F (eds.), *Research in Multi-Level Issues: The Many Faces of Multi-Level Issues* (pp. 273-303). Oxford, UK: Elsevier Science.

Compin, F. (2008). The role of accounting in money laundering and money dirtying, *Critical Perspectives on Accounting*, 19(5), 591–602.

Davis, J.S. and Pesch, H.L. (2012). Fraud dynamics and controls in organizations.

Accounting, Organizations and Society 38, 469–483.

de Goede, M. (2012). *Speculative Security: The Politics of Pursuing Terrorist Monies.* Minneapolis, MN, University of Minnesota Press.

DeRosa, M. (2004). *Data Mining and Data Analysis for Counterterrorism*. Washington DC, Center for Strategic and International Studies.

Dey, B.L., Babu, M.M., Rahman, M., Dora, M. and Mishra, N. (2019). Technology upgrading through co-creation of value in developing societies: Analysis of the mobile telephone industry in Bangladesh, *Technological Forecasting and Social Change*, 145, 413-425.

Dibb, S., Ball, K., Canhoto, A., Daniel, E.M., Meadows, M. and Spiller, K. (2014). Taking responsibility for border security: commercial interests in the face of e-Borders, *Tourism Management*, 42(1), 50–61.

Donaghy, M. (2002). Monetary privacy in the information economy. *International Sociology*, 17(1), 113–133.

Eisenhardt, M. (1989). Agency theory: An assessment and review. *Academy of Management Review 14*(1), 57–74.

Ericson, R. and Doyle, A. (2004). *Uncertain Business: Insurance and the Limits of Knowledge*. Toronto: University of Toronto Press.

FATF. (2018). *Financial Flows from Human Trafficking*. Paris, Financial Action Task Force: 71. Retrieved 28 April, 2019 from https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.

FATF. (2019). *History of the FATF*. Financial Action Task Force. Retrieved 26 April, 2019, from https://www.fatf-gafi.org/about/historyofthefatf/#d.en.3157.

Gabbioneta, C., Greenwood, R., Mazzola, P. and Minoga, M. (2013). The influence of the institutional context on corporate illegality. *Accounting, Organizations and Society*,

38, 484–504.

Gill, M. and Taylor, G. (2003). Can information technology help in the search for money laundering? The view of financial companies. *Crime Prevention and Community Safety*, 5(1), 39–47.

Godfrey, R., Brewis, J., Grady, J. and Grocott, C. (2014). The private military industry and neoliberal imperialism: Mapping the terrain. *Organization*, 21(1), 106–125.

Grint, R., O'Driscoll, C. and Paton, S. (2017). *New technologies and anti-money laundering compliance*. London, Financial Conduct Authority, 54.

Huysmans, J. (2014). *Security Unbound: Enacting Democractic Limits.* London: Routledge.

JMLSG, (2006). Joint Money Laundering Steering Group: *Prevention of Money Laundering/ Combatting Terrorist Financing*. http://www.jmlsg.org.uk/industry-guidance/article/guidance, accessed 5th June 2019.

Jun, S., Yoo, H.S. and Choi, S. (2018). Ten years of research change using Google Trends: From the perspective of big data utilizations and applications, *Technological Forecasting and Social Change*, 130(C), 69–87.

Kaminski, P. and Schonert, J. (2018). *Monitoring Money-Laundering Risk with Machine Learning*. McKinsey Quarterly. New York, McKinsey & Company, Inc: 2.

Kuljis, J., Macredie, R. D., and Paul, R. J. (1998). Information gathering problems in multinational banking. *Journal of Strategic Information Systems*, 7(3), 233-245.

LaBrie, R.C., Steinke, G.H., Li, X. and Cazier, J.A. (2018). Big data analytics sentiment: US-China reaction to data collection by business and government, *Technological Forecasting and Social Change*, 130, 45-55.

Lacey, R. and Fiss, P.C. (2009). Comparative organizational analysis across multiple levels: A set theoretic approach. In King, B, Felin, T and Whetten, D. (eds) *Research in the Sociology of Organizations: Comparative Approaches to Organizational Research.*

Elsevier, New York, NY. pp 91–116.

Lepoutre, J. and Oguntoye, A. (2018). The (non-)emergence of mobile money systems in Sub-Saharan Africa: A comparative multilevel perspective of Kenya and Nigeria, *Technological Forecasting and Social Change*, 131, 262–275.

Levi, M. and Gilmore, B. (2002). Terrorist finance, money laundering and the rise and rise of mutual evaluation: a new paradigm for crime control? *European Journal of Law Reform*, 4, 337–364.

Loader, I. and Walker, N. (2010). *Civilising Security.* Cambridge: Cambridge University Press.

Longfellow, T. (2006). Compliance tips regarding anti-money laundering. *Journal of Financial Planning*, Sep. 2006, Supplement, 15.

Lopes Costa, P., Graça, A.M., Marques-Quinteiro, P., Santos, C.M., Caetano, A. and Passos, A.M. (2013). Multilevel research in the field of organizational behavior: An empirical look at 10 years of theory and research, *SAGE Open*, July-September 2013: 1–17.

Meifang, Y., He, D., Xianrong, Z. and Xiaobo, X. (2018). Impact of payment technology innovations on the traditional financial industry: A focus on China, *Technological Forecasting and Social Change*, 135, 199–207.

Miles, M. B. and Huberman, A.M. (1994). *Qualitative Data Analysis.* Thousand Oaks, CA, Sage.

Mitchell, A., Sikka, P. and Willmott, H. (1998). Sweeping It under The Carpet: The Role of Accountancy Firms in Money laundering, *Accounting, Organizations and Society*, 23(5/6), 589–608.

Morales, J., Gendron, Y., Guénin-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., Everett, J., Rahaman, A.S., Martinez, D. (2013). Accounting and networks of corruption *Accounting, Organizations and Society* 38 505–524.

Pok, W.C., Omar, N. and Sathye, M. (2014). An evaluation of the effectiveness of anti-money laundering and anti-terrorism financing legislation: Perceptions of bank compliance officers in Malaysia. *Australian Accounting Review*, 24, 394–401.

Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society* 38, 525–543.

Ryder, N. (2008). The financial services authority and money laundering. *The Cambridge Law Journal*, 67(3), 635–653.

Sathye, M. and Islam, J. (2011). Adopting a risk-based approach to AMLCTF compliance: the Australian case, *Journal of Financial Crime*, 18(2), 169–182.

Shadnam, M. and Lawrence, T.B. (2011). Understanding widespread corruption in organizations: An institutional theory of moral collapse. *Business Ethics Quarterly*, 21(3), 379–407.

Sica, V. (2000). Cleaning the laundry: States and the monitoring of the financial system. *Millennium-Journal of International Studies*, 29(1), 47–72.

Strauss, A. and Corbin, J. (1990). *Basics of Qualitative Research*. Sage: Newbury Park, California.

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review*. 33(3), 341–353.

Whisker, J. and Lokanan, M.E. (2019). Anti-money laundering and counter-terrorist financing threats posed by mobile money. *Journal of Money Laundering Control*,

22(1), 158–172.

Williams, J.W. (2013). Regulatory technologies, risky subjects, and financial boundaries: Governing ‘fraud’ in the financial markets *Accounting, Organizations and Society,* 38, 544–558.

Zdanowicz, J. S. (2004). Detecting money laundering and terrorist financing via data mining. *Communications of the AC,* 47(5), 53–55.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30: 75-89.