**ORIGINAL PAPER**

# A Micro-ethnographic Study of Big Data-Based Innovation in the Financial Services Sector: Governance, Ethics and Organisational Practices

Keren Naa Abeka Arthur[1] · Richard Owen[2]

## Abstract

Our study considers the governance, ethics and operational challenges associated with the acquisition, manipulation and commodification of 'big data' in the financial services sector. To the best of our knowledge, there are no published studies describing empirical research undertaken within companies in this sector to understand how they are responding to such challenges: our field-based research is a significant initial contribution in this respect. We describe the results of a micro-ethnographic study undertaken in a small-to-medium-sized company developing disruptive, technology-related platforms and services in the banking and retail sectors based on big data and associated analytics: these are used to derive commercially valuable insights from personal customer data in exchange for cash back and targeted rewards. The company was found to employ a multi-level innovation governance approach, underpinned by an ethical strategy based on a principle of mutual benefit (among stakeholders). Opt-in and informed consent for using data for specific purposes was supported by principles of data minimisation and anonymisation, with unrestricted use of secondary, anonymised and aggregated data to develop insights. Governance, which included contextual data protection legislation, payment-card industry data usage standards and internal corporate controls, presented as bespoke organisational practices relating to data security and privacy. These in total set the governance and ethics frame for big data innovation at the company within which it has had to be both adaptive and responsive under conditions of normative and regulatory uncertainty.

**Keywords** Financial innovation · Big data · Governance · Ethics · Organisational practices

## Introduction

Innovations in 'big data' analytics and the emergence of the 'big data industry' and secondary data market (Martin 2015) have been accompanied by increasing discussion (and concerns) regarding privacy, data security, trust and the need for effective governance (Bollier 2010; Fulgoni 2013; Floridi and Taddeo 2016; Herschel and Miori 2017; Manyika et al. 2011; Nunan and Domenico 2017; Sunil 2012).

These include issues relating to risk, e.g. that collection, analysis and valorisation of big data rests on tightly coupled and inter-dependent systems characterised by dynamic complexity in which 'normal accidents' will inevitably occur (Nunan and Domenico 2017). The discussions also have ethical dimensions (Richards and King 2014) as these relate to data, algorithms and practices (Floridi and Taddeo 2016), with cross-cutting issues relating to personal/group privacy and categorisation, widespread 'surveillance as pollution' (Martin 2015), bias, discrimination and learned prejudice, consent, identity, data ownership and transparency (Ibid; RSS 2015). Big data could be used to target and manipulate people (and exploit their vulnerabilities) to consume or behave in certain ways (Herschel and Miori 2017), with the potential to impact identity. There are also questions relating to moral judgement and accountability in decision making, particularly when big data analytics are linked to machine learning (RSS 2015; Floridi and Taddeo 2016).

✉ Richard Owen
  richard.owen@bristol.ac.uk

  Keren Naa Abeka Arthur
  keren.arthur@ucc.edu.gh

1 Centre for Entrepreneurship and Small Enterprise Development, University of Cape Coast, Cape Coast, Ghana

2 School of Management, University of Bristol, Priory Road Complex, Priory Road, Bristol BS8 1TU, UK

A particular ethical concern relates to privacy. Firms may, for example, inadvertently be privy to information they never intended to collect (Herschel and Miori 2017). Or they may be able to (re)-identify individuals or groups, intentionally or unintentionally, by data mining, linking, merging and re-using datasets, datasets which individually may not have been considered as having privacy implications (Floridi and Taddeo 2016; Nunan and Domenico 2013). Data could also 'be collected regardless of, and potentially without knowledge of, the purpose for which it is to be finally used' (Nunan and Domenico 2017). But even in those cases where motivation and purpose are clearer, *how* technology companies gain informed consent for the use and manipulation of personal data for commercial purposes remains problematic. Flick (2013, 2016), for example, argues that such companies often use 'disclosure and consent' mechanisms such as (sometimes long and impenetrable) end-user licence agreements or terms of service which the consenter must read and agree to. However, she argues that technologies remove face-to-face contact and dilute the ability of technology companies to determine the competence and level of understanding of those from whom consent is sought. This raises significant questions as to whether effective consent is truly 'informed', a situation she argues that is exacerbated when using big data.

Such issues potentially affect a wide number of sectors, including financial services, where innovation in big data manipulation and application is accelerating rapidly as companies realise the competitive advantage this can bring (Manyika et al. 2011). Despite this, we are not aware of any empirical research undertaken within companies involved (directly or indirectly) in the financial services sector to understand how they are addressing the governance and ethics dimensions associated with innovation based on big data, or how values such as privacy are perceived and managed (Turner et al. 2012). Likewise, there is little understanding of how ethical values are being internalised within companies and the factors influencing these (e.g. whether these are driven by external regulatory pressures, their own commitment to an ethical and responsible innovation approach or a combination of both). In order to investigate these, we undertook an exploratory, ethnographic study within a rapidly expanding, small-to-medium-sized company developing disruptive, technology-related platforms and services that support big data retrieval, analytics and development of commercially valuable insights in the banking and retail sectors. The paper is laid out as follows: we first briefly review literature on big data analytics and its governance in financial services. We then describe innovation within the company over its history and how it has seized the emerging opportunities presented by big data. Finally, we go on to describe and discuss the innovation process and its governance within the company in detail, how issues of data privacy and security are handled and how responsible and ethical behaviour is perceived by employees.

## Defining Big Data

A number of authors (e.g., Krishnan 2013; Laney 2001; Madden 2012; Manovich 2012; Russom 2011; Schroeck et al. 2012; Sunil 2012) define big data around three key dimensions of data *variety*, *volume* and *velocity,* i.e.it constitutes data of different formats (variety)—both structured (clearly defined and organised data types) and unstructured—that challenges or exceeds an organisation's storage and processing capacity because it is so large [comprising terabyte and petabytes of information (volume)], and which must be processed quickly (usually in milliseconds) for effective real-time decision making (velocity). Some have argued that this definition ignores other important dimensions such as the capacity to provide value for organisations (Bhasin et al. 2012; Boyd and Crawford 2012; Nunan and Domenico 2013; Sunil 2012) as well as dimensions of complexity, (un)reliability and uncertainty (Schroeck et al. 2012).Therefore, this definition has more recently been extended to include a fourth V—veracity—which focuses on issues such as data quality (Hitzler and Janowicz 2013; Normandeau 2013). These emphasise the notion of "data as a resource" (Kambatla et al. 2014) that can confer competitive advantage to organisations (Brown et al. 2012; Brynjolfsson et al. 2011; Bughin et al. 2010; LaValle et al. 2011).

The challenge of effective manipulation of big data by businesses to derive value often necessitates the use of technologies that automate decision-making processes in a continuous and autonomous manner (Yulinsky 2012). Using processes of search and analysis to identify useful information (i.e. "data mining"), organisations are able to convert data into something of value (Fayyad et al. 1996; Frawley et al. 1992; Gantz and Reinsel 2011; Linoff and Berry 2011). This is often done using a mix of cost-effective data collection, extraction and analysis tools and technology solutions referred collectively to as *analytics* (Chaudhuri et al. 2011; Chen et al. 2012; Russom 2011; Turban et al. 2008; Watson and Wixom 2007). In combination, these technologies support real-time data retrieval, analysis and fast-paced decision making.

## Big Data Innovation in Financial Services

Big data is a concept that extends across many sectors, including finance and insurance. These sectors, it is argued, are well positioned to benefit once barriers (e.g. lack of IT concentration and lack of a data-driven mind-set) are removed (Manyika et al. 2011) due to the availability of

high quantities (petabytes) of data, analytical talent existing in financial institutions and the opportunities presented by the transactional and customer-centric nature of the sectors. By using big data to, for example, identify complex patterns of fraud (Economist 2012), assess and support approval of loans (Sauer 2013), manage efficiency and risk (Bhasin et al. 2012; Sauer 2013) and support trading analytics in capital markets (e.g. high-frequency trading, pre-trade decision support) (Verma and Mani 2012), financial institutions have great potential to leverage big data to their advantage (Turner et al. 2012), particularly the use of unstructured data in the social and geospatial domain. The relatively cautious approach taken to date in part reflects concerns around trust, identity, privacy and security associated with the adoption and use of new technologies in hyper-connected environments that allow acquisition and manipulation of big data, such as cloud computing (Mcgarvey 2012a).

Research across the financial (Coumaros et al. 2014; IBM 2011, 2012; Ngai et al. 2009; Schroeck et al. 2012; Turner et al. 2012) and retail sectors (e.g. Worthington and Fear (2009)) suggests that one of the primary areas for innovation using big data to date has been in the area of customer relationship management (CRM) (Ahn et al. 2003; Blattberg and Deighton 1996; Brassington and Pettitt 2006; Chaffey 2007; Peppard 2000). Within CRM, others have highlighted a further narrowing of big data initiatives to marketing (Peppard 2000) and loyalty programmes (Ngai et al. 2009). These initiatives primarily involve the use of data analytics for customer profiling and segmentation, trend analysis and predictive modelling so as to improve the customer experience through personalised product and service offerings, to identify prospective customers and to analyse the success or failure of marketing programmes (Hildebrandt 2006; Rygielski et al. 2002; Sauer 2013; Shaw et al. 2001). In the retail sector, where supermarket loyalty programmes have proliferated significantly, such data have also been used for evaluating in-store advertising, pricing new product line development and evaluating supplier activity (Worthington and Fear 2009).

The global proliferation of merchant-funded reward programmes is a good example of big data initiatives geared towards CRM in financial services (Bareisis 2012; Caltabiano and Ferguson 2009; Rowley 2004, 2005; Yadav 2012). Managed by an in-house or third-party platform vendor (Bareisis 2012; Bruene 2014), such programmes allow merchants in various shopping categories to come together in a coalition to provide personalised offers, including rebates, cash back and discounts to a sponsor's (e.g. a bank or other financial institution's) loyalty programme member (Caltabiano and Ferguson 2009; Yadav 2012).

Loyalty programme members benefit from rewards in exchange for consent for businesses to use their personal (e.g. transaction) data, e.g. to develop commercially valuable insights for merchants. Sponsors (e.g. banks) concurrently enjoy increased engagement with their customers at decreased cost, since merchants pay for the privilege of gaining access to new channels for customer acquisition and revenue lifts (Caltabiano and Ferguson 2009; Rowley 2004, 2005). Third-party platform providers also profit from fees paid by sponsors, merchants or both for their services (Bareisis 2012; JSR 2011). Accordingly, as Russom (2011) has argued, big data in various sectors, including financial services, has evolved from being a by-product to a source of significant business opportunity.

## Governance and Ethical Dimensions of Big Data Analytics in Financial Services

While there is a considerable literature on ethical finance, and a growing body of academic work relating to concepts of ethical and responsible innovation (e.g. Baucus et al. 2008; Fassin 2000; Meel and Saat 2002; Schumacher and Wasieleski 2013; Stilgoe et al. 2013), there has to date been only limited study of ethical and responsible *financial* innovation (e.g. Armstrong et al. 2012; Asante et al. 2014; Muniesa and Lenglet 2013; OCC 2016), most of which is theoretical in nature. We are unaware of any studies investigating the governance and ethics dimensions of innovation based on big data in financial services.

More generally, big data governance incorporates policies, processes and institutions aimed at governing and managing data acquisition, usage/manipulation and storage across the entire lifecycle (Sunil 2012; Tallon 2013). Both statutory and self-regulatory approaches to governance are evident (Bollier 2010; Sunil 2012; Celma et al. 2014).While statutory regulation (e.g. country specific Data Protection Acts) is often loosely defined around data usage (Bollier 2010), including aspects of privacy, self-regulation is often concerned with how data are organised and managed (Cheng et al. 2013; Loshin 2013; Sunil 2012; Tallon 2013) including data security considerations.

Governments often monitor and enforce statutory regulation through instruments such as periodic audits, assessments and prosecutions (Celma et al. 2014; Chaudhary et al. 2013). Bollier (2010) has suggested that there is in general a preference by industry participants and policy makers for non-regulatory approaches that involve streamlined financial reporting, transparency and open source analytics. Such self-regulation is enacted primarily in corporate institutions via data governance, business intelligence or information technology teams/departments, supported by standards and certification (Russom 2011; Venkatasubramanian 2012). These standards have evolved significantly in the last two decades to become a policy-driven activity (Chen et al.

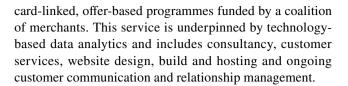2012; Krishnan 2013) that stresses the need for comprehensive oversight (Loshin 2013) and data stewardship.

Issues such as data organisation and quality, metadata compilation, data integration with business processes and master data (Sunil 2012), information life cycle management, data privacy and security (Bollier 2010; Manyika et al. 2011; Nunan and Domenico 2013; Sunil 2012) have all come to the fore as industry experts have attempted to consolidate best practices aimed at enabling organisations to consistently maximise data value within the financial sector (Bollier 2010; Chaudhary et al. 2013; Dias 2013; Sunil 2012). These statutory and self-regulatory frameworks are supported by de facto governance based on the principle of market choice (Boyd and Crawford 2012) as consumers engage more with the decision-making process of whether to share their data or not (Rose et al. 2013). Rose et al. report that while financial data (e.g. credit card information) are considered the most sensitive, individuals are willing to share this if they can trust an organisation to provide good data stewardship.

In general, the governance and ethical dimensions of big data in financial services are as yet little explored. We know very little about the nature and process of innovation in the big data and business analytics space and how this is governed within and beyond companies in the financial sector, and how ethical aspects such as privacy, access and consent are handled (Boyd and Crawford 2012). There is in particular little empirical understanding as to how new business models, products and processes (Manyika et al. 2011; Mcgarvey 2012b; Sauer 2013) based on big data analytics emerge within organisations in the financial sector and how these are governed across the lifecycle, from ideation to commercialisation and diffusion (Asante et al. 2014). In order to address these questions, we undertook empirical ethnographic research within a company innovating disruptive, technology-related platforms and services supporting CRM-related business analytics in the banking and retail sectors.

## Research Methodology

### Case Study Description

Our research was undertaken in a small-to-medium-sized company (hereafter 'the company') which originally created loyalty cards and managed loyalty programmes for sports clubs in exchange for a success-based service fee. Over the last decade it has grown rapidly and undergone significant repositioning, now mainly providing services for banks, owners of large databases (publishers) and merchants. The company currently operates as a professional service agency, primarily involved in the provision of end-to-end,

card-linked, offer-based programmes funded by a coalition of merchants. This service is underpinned by technology-based data analytics and includes consultancy, customer services, website design, build and hosting and ongoing customer communication and relationship management.

## Data Collection and Analysis Methods

We adopted a 'compressed time' mode of ethnography (Jeffrey and Troman 2004; Asante et al. 2014) conducted over an intense period of 3 weeks, with the researcher immersed each day in the company as a quasi-temporary employee, and with subsequent follow-up work over a period of 6 months. Working from a designated desk in the office, data were collected using ethnographic methods of in situ observations (employee routines and activities, including meetings), complemented by fifteen in-depth, semi-structured interviews each of approximately 45 min duration with managers and associates across the company (and including one external auditor), a review of internal documents provided by the company (such as organisational structure charts and diagrams relating to the process and governance of innovation in the organisation) and a workshop with staff to explore ethical and governance dimensions of innovation within the company (Brannan et al. 2012; Eberle and Maeder 2010; Neyland 2007; Thomas 2003; Watson 2012). We employed a narrative analysis approach aimed at describing how big data-based innovations have emerged, how these are governed, how ethical values such as data privacy are addressed and how ethical and responsible behaviour are perceived by employees (Riessman 2002, 2008; Richardson 1995). This was done by documenting and organising collected data into concepts in order to identify patterns and connections and present an accurate account of the innovation and associated governance processes within the company (Schutt 2012).

## Results

The company has developed a number of innovations over its history which, when viewed from a chronological perspective, provide a rich picture of how it has both embraced the emerging opportunities presented by big data, and how it has attempted to respond to the associated challenges of ethics and governance from an organisational perspective.

One of the most significant earlier innovations was a technology platform that allowed transactions at participating retailers to be tracked for the automatic provision of rewards. Developed by the company over a period of approximately 18 months, it links customers via their debit/credit card transactions to offers, without the need for physical coupons. This unique capability became the foundation of the company's service offering and helped unlock key relationships

with tier-one merchants (e.g. retailers) and clients (e.g. banks) in the financial services sector.

The innovation enabled the company to develop and operate a successful merchant-funded reward programme. Under this business model, clients (e.g. banks) agreed which elements of their loyalty programme they wanted to outsource to the company for a fee, as well as the type of reward they wanted for their customers (e.g. cash back). Through this agreement, the clients' customers would gain access to a cash-back scheme (e.g. a percentage cash value of transactions which can be converted to cash payable into their bank accounts) or non-cash, merchant offers. These were funded by the company's coalition of merchants, to whom the company pitched to join its network in exchange for a platform on which they could market to existing and potential customers. Once the company had matched merchant offers to its clients (based on their requirements), offers were then published to qualifying customers. As customers took advantage of these offers, the company was updated with qualifying transactions data via acquirers or other entities to allow it to process rewards for customers. Acquirers were required to alert the company *when* one of their client's customers used their debit/credit cards with coalition merchants (i.e. 'qualifying transactions') without providing access to detailed payment-card data (e.g. information on what they bought). The company had to demonstrate to acquirers the support of its coalition of merchants and associated benefits (e.g. additional card transactions) in order for acquirers to agree to provide this service. Although some of the company's clients included financial institutions that had access to vast amounts of personal and transaction data, the outsourcing and contractual relationship between the clients and the company at the time required these clients only to supply limited payment-card transaction data (e.g. information on *who* had made a purchase (and when) and the *value* of the purchase), mainly to enable the company to calculate earnings for the customer in the cash-back scheme. Under this scheme some (limited) analytical insights were provided back to the merchant, allowing them, for example, to know more about their customers and allowing tighter targeting of offers.

### The Big Data Moment: The Commoditisation of Payment-Card Data

Under the initial scheme described above, while qualifying transactions data provided by participating merchants through their acquirers were useful, they were limited in nature. The company's next innovation involved a change in its business model, whereby *clients* (e.g. banks) allowed the company to manage personal and transactions data *they* held on their behalf in exchange for data analytics capabilities that allowed them to both target cash-back offers to their customers *and* provide more detailed, commercially valuable insights. This approach for the first time allowed banks to commoditise the vast amount of payment-card data they held, providing a comprehensive picture of customers' spending behaviour across multiple retailers and sectors (e.g. information on what customers bought, how much they spent, which retailer they bought from, location of the purchase): data which are of considerable value to merchants. Thus, financial institutions could now explore and exploit the wider commercial value of the very large amount of payment-card data they had been sitting on for years, "transforming into something valuable what used to be just a waste product archived for regulatory purposes" (Company Director of Data and Insight).

Within this second significant innovation, coalition merchants agree to be either part of a "core" network (offering cash back on qualifying transactions) to activated customers as part of a longer-term contract, or a "non-core" network offering short-term, trial offers available only to a selected group of activated customers. The company analyses the payment-card transaction data it has access to using its capabilities, knowledge and expertise, in order to identify insights which are then used to further target cash-back offers to customers as well as strategically drive sales, assess performance and measure effectiveness of the scheme. These insights are either provided to merchants as part of their contract package, or sold as an additional 'bolt-on' service. Offers are published to qualifying customers via the bank's website and via email, following which the company manages the post activation engagement and communication to enable the scheme to function effectively.

### Value Proposition, Opt-In and Informed Consent

For the banks, a key driver is generation of customer loyalty and new accounts through cash-back offers for existing and new customers. The cash-back schemes are funded solely by merchants in exchange for commercially valuable insights generated from the detailed payment-card data the banks hold. Benefits for merchants include (a) a comprehensive sector analysis of their market share; (b) grouping of their existing and potential customers into different categories (e.g. 'high value loyals'—big category spenders who are loyal to the merchant or 'switcher prospects'—low-to-medium spenders that do not currently spend with that merchant) and (c) targeting existing and prospective customers using various offer strategies.

The company profits from fees paid by banks (i.e. the clients) and from commissions taken from merchants on transactions, while customers are rewarded in the form of cash-back when they join the client's reward scheme (other redemptions are also offered including donations to charity). The *mutual*

*nature* of the value proposition was emphasised by the company's CEO as:

> the organization delivers long term benefits to multiple stakeholders—while card holders get rewarded for their spend, issuers [i.e. clients] receive a simple, integrated proposition for managing their loyalty programme, and merchants get access to a cost effective medium for marketing and improving sales.

The ethical strategy of gaining *informed consent* is central to the operation of the scheme. Customers must choose to *opt in* to the scheme and *consent* to allowing their personal transaction data to be used *in exchange* for rewards provided under the merchant-funded rewards programme. Mutual benefit across stakeholders, opt-in and informed consent form cornerstones of the company's ethical strategy for data access and commodification under which this big data—driven scheme operates.
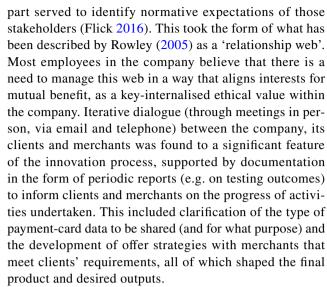
## Innovation Management within the Company

The innovation process within the company can be characterised as being an informal, quasi-stage gating approach, with loosely phased activities (*ideation, product development, pilot* and *launch)* punctuated by decision gates. This is co-ordinated by both a small product team (who manage planning and post-launch processes for new innovation concepts) and a small project team (who oversee the development and launch of those concepts), operating in a way described by the product manager as "*like an octopus with loads of arms pulling everything together*" (see Asante et al. 2014 where we observed a similar role played by the new product development team within a global asset management company).

Iterative testing of the necessary technological platforms (e.g. software coding by developers), in common with practices in other technology companies, was observed to be an important element of the innovation process. This focussed on ensuring system security and in some cases, involved the employment of the services of a hacker, who is given minimal access to the company. In some cases, a limited launch (e.g. to a small group of its client's customers) served to test the technical features of technology products and the effectiveness of marketing materials: these were characterised by multiple, informal feedback sessions with the client which led to the refinement of the final offering.

## Stakeholder Engagement

Feedback from interview respondents suggested innovation was a non-linear, complex and iterative process involving multiple stakeholder interactions, which in part served to identify normative expectations of those stakeholders (Flick 2016). This took the form of what has been described by Rowley (2005) as a 'relationship web'. Most employees in the company believe that there is a need to manage this web in a way that aligns interests for mutual benefit, as a key-internalised ethical value within the company. Iterative dialogue (through meetings in person, via email and telephone) between the company, its clients and merchants was found to a significant feature of the innovation process, supported by documentation in the form of periodic reports (e.g. on testing outcomes) to inform clients and merchants on the progress of activities undertaken. This included clarification of the type of payment-card data to be shared (and for what purpose) and the development of offer strategies with merchants that meet clients' requirements, all of which shaped the final product and desired outputs.

In the case of the second innovation described above, for example, the concept was firmed up only after a series of iterative workshops, informal face-to-face discussions and email and telephone conversations between the company and multiple client departments that included everyday banking, product, IT, legal, sourcing and risk. Matters discussed extended not only to the product/service design but also issues of confidentiality, compliance with certain UK Financial Conduct Authority (FCA) standards, definition of terms and finalisation of the contract agreement. This included clarification of the external regulatory requirements on access to and use of data. As the head of HR, compliance and payments noted, there were a lot of uncertainties about what was expected and/or acceptable. She explained,

> some people were convinced that the organization had to be regulated by the FCA and there was a lot of back and forth about it; this was only finalized after I did my research and sent emails to them, highlighting statements that meant we didn't have to be regulated by the FCA as we were not offering a financial product'.

Client (e.g. bank) approval appeared to be a very important part of the innovation governance process. This was evident, for example, in approvals required by the client on the content of messages sent to customers by the company on its behalf as part of its customer engagement management activities. In one example concerning platform development and supporting technologies, the technical project manager in the company described the client's compliance team as "the most powerful department within the client's organization as without their approval the platforms developed cannot go live". In most cases, this department is charged with ensuring that these platforms meet external requirements set by the FCA, the Advertising Standards Agency and the client's own internal policies, for example, on issues regarding how the programme is advertised, and the content and

wording of supporting text written on the client's website, in order to avoid misrepresentation.

## Regulatory Environment

In contrast to sectors such as chemicals, pharmaceuticals and novel foods, there are no 'data-before-market' regulatory approvals required for the innovations described above: the company did (and does) not require any *direct* regulatory approval prior to new product launch. Outwardly this may suggest a regulatory void. However, as we found in our previous study (Asante et al. 2014), the company's operational activities (including innovation) are governed by *contextual legislation* in the form of the UK Data Protection Act (DPA 1998)[1] and *industry guidelines* such as the Payment Card Industry (PCI) Standard, required for all organisations processing payment-card data and which we describe in more detail below. By engaging with the compliance departments of its clients (see above) innovation is also contextualised by *indirect oversight* from the FCA. This was reflected by comments made in an interview with the company's accounts director of the need to "keep audit trails on its global administration system every time an advisor communicates with a customer for use by the FCA, if needed, in ensuring that treating customer fairly (TCF) policies are adhered to".

## Towards Professionalisation and Standardisation of Processes

Over time the company has moved progressively towards a more organised (and standardised) innovation governance model as it has grown, with more systematic internalisation and integration of ethical values, principles and strategies into the company and its innovation processes, in part linked to functional necessity (Schumacher and Wasieleski 2013, p. 2). This shift has been influenced by a number of factors, including the fast growth of the company and its associations with tier-one financial institutions and merchants. Most employees explained that the increasing size of the company brought into the organisation experienced people (especially in senior management) who appreciated the benefits of standardisation and became advocates for putting appropriate processes in place. The development of a more formal innovation governance model is ongoing and includes the organisation on paper of detailed tasks and activities that will guide approvals and the product design, build and testing process. This coupled with a clear definition of internal stakeholder roles and accountabilities, the

Director of Product Development suggested, "promises to be an effective way of filtering, evaluating and guiding the development of new ideas".

## Governance and Ethics of Big Data Analytics

Having described the innovation process and its governance within the company, we now turn specifically to governance and ethical considerations as these relate to big data, the foundation for the company's innovations in the customer relationship management web. Although the loyalty programme management industry was not new at the time that the company began operations, there was at that time no specific regulation in place to govern its activities. What existed was a requirement in law for the company, as an organisation processing customer data, to register with the Information Commissioner's Office (ICO) (an independent authority established by the UK government in 1984 to oversee data privacy among other things) and to renew this annually. By registering with the ICO, the organisation was obliged to comply with a set of principles within the Data Protection Act (DPA) and guidelines provided by the ICO which included *processing data fairly, lawfully* and *for a specific purpose*, ensuring *information security* and respecting *customer privacy*. The DPA covers a variety of privacy-related issues relating to personal data processing and information standards. Its guidelines encourage *transparency*, requiring organisations to outline reasons for collecting and using data, *informing* individuals through appropriate privacy notices when collecting data, ensuring that these personal data are accurate and presented, if necessary, in a way that does not identify individuals (referred to as *data anonymisation* (ICO 2012)). This is supported by a set of *rights* with regard to personal data (e.g. a right to object to data processing likely to cause distress or result in direct marketing), which individuals can exercise in order to ensure fairness.

The DPA also restricts the amount of personal data organisations can hold and for how long; however, these guidelines are flexible and allow organisations to decide on maximum thresholds based on individual business needs. The DPA can be enforced by the ICO through periodic audits, advisory visits or the submission of self-assessment questionnaires by data controllers. Audits tend to be limited to large companies, while advisory visits and self-assessments are targeted at small-to-medium-sized companies. Within the company, respondents reported having had no engagements with the ICO since its initial registration, with compliance largely being monitored internally. However, it was noted that if a data breach were to be identified by the company and reported, the ICO reserves the right to use monetary penalty notices, "stop now" orders and prosecutions if

---

[1] https://www.gov.uk/data-protection/the-data-protection-act.

necessary to enforce compliance. The company has reported no data breaches since it started operations.
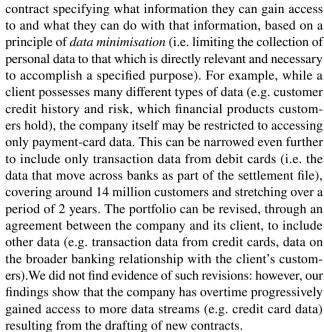
With the development of the first early innovation described above, the company was additionally required to seek certification by the Payment Card Industry (PCI) since it was now accessing payment-card data. The PCI Data Security Standard (DSS) certification is a sign of trust that the company adheres to a set of rules and practices prescribed by the PCI Standard Council to enhance card holder data security. The company's Head of Data and Insight differentiated between DSS and DPA in that:

> PCI DSS certification limits its focus to preventing fraud and protecting the banking details of customers, while DPA registration covers more broadly the protection of personal data and privacy by giving data subjects certain rights in respect of their data.

The PCI DSS is a global standard mandated by banks for all merchants who take payments from customer debit/credit cards. It "facilitates the broad adoption of consistent data security measures" (PCISSC 2013, p. 5) by providing guidelines on technical and operational issues such as building and maintaining secure networks (e.g. using firewalls), protecting card holders (e.g. through encryption), maintaining a vulnerability management programme, implementing strong access control measures and regularly monitoring and testing security systems. It is enforced internally by the company, with periodic assessments carried out by an auditor contracted by the organisation. These involve an inspection of systems and a discussion with employees in order to understand how data are collected, stored and deleted, whether encryption meets the required standard and whether the necessary security measures for desktops and network (e.g. firewalls) are in place. In addition, the auditor checks how visitors are managed in order to ensure that the building and machines are safe, that background criminal record checks have been conducted on all employees (these are occasionally shared with the company's clients) and that they have been adequately trained on the principles of the PCI DSS, training that is delivered annually via a third party. On successful completion of the PCI assessment the auditor delivers a report to the PCI Standards Council recommending certification or renewal.

## Organisational Practices

The DPA and PCI DSS provide only high-level principles within which the company, in collaboration with clients, has had to design its own bespoke tools, internal policies and mechanisms to ensure compliance. The company gains access to data through agreements made between itself and its clients. This normally takes the form of clauses within a contract specifying what information they can gain access to and what they can do with that information, based on a principle of *data minimisation* (i.e. limiting the collection of personal data to that which is directly relevant and necessary to accomplish a specified purpose). For example, while a client possesses many different types of data (e.g. customer credit history and risk, which financial products customers hold), the company itself may be restricted to accessing only payment-card data. This can be narrowed even further to include only transaction data from debit cards (i.e. the data that move across banks as part of the settlement file), covering around 14 million customers and stretching over a period of 2 years. The portfolio can be revised, through an agreement between the company and its client, to include other data (e.g. transaction data from credit cards, data on the broader banking relationship with the client's customers).We did not find evidence of such revisions: however, our findings show that the company has overtime progressively gained access to more data streams (e.g. credit card data) resulting from the drafting of new contracts.

As described above, the company's ethical strategy for data access rests on customer opt-in and informed consent. This is sought by the company through its clients (e.g. banks), who are required by the FCA to notify customers of any new way in which their data are to be used. A customer's transactional data are only made available after he/she has formally consented to register for the programme and agreed that their data can be used. When a customer expresses interest in the programme to his/her bank by signing up, the bank initially sends minimum personal information about the customer (including only the last 4 digits of the payment card, date of birth, identification number and email or telephone number), in line with the data sharing agreement earlier negotiated. This information is used by the company to create a skeleton account, following which the company contacts the interested customer concerning activation. As part of the activation process, the customer then provides full personal details including name, address, complete payment-card number. Four to five days after the customer has activated the account, the bank begins to send transactional data to the company. In this model, the company receives only minimum customer data prior to activation. Both skeleton account data and full data provided during activation are stored at an external, tier-one data centre for a period of 4 years, in compliance with agreements made with clients concerning deletion of data. This time period, they believe, enables them to strike a balance between maintaining the data long enough for analysis and audit trail purposes while not holding data longer than necessary.

The company is not allowed to disclose, use or commodify *personal* (e.g. transaction data) for any purpose other than that explicitly articulated in the contract. However, where the company has *derived* the data itself (i.e. secondary

data), these can be used in whatever way the company deems appropriate to generate insights. This process requires data anonymisation and aggregation of results, effected through a variety of data management software, reporting and statistical tools. The company's business model thrives on the principle of *unrestricted use of anonymised data*. Under this principle, it freely develops insights based on groups of card-holders and in doing so attracts merchants into its coalition network. If there are situations of ambiguity (e.g. where the company is concerned about whether data should be shared or not), the company's legal team plays a significant role in clarification, and in some cases approval is sought from the compliance department of the company's clients. The quality and accuracy of data and insights that are reported to merchants is crucial for ensuring continuous engagement and the company uses a methodology that tests the quality of anonymised data and associated insights by measuring the extent to which these impact merchant performance (e.g. sales uplift).

In order to ensure compliance with the DPA and PCI DSS, the company also imposes a set of *internal rules* on its employees. Supported by an audit log and automated controls, employees' computer activities are continuously monitored, with in-built instructions to automatically prompt the company if rules are breached. This automated approach to ensuring data security further extends to all stakeholders who use the company's platforms and systems. We observed one instance of a failed hacking attempt during the period of the study. Once this had been identified automatically, within a day the hacker had been identified and internal and external stakeholders involved in a series of discussions on a way forward. Processes and systems for data encryption are accompanied by access to data on the principle of a 'need to know' basis. The company also aims to encourage responsible behaviour by building a culture of transparency and openness, with an open plan office setting, strict recruitment processes and an induction plan that links these values to employee objectives.

## Perceptions of Ethical and Responsible Behaviour

Responsible and ethical behaviour as this related to big data access and use was found to be framed around values of security, privacy and mutual benefit. Respondents stated these in terms of

> using customer data in a way that they would expect they've given a reasonably informed consent to and made a reasonably informed judgement about a value they get in exchange [as well as] compliance with regulation on security and privacy.

All respondents demonstrated awareness of ethical issues regarding privacy and security of big data in the payment-card industry and commitments to comply with associated regulation and standards. Respondents perceived responsible behaviour in relation to their (differentiated) role(s), e.g. using their specific knowledge and expertise to enhance discussions and raise issues of concern. So, for example, while the data and insight team were observed to focus on safeguarding payment-card data and "whether the organization can do a piece of analysis at an aggregated, anonymised level", members of the company's legal department were consulted for clarification on privacy issues, while those in managerial roles took on the additional role of ensuring compliance of team members to organisational and regulatory policies and expectations.

Respondents described three motivating factors for responsible behaviour: a yearning to see the company grow and thrive, a desire to maintain a positive reputation and a longing for self-fulfilment. Regarding the first factor, respondents perceived a positive correlation between responsible behaviour and organisational growth which was reflected in statements such as "the whole business model of the organization hangs on trust, therefore the organization has to behave in a way that does not undermine that trust", and "if we breached PCI, we could go out of business". Personal employment security, working with talented individuals, and personal connections to the company and its entrepreneurial ethos, all contributed variously to desires to see the company grow and the role of responsible behaviour in promoting this. Those respondents who emphasised reputation expressed concern about not wanting to do anything "that makes them uncomfortable", "goes against their values and principles", "compromised their name" or "tarnished their image". These values appear to have been influenced to some extent by experiences they had prior to joining the company. For example, one respondent mentioned that her experience in previous positions in the financial services sector helped shape her values and encouraged her to move on to what she described as "a more responsible organization that gave back to customers". In terms of self-fulfilment, respondents highlighted a "desire to make a positive impact on key stakeholders" and the satisfaction they gained in 'doing things right' and influencing society for good as drivers for responsible behaviour.

## Discussion and Conclusions

We have investigated how one company has approached the governance and ethics dimensions associated with innovation in financial services using big data. The company in our case study has exhibited a considerable degree of technological innovation over time to allow exploitation of big

data and associated analytics. In doing so, it has positioned itself as a key intermediary and data aggregator/steward at the centre of an extensive, dynamic and managed stakeholder relationship web and information supply chain (Martin 2015). In contrast to our previous research in the asset management sector (Asante et al. 2014), where regulation was found to play a direct role in approving new products prior to launch and commercialisation, in the current study innovations were not subject to such 'data-before-market' legislation. This does not however imply that the company's operations, and more specifically innovation based on big data, fall into a governance void: as with our previous study, we found the big data innovation environment in this respect to be governed by contextual legislation and industry standards (here relating to data protection and usage),[2] these being themselves underpinned by values and principles relating to privacy and data security.

Our findings suggest the company has internalised and progressively embedded these values and principles into its policies and operations, framing innovation and its governance. By internalising, integrating and progressively institutionalising these, the company has fostered the co-existence of innovation with an associated ethical orientation considered essential for long-term corporate survival and growth (Schumacher and Wasieleski 2013). This has required the translation of broad ethical values prescribed within an emergent external regulatory environment into bespoke corporate policies and processes, necessitating the company to develop and implement its own operational practices, particularly in relation to data minimisation, anonymisation and aggregation.

Floridi and Taddeo (2016) have defined three key issues relating to the ethics of organisational practices as these relate to big data: user privacy, consent and secondary (data) use: the organisation has had to engage with all three issues over time. The company was found to be grounded in a philosophy of 'privacy as information rules' (Richards and King 2014) where by privacy is not 'thought of merely as how much is secret, but rather about what rules are in place (legal, social or otherwise) to govern the use of information as well as its disclosure' (Ibid; see also Martin 2015, p. 74). Grounded in principles of data minimisation and anonymisation, these information rules were strictly enforced (e.g. through automated controls and breaching sanctions), set within an organisational culture in which such rules were continuously reinforced. These placed restriction on use of personal ('qualifying') data while furthering a corporate

principle advocating the unrestricted use of secondary, anonymised and aggregated data to provide commercially valuable insights. This was supported by an ethical strategy based on opt-in through informed consent for data to be accessed and manipulated for specific purposes, with the rules (and normative expectations) around information access and use being clearly defined *ex ante* through stakeholder engagement and contracting within which access by the company to data not specifically relevant to the purpose was excluded.

This strategy hinges on customers opting into the scheme after reviewing and agreeing to its terms and conditions, wherein the possibility of sharing anonymised data "as part of statistics or other aggregated data" with third parties is disclosed. This is further supported by general communications from the client (e.g. bank) to its customers advising them of new ways in which their data would be used if they choose to opt into the scheme (e.g. variation notices). However, we suggest that the scheme's data supply chain and secondary data market activities are only partially visible to customers (Martin 2015, p. 80). Additionally, as we have discussed above, Flick (2016) and other authors (e.g. Mantelero 2014) have argued that this model of "notice and consent" is inadequate in the context of big data analytics, in part because these involve the use of complex data acquisition and processing tools that consumers may not have sufficient competence to understand, thus limiting their ability to evaluate the implications and consequences of their choices in order to make an informed decision (Richards and King 2014). While Flick (2013, 2016) stresses the importance of the *quality of disclosure* in terms of the content of terms and EULAs and how this content is displayed, even so she argues that in contexts such as big data disclosure alone is insufficient. She advocates for a communication framework in which stakeholder's normative expectations can be surfaced and articulated (e.g. around data access and privacy) as a dialogic and adaptive approach to support a more meaningful and effective process of informed consent. This aligns with emerging frameworks for responsible innovation (Stilgoe et al. 2013) which argue for competencies and capacities of anticipation, reflexivity and inclusive deliberation to be embedded in an around innovation management processes. Indeed, we found extensive and iterative stakeholder engagement to be a key feature of the innovation environment within the company. But while this did serve to articulate normative expectations of specific stakeholders (e.g. clients), it was not directly motivated or configured to support effective informed consent by customers.

Our findings overall suggest an adaptive, multi-level governance environment that has evolved to include a mixture of statutory, industry-led and internal corporate governance mechanisms underpinned by a set of ethical values, principles and strategies relating to data capture,

---

[2] Since the completion of this study, the regulatory environment has further evolved with the advent of the EU Second Payment Services Directive-PSD2 in 2015 and the EU General Data Protection Regulation-GDPR in 2016 (EU 2016/679).

usage, manipulation and valorisation. In this dynamic big data environment, the company has had to be adaptive and responsive, particularly to the needs of its stakeholders and specifically in the translation of high-level principles into operational practices.

We have been granted access to one company, from which one should not attempt to generalise (i.e. external validity). Likewise, our findings apply to big data innovation in the context of the financial services sector that we have studied. Acknowledging the challenges of access, we recommend the need for more empirical research within companies innovating in the big data space in financial services and beyond in order to provide further insights concerning how these organisations are a) undertaking and managing big data-inspired innovation internally and with stakeholders, b) how multi- level governance is evolving and being enacted and c) how companies are approaching the ethical dimensions associated with the opportunities presented by big data at an operational level.

## Compliance with Ethical Standards

**Conflict of interest** Keren Naa Abeka Arthur declares that she has no conflict of interest. Richard Owen declares that he has no conflict of interest.

**Ethical Approval** This article does not contain any studies involving human participants or animals performed by any of the authors. The study involved observational ethnography within a company for which prior ethical approval was granted by the University of Exeter and for which prior permission was granted by the company.

**Non-disclosure Agreement** This study was subject to a 2-year non-disclosure agreement by the company in which the research was conducted, which expired in December 2016.

## References

Ahn, Y. J., Kim, K. S., & Han, S. K. (2003). On the design concepts For CRM systems. *Industrial Management and Data Systems, 103,* 324–331.

Armstrong, M., Cornut, G., Delacôte, S., Lenglet, M., Millo, Y., Muniesa, F., et al. (2012). Towards a practical approach to responsible innovation in finance: New product committees revisited. *Journal of Financial Regulation and Compliance, 20*(2), 147–168.

Asante, K., Owen, R., & Williamson, G. (2014). Governance of new product development and perceptions of responsible innovation in the financial sector: Insights from an ethnographic case study. *Journal of Responsible Innovation, 1*(1), 9–30.

Bareisis, Z. (2012). *Selecting A merchant-funded rewards platform: An in-depth analysis of MFR vendors*. Boston, MA: Celent.

Baucus, M. S., Norton, W. I., Jr., Baucus, D. A., & Human, S. E. (2008). Fostering creativity and innovation without encouraging unethical behaviour. *Journal of Business Ethics, 81,* 97–115.

Bhasin, A., Kirkpatrick, R., & Thomas, C. A. (2012). Big data for the next big idea in financial services: Understanding customers, global economies and human welfare with analytics. In *Proceedings of the 2012 SAS Financial Services Executive Summit*: SAS Financial Services, Cary, NC.

Blattberg, R. C., & Deighton, J. (1996). Manage marketing by the customer equity test. *Harvard Business Review, 74,* 136–144.

Bollier, D. (2010). *The promise and peril of big data*. Washington, DC: The Aspen Institute.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society, 15,* 662–679.

Brannan, M., Rowe, M., & Worthington, F. (2012). Time for a new journal, a journal for new times. *Journal of Organizational Ethnography, 1,* 5–14.

Brassington, F., & Pettitt, S. (2006). *Principles of marketing*. Essex: Financial Times Prentice Hall.

Brown, B., Chui, M., & Manyika, J. (2012). Are you ready for the era of 'big data? *Mckinsey Quarterly, 4,* 24–35.

Bruene, J. (2014). The Conference Journey: Why We Started Findevr (And Finovate). Retrieved June 6, 2014, from http://www.netbanker.com/2012/04/merchantfunded_rewards_summary_with_infographic.html

Brynjolfsson, E., Hitt, L., & Kim, H. K. (2011). Strength in numbers: how does data-driven decision-making affect firm performance? In *Proceedings of the International Conference on Information Systems:* ICIS, Shanghai, China.

Bughin, J., Chui, M., & Maynika, J. (2010). Clouds, big data and smart assets: Ten tech-enabled business trends to watch. *The Mckinsey Quarterly, 56*(1), 75–86.

Caltabiano, M., & Ferguson, R. (2009). *The mother of invention: The power of merchant-funded rewards in a recession*. Cincinnati, OH: Partnertalk.

Celma, F., Sandall, N., Smout, C., & Brennan, S. (2014). The single supervisory mechanism (SSM): The big data issue. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/single-supervisory-mechanism-ssm-big-data-issue_MFL.pdf. Accessed 3 June 2019.

Chaffey, D. (2007). *E-business and e-commerce management*. Essex: Financial Times/Prentice Hall.

Chaudhary, R., Del Giudice, M., Shah, T. P., & Sifter, C. J. (2013). *Data governance for financial institutions: Regulatory compliance requires more than just technology*. Chicago: Crowe Horwath LLP.

Chaudhuri, S., Dayal, U., & Narasayya, V. (2011). An overview of business intelligence technology. *Communications of the ACM, 54,* 88–98.

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly, 36,* 1165–1188.

Cheng, X., Hu, C., Li, Y., Lin, W., & Zuo, H. (2013). Data evolution analysis of virtual dataspace for managing the big data lifecycle. In *Proceedings from IEEE 27th International Symposium on Parallel and Distributed Processing Workshops and PhD Forum (IPDPSW)*, Cambridge, MA, USA.

Coumaros, J., De Roys, S., Chretien, L., Buvat, J., Kvj, S., Clerk, V., & Auliard, O. (2014). Big data alchemy: How can banks maximize the value of their customer data? Capgemini Consulting.

https://www.capgemini.com/wp-content/uploads/2017/07/bigdatainbanking_2705_v5_1.pdf. Accessed 3 June 2019.

Dias, E. (2013). Big data planning guide for financial services. Perficient. https://cloud.report/Resources/Whitepapers/16f4511c-c6fd-48c4-91fa-d332f40cf2e5_perficient.pdf. Accessed 3 June 2019.

Eberle, T. S., & Maeder, C. (2010). Organizational ethnography. In D. Silverman (Ed.), *Qualitative research*. Los Angeles, CA: Sage.

Economist. (2012). Big data: Crunching the numbers. *The Economist*. http://www.economist.com/special-report/2012/05/19/crunching-the-numbers. Accessed 3 June 2019.

Fassin, Y. (2000). Innovation and ethics: Ethical considerations in the innovation business. *Journal of Business Ethics, 27*, 193–203.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine, 17*, 37–54.

Flick, C. (2013). Informed consent in information technology: Improving end user licence agreements. In J. Weckert & R. Lucas (Eds.), *Professionalism in the information and communication technology industry* (p. 127). Canberra: ANU E Press.

Flick, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics, 12*(1), 14–28.

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*, *374*(2083), 20160360.

Frawley, W. J., Piatetsky-Shapiro, G., & Matheus, C. J. (1992). Knowledge discovery in databases: An overview. *AI Magazine, 13*, 57–70.

Fulgoni, G. (2013). Big data:: Friend or foe of digital advertising? Five ways marketers should use digital big data to their advantage. *Journal of Advertising Research, 53*, 372–376.

Gantz, J., & Reinsel, D. (2011). *Extracting value from chaos. IDC IVIEW*. Framingham, MA: IDC Go-To-Market Services.

Herschel, R., & Miori, V. (2017). Ethics and big data. *Technology and Society, 49*, 31–36.

Hildebrandt, M. (2006). Profiling: From data to knowledge. *Datenschutz Und Datensicherheit - DUD, 30*, 548–552.

Hitzler, P., & Janowicz, K. (2013). Linked data, big data, and the 4th paradigm. *Semantic Web, 4*, 233–235.

IBM. (2011). *From stretched to strengthened: Insights from the global chief marketing officer study*. Somers, NY: IBM.

IBM. (2012). *Leading through connections: Insights from the global chief executive officer study*. Hampshire: IBM.

ICO. (2012). *Anonymisation: Managing data protection risk code of practice*. Wilmslow, Cheshire: Information Commissioner's Office. https://ico.org.uk/media/1061/anonymisation-code.pdf. Accessed 3 June 2019.

Jeffrey, B., & Troman, G. (2004). Time for ethnography. *British Educational Research Journal, 30*, 535–548.

JSR. (2011). *Merchant-funded rewards programs: Moneymakers for financial institutions, market makers for merchants*. San Francisco, CA: Javelin Strategy & Research.

Kambatla, K., Kollias, G., Kumar, V., & Grama, A. (2014). Trends in big data analytics. *Journal of Parallel and Distributed Computing, 74*, 2561–2573.

Krishnan, K. (2013). Introduction to big data. In K. Krishnan (Ed.), *Data warehousing in the age of big data: A volume in MK series on business intelligence*. Waltham, MA: Morgan Kaufmann.

Laney, D. (2001). 3-D data management: Controlling data volume, velocity and variety. *Meta Group*. https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Accessed 3 June 2019.

Lavalle, S., Lesser, E., Shockley, R., Hopkins, M. S., & Kruschwitz, N. (2011). Big data, analytics and the path from insights to value. *MIT Sloan Management Review, 52*, 21–31.

Linoff, G. S., & Berry, M. J. A. (2011). *Data mining techniques: For marketing, sales, and customer relationship management*. Indianapolis, IN: Wiley.

Loshin, D. (2013). Data governance for big data analytics: Considerations for data policies and processes. In D. Loshin (Ed.), *Big data analytics: From strategic planning to enterprise integration with tools, techniques, NOSQL, and graph*. Waltham, MA: Elsevier Science.

Madden, S. (2012). From databases to big data. *Internet Computing, IEEE, 16*, 4–6.

Manovich, L. (2012). Trending: the promises and the challenges of big social data. In M. K. Gold (Ed.), *Debates in the digital humanities*. Minneapolis, MN: The University Of Minnesota Press.

Mantelero, A. (2014). The future of consumer data protection in the E.U.: Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law and Security Review, 30*, 643–660.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., et al. (2011). *Big data: The next frontier for innovation, competition, and productivity*. New York: Mckinsey Global Institute.

Martin, K. E. (2015). Ethical issues in the big data industry. *MIS Quarterly Executive, 14*(2), 67–85.

Mcgarvey, R. (2012a). Credit unions still skeptical about cloud computing. *Credit Union Times*.

Mcgarvey, R. (2012b, September 02). Turning 'big data' into big dollars to grow revenue. *Credit Union Times*.

Meel, M., & Saat, M. (2002). Ethical life cycle of an innovation. *Journal of Business Ethics, 39*, 21–27.

Muniesa, F., & Lenglet, M. (2013). Responsible innovation in finance: directions and implications. In R. Owen, J. Bessant, & M. Heintz (Eds.), *Responsible innovation: Managing the responsible emergence of science and innovation in society* (pp. 185–198). Chichester: Wiley.

Neyland, D. (2007). *Organizational ethnography*. London: Sage.

Ngai, E. W. T., Xiu, L., & Chau, D. C. K. (2009). Application of data mining techniques in customer relationship management: A literature review and classification. *Expert Systems with Applications, 36*, 2592–2602.

Normandeau, K. (2013). Beyond volume, variety and velocity is the issue of big data veracity. Retrieved October 1, 2015, from http://insidebigdata.com/2013/09/12/beyond-volume-variety-velocity-issue-big-data-veracity.

Nunan, D., & Domenico, M. D. (2013). Market research and the ethics of big data. *International Journal of Market Research, 55*, 41–56.

Nunan, D., & Domenico, M. D. (2017). Big data: a normal accident waiting to happen? *Journal of Business Ethics*, *145*(3), 481–491.

OCC, Office of the Comptroller of the Currency. (2016). Supporting responsible innovation in the federal banking system: An OCC perspective. Retrieved November 1, 2016, from https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf.

PCISSC. (2013). *PCI data security standard: Requirements and security assessment procedures*. London, UK: Payment Card Industry Security Standard Council.

Peppard, J. (2000). Customer relationship management (CRM) in financial services. *European Management Journal, 18*, 312–327.

Richards, N. M., & King, J. H. (2014). Big data ethics. *Wake Forest Law Review, 49*, 393.

Richardson, L. (1995). Narrative and sociology. In J. V. Maanen (Ed.), *Representation in ethnography*. Thousand Oaks: Sage.

Riessman, C. K. (2002). Analysis of personal narratives. In J. F. Gubrium & J. A. Holstein (Eds.), *Handbook of interview research*. Thousand Oaks, CA: Sage.

Riessman, C. (2008). *Narrative methods for the human sciences*. London, UK: Sage.

Rose, J., Baton, C., Souza, R., & Platt, J. (2013). *The trust advantage: How to win with big data*. Boston, MA: The Boston Consulting Group.

Rowley, J. (2004). Loyalty and reward schemes: How much is your loyalty worth? *The Marketing Review, 4,* 121–138.

Rowley, J. (2005). Building brand webs. *International Journal of Retail & Distribution Management, 33,* 194–206.

Royal Statistical Society. (2015). The opportunities and ethics of big data. www.rss.org.uk/Images/PDF/influencing-change/2016/rss-report-opps-and-ethics-of-big-data-feb-2016.pdf.

Russom, P. (2011). *TDWI best practices report: Big data analytics.* Renton, WA: TDWI Research.

Rygielski, C., Wang, J. C., & Yen, D. C. (2002). Data mining techniques for customer relationship management. *Technology in Society, 24,* 483–502.

Sauer, C. (2013). Powerful analytical tools help CUS extract actionable trends from mountains of data. *Credit Union Magazine.*

Schroeck, M., Shockley, R., Smart, J., Romero-Morales, D., & Tufano, P. (2012). *Analytics: The real-world use of big data. How innovative enterprises extract value from uncertain data.* Somers, NY: IBM Global Business Services and Saïd Business School.

Schumacher, E. G., & Wasieleski, D. M. (2013). Institutionalizing ethical innovation in organizations: An integrated causal model of moral innovation decisionprocesses. *Journal of Business Ethics, 113,* 15–37.

Schutt, R. K. (2012). *Investigating the social world: The process and practice of research.* Thousand Oaks, CA: Sage.

Shaw, M. J., Subramaniam, C., Tan, G. W., & Welge, M. E. (2001). Knowledge management and data mining for marketing. *Decision Support Systems, 31,* 127–137.

Stilgoe, J., Owen, R., & Macnaghten, P. M. (2013). Developing a framework for responsible innovation. *Research Policy, 42*(3), 1568–1580.

Sunil, S. (2012). *Big data governance: An emerging imperative.* Boise, ID: MC Press.

Tallon, P. P. (2013). Corporate governance of big data: Perspectives on value, risk, and cost. *Computer, 46,* 32–38.

Thomas, A. B. (2003). Research strategies: The case study, ethnography and action research. In A. B. Thomas (Ed.), *Researchskills for management studies.* London: Taylor & Francis.

Turban, E., Sharda, R., Aronson, J. E., & King, D. (2008). *Business intelligence: A managerial approach.* Boston, MA: Pearson PrenticeHall.

Turner, D., Schroeck, M., & Shockley, R. (2012). *Analytics: The real-world use of big data in financial services. How innovative banking and financial markets organizations extract value from uncertain data.* Somers, NY: IBM Global Business Services and Saïd Business School.

Venkatasubramanian, U. (2012). *Data governance for big data systems.* Bangalore: L&T Infotech.

Verma, R., & Mani, S. R. (2012). *Use of big data technologies in capital markets.* Bangalore: Infosys.

Watson, T. J. (2012). Making organisational ethnography. *Journal of Organizational Ethnography, 1,* 15–22.

Watson, H. J., & Wixom, B. H. (2007). The current state of business intelligence. *IEEE Computer, 40,* 96–99.

Worthington, S. & Fear, J. (2009). The hidden side of loyalty card programs. The Australian Centre For Retail Studies.

Yadav, R. (2012). Next generation loyalty management systems: Trends, challenges, and recommendations. Capgemini. https://www.capgemini.com/pt-en/wp-content/uploads/sites/20/2017/07/Next_Generation_Loyalty_Management_Systems__Trends__Challenges__and_Recommendations.pdf. Accessed 3 June 2019.

Yulinsky, C. (2012, 24 January). Decisions, decisions … Will 'big data' have 'big' impact? *Financial Times.*