International Journal of Business Analytics and Intelligence
10 (2) 2022, 25-39
http://publishingindia.com/ijbai/

Ensuring Compliance in the Digital Era: A Knowledge-Based Dynamic Capabilities Framework Wheel for Data-Driven Organisations

Stephen Treacy*

Abstract

Data-driven organisations are becoming increasingly prevalent, yet the degree to which knowledge-based dynamic capabilities (KBDC) have been explored in conjunction with data governance and compliance remains scarce. While there is ample support for the presence of KBDC within data management and strategy development, data compliance represents a compelling setting, given the increasingly stringent data protection regulations being enforced worldwide. This has led to a distinct lack of prior research exploring the area, especially as previous studies have chosen to focus instead on the data regulations and implications themselves, rather than a standalone theory. We interview 19 data compliance experts across seven countries to explore how KBDC mechanisms can be used to: (i) develop, (ii) establish, and (iii) commit to a data compliance strategy. Through this study, we present a conceptual data compliance strategy framework wheel for data-driven organisations, and discuss the implications for both IS and practice.

Keywords: Data Driven Organisations, Knowledge Based Dynamic Capabilities Theory, Data Compliance, Data Governance

Introduction

The rapid proliferation of data facilitated by the Internet, cloud computing, social media, and mobile devices has an abundance of value potential that must be capitalised (Hartmann et al., 2016). Organisations have begun to move away from product-based offerings, towards a more complex, data-driven business model (Weiner & Weisbecker, 2011), where the facilitation of data-related ventures to capture value has been seen to be prolific (Manyika et al., 2011; Chesbrough & Rosenbloom, 2002). In the current digital economy, successful companies will be those who have developed big data-driven decision making (McAfee et al., 2012). However, the compliance and regulation involved in these business models, particularly for multinationals, is not straightforward due to the highly unstructured nature of data, and the proliferation of separate data laws globally. Furthermore, in recent years, the onus of protecting personal data was left to the individual; however, this expectation is shifting. Organisations are now being expected to assume the role of data steward and this is affecting the ways in which businesses can use data. Unfortunately, most organisations only have a diffuse understanding about the evolving landscape of data regulatory compliance, and its impact on data-driven organisations (Matt et al., 2015). Notably, scholars have published surprisingly little on the ability for these organisations to remain compliant across the various data regulations they may be subject to. Consequently, they struggle to successfully design and implement actionable strategies (Bharadwaj et al., 2013; Svahn et al., 2017). To that end, this paper explores knowledge-based dynamic capability (KBDC) theory in response to regulation and compliance, and presents a conceptual data compliance strategy framework wheel for data-driven organisations. The remainder of the paper is organised as follows: Section 2 discusses the theoretical and conceptual background of this research, introducing the reader to data-driven organisations and the evolving compliance landscape they are faced with. The theoretical lens of knowledge-based dynamic capabilities

* Lecturer, Director of Information Systems for Business Performance (ISBP), Cork University Business School, University College Cork, Ireland. Email: stephen.treacy@ucc.ie

is then presented, revealing it to be an appropriate theory to investigate an organisation's capability to acquire, combine, and generate knowledge to explore, analyse, and address the environmental dynamics. The research gap, which will be addressed in this study, is then presented. Section 3 presents the research strategy adopted herein, before section 4 provides the main findings of this investigation. These findings identify a preliminary conceptual data compliance strategy (DCS) framework wheel for data-driven organisations. Finally, section 5 provides the conspectus, highlighting the principal conclusions for industry applications, areas for future research, and the study's limitations.

Theoretical and Conceptual Background

Data-Driven Organisations

Through the opportunities afforded from ongoing digitalisation and advancing competition, an increasing number of services and products are delivered with technology that is able to gather and process large quantities of data and facilitate continual transformation of business activities (Kammler et al., 2019). While this has enabled greater information accessibility, and created new opportunities, organisations are increasingly realigning their structures, operations, and strategies with IT to realise the benefits on offer, including improvements in performance, cost, and service quality (Hansen et al., 2011; Dremel et al., 2017; Kohli & Johnson, 2011). Data now has a huge influence on both operational and strategic decision making processes (Alhassan et al., 2016), as the information derived from it becomes the unique corporate asset which has the potential to set an organisation apart (Aiken & Harbour, 2017). While digital technologies connect people, things, and locations to create and analyse large amounts of data, it also fundamentally alters communication and interactions between all stakeholders and reshapes the existing political, social, and economic landscape (Holotiuk & Beimborn, 2017; Hansen & Sia, 2015; Hess et al., 2016). Big data has thus become both a driver and an output of the digitisation of society and has completely changed the game of data analytics (Mayer-Schönberger & Cukier, 2013), with the interest, and subsequently, adoption of analytical tools and techniques for big data problems in the industry growing substantially in recent years (Sharma et al., 2020). It is therefore unsurprising that while data is now seen as the source of competitive advantage for organisations, it can also lead to trade-offs between data value and ethics, particularly from a consumer perspective (Vidgen et al., 2017). The processing of consumers' personal information is an unavoidable element for any organisation, with organisations requiring consumer information for several reasons, including the sale and delivery of products, personalised services, and customer profiling (Hui et al., 2007). Steady advancements in technologies that enable organisations to aggregate and analyse data for the very purpose of improved decision making may threaten an individual's right to data privacy (Acquisti et al., 2015). Inevitably, there has been a growing demand for stronger ethics surrounding the commercial use of data in recent years, putting increased pressure on organisations to meet the ethical expectations of the consumers, their employees, and the society at large (Loi et al., 2019). This reflects the muddy reality of our new digital world, and the emerging political and social complexity that encircles the collection and use of personal data (Nunan, 2020). The pushing of existing technological boundaries and the corresponding regulations have led to data privacy becoming a major area of concern for organisations (Royakkers et al., 2018) that are recognising the inherent risks associated with the use and management of big data.

Evolving Regulations

The over-reliance of contemporary business models on extensive data collection practices has raised much concern over issues relating to consumer privacy (Morey et al., 2015). Managing personal data has led to contrasting views, with some organisations believing that they own their customer's information, and should therefore exploit access to it for business purposes (Lauer & Deng, 2007), while other organisations take the opposite view that this information is borrowed from their customers and as such hold its privacy in high regard. Regardless, as data-driven organisations continue to seek innovative methods for the exploitation of the exponential growth of data available, it has similarly resulted in calls to standardise and regulate the way data is collected, processed, and accessed. Current literature across psychology, law, marketing, economics, and particularly, the IS field (Smith et al., 2011; Xu et al., 2011), reflects this demand, and outlines the increase of

data privacy laws across varying geographic jurisdictions, leading to a renewed focus being placed on the practices of accurate data governance for data-driven organisations (Arora, 2019; Barrett, 2019; Beckett, 2017; Determann & Gupta, 2018; Feng, 2019; Merrick & Ryan, 2019). As a direct result, governments are increasingly being called upon to protect people's data due to the growing numbers of incidents involving the improper use of personal data (Winegar & Sunstein, 2019). For example, under the General Data Protection Regulation (GDPR), the term '*personal data*' now refers to any kind of information regarding an individual, including name, identification number, location data, and factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the natural person (Politou et al., 2018; Erickson, 2018). The regulations apply to anyone or any company that is actively collecting and processing personal data about EU data subjects, regardless of where the organisation is based and irrespective of where they store the data (Tankard, 2016). The significant financial penalty system that has been introduced as part of the new legislation has forced the organisations choosing to service the EU to weigh up the benefits of collecting, storing, and aggregating personal data, since to do so without valid consent or in an unsafe manner would likely end up costing more than it is worth, if fined under the regulations (Voigt & von dem Bussche, 2017). Several authors have argued the ways in which GDPR is problematic; for instance, most recently criticism was levelled towards the regulation based on the challenges when collecting ethnicity data required for analysing Covid mortality rates (Webber, 2020). Similarly, the California Consumer Privacy Act (CCPA) was introduced to regulate the protection, retention, deletion, and management of consumer privacy information in the state (Diamond, 2019; Barrett, 2019). Much like GDPR, there are mixed views on the effectiveness of the Californian regulation within the literature, such as the limitations surrounding the sale of personal information (Illman & Temple, 2019), pointing to the significantly smaller scope and weaker protection it offers (Pernot-Leplay, 2020). Other recent examples have included the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the Lei Geral de Proteção de Dados Pessoais (LGDP) in Brazil, India's Personal Data Protection Bill (Patnaik, 2020), and the Chinese Cybersecurity law (Greenleaf & Livingston, 2017), with new regulations also taking shape in Dubai and Egypt (Nunan, 2020). In synthesis, this trend of introducing customised data protection and compliance regulations is continuing to emerge across the global markets, which is increasing the emphasis on data privacy, specifically for organisations that collect and process personal data for business operations across multiple jurisdictions. Compliance should no longer be conceived as a chaotic or expensive burden; rather, it should be viewed as a trust-based form of competitive advantage (Voss & Houser, 2019). Since companies have shifted towards the treatment of data as a corporate asset, research on the topic of data governance has steadily increased. Yet, conversely, there is still a lack of research surrounding data governance activities to incorporate this multitude of regulatory expectations (Cheong & Chang, 2007; Alhassan et al., 2016).

Knowledge-Based Dynamic Capabilities

Ensuring data compliance is not just about the availability of access and analysis, it follows a chain of activities including the collection of needed data, storing, preparation, analysis, and effective decision making (Janssen et al., 2017), with each of these activities requiring different sets of managerial resources and capabilities (Shamim et al., 2020). With this in mind, the knowledge-based view (KBV) of the firm suggests that knowledge is a vital strategic resource of any organisation, with the main purpose of the organisation to translate knowledge into commercial outcomes (Grant, 1996). The dynamic capabilities view also argues that possessing strategic resources is not enough; that to acquire sustainable advantage, organisations should also be able to create and reconfigure competencies to create value from resources (Teece et al., 1997; Teece, 2007). The combination of these research streams has led to the KBDC view, which refers to the organisational capability to acquire, combine, and generate knowledge to explore, analyse, and address the environmental dynamics (Zheng et al., 2011). Furthermore, dynamic capabilities depends on knowledge management and learning mechanisms to drive the development of dynamic capabilities in these organisations (Eisenhardt & Martin, 2000). In the context of this study, the KBDC view provides an appropriate theoretical foundation to explore compliance, given how KBDC is used in existing literature as an overarching theoretical framework to discuss big data related

capabilities (Shamim et al., 2019; Shamim et al., 2020; Zheng et al., 2011). Facilitating these capabilities enables the organisation to improve the quality of decision making, while big data governance can ensure the provision and quality of big data, along with the knowledge to facilitate big data proficiency (Janssen et al., 2017). Along with managing access to big data, KBDC also enables the provision of data-related knowledge to those responsible for data analysis, processing, and decision making, such as data sources, and the difficulties associated with data (Janssen et al., 2017). Contemporary literature acknowledges the management of data, facilitating an effective strategy as dynamic capabilities (Côrte-Real et al., 2017; Shamim et al., 2019).

Research Gap

Firms use a wide array of strategies to comply with government regulations (Desai, 2016) and with privacy concerns increasing rapidly, there is a pressing need for better mechanisms which can help protect individuals' privacy (Kumari & Chakravarthy, 2016). Unfortunately, there exists scant empirical research on how organisations, particularly data-driven organisations, respond, plan, and adapt to these evolving government regulations (Wang & Yu, 2017). This is partly due to the fact that producing an appropriate strategy for privacy design for these organisations and its customers is not a simple task (Preibusch et al., 2013). Indeed, engineering systems to undertake the challenge of dealing with privacy concerns has been described as being "*bewildering complex*" with no easy-fix solution (Gürses, 2014). This is in part due to the fact that they may be subject to several data regulation laws as outlined previously, depending on their geographic profile. We argue that the restrictions imposed through global legislations surrounding personal data are evolving rapidly, and accordingly, it has become an area of particular concern. This trend of increasing regulations, in addition to the disparities between these different regulations, serves to increase the difficulty in achieving full compliance. While extant literature identifies GDPR as the strictest legislation (Barrett, 2019; Determann & Gupta, 2018; Goddard, 2017; Merrick & Ryan, 2019), several authors disagree as to whether it fundamentally ensures global compliance (Illman & Temple, 2019). To complicate matters further, privacy and security breach requirements are evolving rapidly, and organisations need to keep abreast of the legislations to understand, assess, and comply with the data laws in the event of such a breach (Brody & Nielson, 2005). Indeed, while many organisations have allocated budget, time, and resources to ensure compliance with data protection laws, the true test lies in their ability to build a bedrock system to manage these evolving regulations. While the development of mechanisms to support compliance has garnered attention in academic circles, to date there is not only scant empirical literature on KBDC and data compliance, but theoretical gaps also remain in our understanding of how KBDC can be embraced to provide strategy formulation. Based on our understanding of KBDC, we suggest that KBDC can enhance data compliance strategies for data-driven organisations through the identification of key mechanisms across three distinct research questions: (i) *What KBDC mechanisms are required in developing a data compliance strategy for data-driven organisations?*; (ii) *What KBDC mechanisms are required in establishing a data compliance strategy for data-driven organisations?*; and (iii) *What KBDC mechanisms are required in committing to a data compliance strategy for data-driven organisations?* To sum up, we present an investigation, from the views of experts, into how, through the KBDC perspective, data-driven organisations can develop, establish, and commit to an effective data compliance strategy, in response to continually evolving regulations.

Research Strategy

This section focuses on the key research decisions and the methodological selections used to guide this study.

Judgment Study

For the purpose of this study, the definition provided by Garthwaite et al. (2005) for experts is adopted, who describe them as being "*persons to whom society and/or peers attributes special knowledge about matters being elicited*" (p. 681). Expert judgment can be used informally, when no data are available, and formally, to bound problems and qualitatively structure models (Wilson, 2017), through the use of semi-structured interviews, providing a naturalistic method to validate theoretical artifacts in real environments or organisational contexts (Venable et al., 2016). This approach allows

the researcher to explore emergent themes within the interview setting as they arise, while also enabling the researcher to pursue additional lines of questioning towards areas of interest in which the experts had evident experience. Through integrative assessment, the selected experts can communicate and synthesise understanding for societally important questions, which was fundamental in achieving a detailed understanding of the topic (Knox & Burkard, 2009). The execution of surveys had been considered; however, the incompatibility of this instrument to the subtleties of IT in complex settings indicated that a solely qualitative approach would be more suitable (Palvia et al., 2003). The use of focus groups was additionally explored but ruled out due to the sensitivity of the topic, particularly in regard to compliance, as participants may not discuss opinions and experiences openly in this format (Morgan, 1997). The selected methodology was deemed suitable as it reinforces understanding and aids in extracting the underlying intentions of interactions, which ultimately complement the process of deriving precise findings and addressing the scope of the research problem area. The expert sampling was achieved with an initial purpose in mind as per Lincoln and Guba (1985), which was to ensure the appropriateness of the data collected in conjunction with the representation of the phenomenon under investigation (McIntosh & Morse, 2015). With this in mind, and following case selection methodologies described by Yin (2008) and Seawright and Gerring (2008), the selection of experts ensured multiple objectives: (1) experts occupied roles that made them knowledgeable about the issues being researched; (2) a representative sample of experts was obtained; (3) useful variations of theoretical interest were achieved; and (4) experts have several years of experience working with data protection and/or data privacy in multinational data-driven organisations. Based on this selection criteria, 19 interviewees across seven different countries were selected, with roles including Senior Director, Head of Data Operations, Global Privacy Manager, and Data Protection Officers, as outlined in Table 1.

Table 1: Expert Details for Judgment Studies, Including Their Roles, Industries, and Market Experience

Sr. No.	*Expert Role*	*Industry*	*Market*
E-1	President of a Data Quality Consultancy	Consultancy	US
E-2	Data Governance & Protection Consultant	Consultancy	India
E-3	Head of Data Operations	Software	Europe
E-4	Data Driven Technical PM	Technology	US
E-5	EMEA Head of Privacy	Financial Services	Europe
E-6	Global Head of People Data Privacy	Social Media	Europe
E-7	Data Protection Officer	Airline	Europe
E-8	Director, Supplier Data Compliance	Software	Europe
E-9	Independent Data Privacy Consultant	Consultancy	Europe/US
E-10	Data Protection & Privacy Specialist	Software	Europe
E-11	EU DPO & Privacy Compliance Manager	Data Measurement	Europe
E-12	Sr. Director, Data & Analytics	Software	Europe & US
E-13	Data Governance & Strategy Researcher	Financial Services	Europe/India
E-14	GDPR & Data Protection Consultant	Consultancy	Europe/Global
E-15	Chief Privacy Officer	Legal Firm	California/US
E-16	Senior Data Protection Specialist	Automotive	Brazil
E-17	Enterprise Data Architect	Financial Services	Canada/Holland
E-18	Data Privacy Officer	Financial Services	South Africa
E-19	Director of Data & Tech Compliance	Financial Services	Singapore

Data Analysis

Following the theme development model proposed by Vaismoradi et al. (2016), data analysis consisted of four distinct stages: initialisation, construction, rectification, and finalisation. Under the initialisation stage, the researchers focused on the transcriptions, highlighted meaningful abstractions using thematic codes, for example the occurrence of a potential concept or theme, conflicting views, and writing reflective notes. During the construction stage, the researchers classified, compared, and labelled the themes identified against the research instrument, while applying open, axial, and selective coding (Wolfswinkel et al., 2013). This coding process inductively established a set of main categories and sub-categories that visualised how the collected data portrays the identified research questions (Oates, 2005). As per Yin (2008), drawing explanations, re-checking data, and reviewing findings among third parties was also performed during this stage to ensure validity. Under the rectification stage, the researchers concentrated on streamlining the themes by excluding any redundancies and relating potential themes to established knowledge, facilitating a matrix of categories. This allowed the researchers to reflect on the data in new ways, as well as to eliminate irrelevant, overlapping, or repetitive data. As a result, the findings from the expert judgment studies consisted initially of 16 themes across the three research questions, which was subsequently reduced to 14. Lastly, as part of the finalisation stage, the focus was to analyse the areas of commonality among the respondents, and to tell the story as it was presented.

Findings

This section presents the results from the multiple judgment studies investigated. Fig. 1 presents the conceptual data compliance strategy (DCS) framework wheel for data-driven organisations that has emerged from this research. Only mechanisms that were observed multiple times, by two or more experts, formed the basis of these findings, ensuring generalisability and consistency on a conceptual level. The inner blue core, which represents strategy development, consists of five fundamental mechanisms that organisations must achieve before they can continue any further. Once these mechanisms have been addressed, organisations can progress to the next level of the DCS, which outlines the mechanisms necessary to establish the strategy. These mechanisms represent an ongoing process, one that should be continually pursued to ensure best practices. Lastly, once organisations are comfortable with addressing the issues on the secondary layer, they can proceed to the outer layer, which represents the mechanisms necessary to commit to their data compliance strategy. In answering the three research questions outlined previously, each layer outlines the emergent mechanisms that resulted from the data analysis, as evidenced through the coding samples and descriptions provided below:

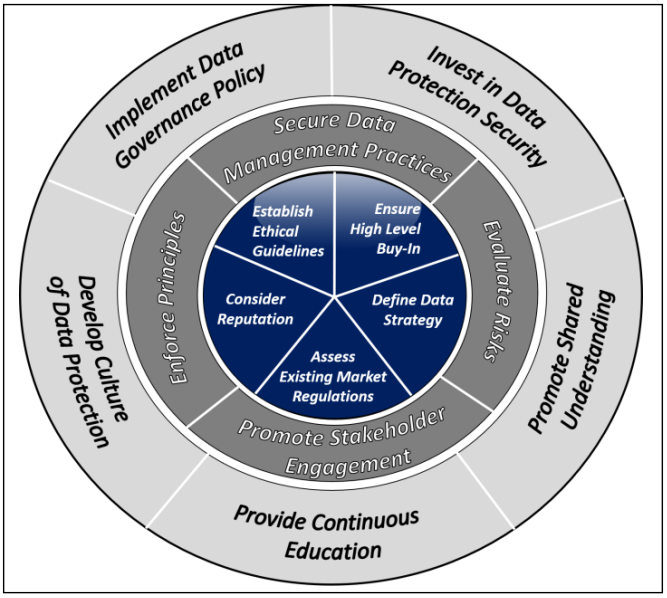

Fig. 1: Conceptual Data Compliance Strategy (DCS) Framework Wheel for Data-Driven Organisations

Phase 1: Developing a Data Compliance Strategy

Five KBDC mechanisms emerged from the data when investigating research question one. Firstly, experts were adamant that any data compliance initiative required ensuring high level buy-in from senior leadership. It was described by experts as being foundational when it comes to organisation-wide strategies, as they will need the support and funding from the leadership to make it a priority within the various teams, to assign responsibility for its development, and to ensure its delivery within a timely period: "*It needs to come from the top down… because then their leadership team will listen to them*

and take it back to their own teams" (E-10). There was a consensus among the experts that by having the support on the executive level, it focuses the organisation to recognise the level of importance being placed on these initiatives, and to subsequently get better buy-in from the different business teams across the organisation: "*Having executive sponsorship is key to champion it and push it*" (E-12). Conversely, by failing to have the support of the higher-level executives, the project will be put in immediate jeopardy, as it does not have the same level of urgency, accountability, or support required to make it a success: "*If you don't get the buy-in from your senior leadership team, you're at nothing*" (E-14). Secondly, the experts advised to define the data strategy by identifying the data being collected, utilised, and stored to support business goals. Several experts stressed the importance of understanding the data strategy of the organisation first before implementing a compliance initiative to support it: "*I had five key themes based on business goals, and I was able to show how the data strategy would underpin the business objectives*" (E-3). Caution was urged for organisations that have business models centred around functions such as sales and marketing, as these models would be traditionally focused on acquiring as much data as possible. Similarly, if the organisation relies on selling data, these models involve extensive processing of personal data, which naturally makes it more difficult to comply with data regulations when compared to organisations that handle less data: "*Business models matter. If you sell data for a living, that is going to be hard for you when you're dealing with the CCPA because you are not allowed to sell data without the consent of the individual*" (E-10). An organisation should first determine the type of business it is and the business model it is using. This will impact the necessary considerations for a global data protection strategy tailored to the organisation. Organisations must also question the value they apply to their data: "*We've started to realise the data was an asset, not even just an asset, but a high value asset*" (E-8). The strategy should be extremely clear and showcase how the organisation will prosper through its adoption.

Thirdly, it is imperative to assess existing market regulations (examples of which can be seen in Section 2.2) across the various geographies the organisation is operating in due to the variances of the regulations to which they are subjected. Some organisations have chosen to adopt a global baseline policy akin to GDPR, and then make alterations where and when local regulations differ: "*Essentially, because GDPR was first, that sets the baseline for what we have done from a compliance perspective, and now, as we see nuances across each of the countries and states, we will make the necessary changes*" (E-12). However, understanding the local nuances and the intricacies of different countries' laws should not be overlooked, even when organisations choose a gold standard baseline with which to comply: "*The difficulty if they apply the gold standard that might apply in one jurisdiction right across all their different territories, they might be at a huge regulatory disadvantage when they're in one territory*" (E-14). The differences among these laws make operating in a global environment significantly complex. It is the responsibility of the organisation to make sure they are kept apprised of these laws and incorporate changes where necessary to ensure an effective data compliance strategy. Indeed, it was recommended that when it comes to a data protection strategy, it should be predicated on from where the organisation is operating: "*You should have a strategy for GDPR compliance, for CCPA, for Canadian law, Indian law, Singapore law and so on because these laws are all different*" (E-2). Fourthly, organisations are encouraged to consider their reputations and reflect on their attitudes towards data, privacy, and data protection. Data breaches and privacy issues are a major source of concern, as they cause serious reputational damage which may have other significant consequences: "*People have also seen the damage of being found out. And if you're found out there's no going back from that. There really isn't*" (E-10). Some experts suggest that "*The only time organisations really start paying attention is when they start to see some of the sanctions that are out there and the reputational damage*" (E-15). The reputational damage from the Cambridge Analytica scandal lives on, and it is critical for businesses to reflect on their policies and learn from the mistakes of others: "*We had an exodus of people leaving Facebook after the Cambridge Analytica case, and we're seeing Apple now with their latest iOS really doubling down on privacy, because Apple is smart*" (E-10). It is vital therefore that every organisation should rigorously develop their own privacy policy to reflect how they wish their reputation to be viewed when it comes to data collection, use, and storage, and that they have established best practice policies. Apple was

outlined as being particularly effective in this regard: "*Each company has to decide for itself its own privacy philosophy and its own data protection approach. Apple has a very strong privacy image. It knows what it wants, with privacy at the forefront from its public statements, and that's the way it approaches things*" (E-5). Lastly, the establishment of ethical guidelines was also identified as vital. It is extremely important to collect the data required in an ethical way and then process it lawfully which would positively influence customer trust: "*Trust is a key component. Trust, and the ethical use of data*" (E-15). This impacts the organisations using AI or machine learning models in particular. The problem, however, is that because ethical development is not seen as something that generates revenue by most organisations, too often it can be neglected and viewed as a defensive exercise: "*Defence is the stuff you have to do even though you're not going to make money from it, so ethics falls under that category*" (E-1). Similarly, it was noted that while organisations can be compliant with the regulations they are subject to, they can still be considered to be unethical with regard to how they intend on using the data at their disposal: "*You can be completely compliant with the GDPR and still be completely unethical. The way people approach data doesn't necessarily have to just be compliant. It needs to go beyond that. You need to come at it from a do-no-harm type of approach*" (E-10). To lay solid foundations of an effective data compliance strategy, it is up to the organisation to instil best practice ethical guidelines that will reflect on their public reputation, as outlined previously: "*From an ethical perspective, you need to figure out who you want to be as a company. Is privacy and data protection a priority for you?"* (E-10). An organisation needs to discern what its ethical outlook is, which can then be used to determine its data strategy, before being subsequently applied to all their markets.

Phase 2: Establishing a Data Compliance Strategy

The data analysis revealed four primary KBDC mechanisms that were required in establishing a data compliance strategy for data-driven organisations. The first mechanism to emerge was the importance of securing robust data management practices, including data mapping, data classification, and the creation of comprehensive data retention schedules. GDPR was highlighted as driving awareness towards the importance of these techniques: "*One of the standout lessons from GDPR is the importance of data mapping and understanding what you have got*" (E-9). Some experts were adamant that it should be the first thing an organisation engages in when developing their data strategy: "*One of the things you have to have, is how you define data, and how you classify data*" (E-8). While this is perhaps unsurprising, what was unexpected was a majority of experts revealing how challenging organisations found it to get to grips with their data, with some disclosing that "*The main challenge was the amount of data we collect, identifying it, where the data is, and making sure we had that documented*" (E-11), while others described the difficulty of having to "*map every piece of data that we were getting, where it was kept, who was collecting it, who within the company was receiving that information, who they were sharing it with, and were they sharing it with another controller… It was like a spider's web*" (E-7). Difficulties further arise with the level of detail being collected about an organisation's data use, leading to the creation of metadata: "*As soon as you start tracking data, or start mapping data, you start creating metadata, in terms of data, data ownership, data regulations for security and retention etc…*" (E-17). This level of detail is required however if the ethical guidelines outlined previously are to be adhered to. Once the organisation is comfortable with the classification and mapping of data, they must then also consider the issue of data protection and retention: "*You need data protection to manage all the data protection compliance pieces. You need information lifecycle management to manage that whole lifecycle and understand retention as well*" (E-14). Considering the global trend towards increasing data protection regulations, data management should now be a core consideration for organisations. Secondly, ensuring stakeholder engagement was deemed an important, but in some cases overlooked, mechanism. Without engaging the different functions of the business in the rollout and implementation of a global data protection strategy, organisations run the risk of creating a silo mentality within the business units towards the strategy and data protection in general: "*Silos make it difficult to share data and this gets in the way*" (E-1). This was echoed by several experts, suggesting that this silo mentality creates difficulty in achieving buy-in across the different business teams in the organisation: "*There is a bit of a silo mentality about data, about how you use it, where it is, who is responsible for it, especially on the accountability*

side" (E-5), in addition to misrepresentation or confusion about how compliance is to be achieved: "*There's not enough people understanding the data, a lot of people are scared of it. People do not properly ask the right questions of the data and the organisational things you do. Silos get in the way*" (E-12). The interdisciplinary nature of data protection is the reason provided by another participant for ensuring that "*all parties are at the table*" (E-5) in this respect. Promoting stakeholder engagement is therefore paramount across the various areas to achieve synergy and cohesion among the different units due to concerns of "*privacy, security, global operations. There are so many stakeholders that need to come together for it to be successful*" (E-8) and to ultimately achieve "*better buy-in from the different business teams*" (E-3).

Thirdly, enforcing principles of data protection emerged as a common mechanism and builds on the previous themes of defining the data strategy and establishing ethical guidelines outlined in research question one. As many data regulations share common principles, most notably the GDPR and the regulations inspired by it, any global data protection strategy must be reflective of what they encompass, as argued by one expert: "*Organisations understand that they cannot go with a strategy that is not reflective of the underlying principles of GDPR*" (E-5). Several principles were detailed by the experts, including privacy by design, data minimisation, and transparency. "*We are still leveraging a lot of our privacy programme that we developed for GDPR compliance for our jurisdictions. For example, our subject access rights process which we designed for GDPR, we've now leveraged that for other countries, particularly to comply with California law in the US*" (E-11). It is up to these organisations themselves to decide on what principles they will operate under, and how they shall be enforced across the business units: "*Our Chief Technology Officer's team are setting up data principles including what we do with the data, what won't we do with the data, the data ethics guidelines etc…*" (E-10) as "*organisations must have a global brand strategy in terms of principles*" (E-14). The experts agreed that data protection principles should be built into the organisation from when data enters the organisation through its entire lifecycle, which should then be leveraged to meet future regulations across the global markets. Finally, it is imperative for the organisation to evaluate the risks in their strategy, given that the more data collected, the higher the associated risk: "*The more you collect, the more toxic it gets, and the more you use it, the more risk we accrue and then the bigger the fine, and the bigger the breach*" (E-5). This may be why many organisations are currently taking a risk-based approach when it comes to data protection, with some experts advising organisations to "*get your risk down to the lowest manageable, lowest tolerance that your business can sustain*" (E-6). While developing this strategy, it is advisable for organisations to establish a data classification system which categorises data according to the level of risk it bears to the organisation: "*It is the risk tied to data, high data will be sensitive like your credit card information, your health information etc… Then medium risk could be more around your name and your address. The low risk would just be business to business type of data*" (E-8). This is deemed mandatory and an area of serious concern according to experts, advising organisations to go above and beyond what the regulatory legislations are offering: "*You will always be better off trying to exceed what the regulatory requirements are, and you will always be better off trying to make sure that you are reducing regulatory risk as much as you possibly could*" (E-7). The level of risk organisations expose themselves to also depends on the regions they operate out of, with some jurisdictions demanding more of a risk-based approach than others, with one expert (E-18) highlighting China in particular: "*In China, gosh, that's like a minefield. There is no clarity, so you have to have a risk-based approach*."

Phase 3: Committing to a Data Compliance Strategy

In addressing our final research question, the data revealed five primary KBDC mechanisms that were required. Firstly, for the strategy to be successful the experts agreed that implementing a robust data governance policy was fundamental. One expert insisted it is essential for organisations to understand the foundations of their data and what they are dealing with before a compliance program can ever be built: "*Data governance is not compliance, it's getting your house in order. It's understanding if you're in a building, you have a set of foundations. You've got to understand what those foundations are*" (E-9). Indeed, effective data governance is at the heart of any data regulatory compliance and is seen as a "*key tenet*" (E-12) in any strategy being employed. Similarly, experts argued that without an

effective governance model, any progress or compliance the organisation hopes to achieve will prove difficult, if not impossible: "*Data governance is critical. If you don't have a strong governance process you can't bring in the strategy, all of your good work can get undone*" (E-8). Undoubtedly, the advent of GDPR has forced organisations to reassess their existing data strategies, and in most cases, re-conceptualise existing governance policies and procedures to ensure they remain compliant: "*Becoming GDPR compliant is about accountability, more than anything it's about governance, and data governance*" (E-5). Becoming compliant forces organisations to answer hard questions about what data they are collecting, but also, perhaps most importantly, why they are collecting that data: "*What data are you collecting? What are you doing with it? Who has access to it? What is your lawful basis for processing it?*" (E-15). Forming this policy builds on several steps that we have identified in both previous research questions, including risk assessment, stakeholder engagement, and data management practices. Secondly, the need to invest in data protection security has become a critical component in any organisation's data strategy with the increased prevalence of cyber threats, according to the experts interviewed: "*Data security is a driving force for data strategy*" (E-13), with others arguing that security and data go hand in hand: "*If you're going to have a data strategy, you have to talk about the security*" (E-19). This has come particularly into focus for organisations when considering the penalties being issued to those in breach of these regulatory laws: "*increasing data protection regulation has made companies look at security compliance. If you think about security breaches, you think about the heavy fines that are being given to companies like British Airways or the Marriott*" (E-12). Data-driven organisations must now reassess existing myopic mindsets that this area of responsibility is confined to one business unit, whereas in fact it commands a more diverse input from teams across the whole organisation and different levels for it to be considered successful: "*The attorneys and the people who run the corporations have a myopic view. We've seen lots of money thrown at cyber... I think the pot of resources has not been allocated appropriately. Data protection remains an add on*" (E-9). Several experts gave examples of cross-functional teams working together to ensure that their data protection strategies are workable, and that there is a shared vision across these areas as to how this level of protection is achieved: "*Understanding your data and protecting that data is synonymous. Our cyber team reports to our Chief Legal, so we work hand in hand to identify and make sure that how we treat our data complies with the law, but also that it's protected. We work very closely with our cyber team to ensure that*" (E-11). Some companies are now choosing to take a more holistic approach towards viewing data protection, but again remaining committed to integrating as many units as possible for an effective strategy execution: "*Information security, data integrity, data access etc… We are joining them together to look at it from a more integrated perspective, so we understand what our risks are from a privacy perspective from retention etc…*" (E-17). The experts were in agreement that this represents an area that needs constant attention and funding across any organisation to ensure that the data remains secure. Thirdly, the need to provide continuous education was raised as an important criterion to embed a successful strategy in the company culture, and one that was viewed as a significant challenge for most organisations: "*The challenges mostly are educational, as silly as it sounds*" (E-4). Several experts described how this is a fundamental issue with individuals across different silos, teams and jurisdictions: "*The important aspect first is educating people because people work in silos. They are so focused on their work for their day-to-day job, they don't realise that by making a copy in their system it could potentially be a regulatory issue*" (E-13). This was mapped out further by other experts presenting examples of a global workforce and not being able to trust in their output unless education was provided to them: "*You have to educate the global workforce to handle the data. You can't be looking over their shoulder every single day, particularly if you work in a multinational. You're going to have people who are on the same team, but in completely different regions*" (E-10). Most experts were surprised that although the premise seems basic at the outset, many organisations struggle with ensuring a common standard across the different departments, particularly in the event of staff turnover: "*Continuous education is the way it is going. Every time we have a new team member, it's making sure they are comfortable with the strategy. It's not even talking about GDPR, it's talking about good business practice*" (E-3). Embracing this learning paradigm reflects the culture of the organisation as well (as expanded further below), and instils its importance in the staff at the outset: "*The training is important, the education is really, really key. If you can*

get people on board from day one, then half the battle is won" (E-19). This is vital for every organisation, regardless of their size "*Educating the workforce, no matter how large or small is really, really important, particularly people working with personal data of individuals that they know how to protect it, and how to comply with the law*" (E-11). This holds true not only to ensure that the organisation is adhering to the standards laid out in terms of data management, but also to incorporate this mindset into designing new products and services: "*One of the key principles of GDPR is privacy by design and building privacy into our products. So, we try to educate our staff at the very beginning*" (E-11). The fourth mechanism to emerge focused on the promotion of a shared understanding to communicate the organisation's global data protection strategy effectively to the whole workforce. Several experts interviewed maintain that the ability to tell one cohesive story on how data is handled and protected is simply more practical and better for training purposes: "*You're telling everybody one cohesive story about what to do and what not to do with data, like what is acceptable use in your company*" (E-9). The value this offers is the level of cohesiveness it brings to the staff working across the different geographic locations, and in some cases, it can be the most difficult thing to accomplish: "*It's accessibility, just making it easy, making it super easy, super clear, super obvious. It sounds simple, but it's actually the hardest thing to do*" (E-4). This expert continued by giving the example of breaking down what a data strategy might entail, and the difficulties in translating that to a wider audience: "*Data strategy is this nebulous term. When you think about what your data strategy looks like, having a clear understanding of* 'Here's our policies for different things, here's what you can do and here's what you can't do.' *Everyone is sharing the same mindset*" (E-4). This is critical. The fundamental aim of this shared understanding is that everyone across the organisation, no matter where they are or what their roles are, knows how to interpret and enact the data strategy agreed upon: "*It gives more cohesiveness to the organisation so a worker in Cork has the same understanding as a worker in Shanghai*" (E-6). An example presented involved releasing an organisation's annual data protection training, where "*everybody globally is hearing the same thing, which means marketing teams globally are doing the same types of compliant marketing*" (E-10). The challenge for the organisation, however, is to "*bring it down to a very much common-sense language and weave its way into the day to day*" (E-3) for their employees to ensure a successful uptake of materials and learnings. Lastly, the experts advised organisations to develop a culture of data protection and stressed the importance in the "*mind shift in terms of how we need to change our processes*" (E-4) that is required in making the data strategy a success: "*If your organisation culture is not supportive enough or not nurturing enough, then you will not receive the expected output*" (E-13). Culture plays a role as early as the onboarding of a new employee. Bad habits can flourish and be passed on to subsequent new hires which raises the risk levels surrounding data in the organisation. With large numbers of employees, risk can already be high, and governance is not a silver bullet. The organisation's culture must support and nurture good data protection habits through education and avoid the 'blame culture' as this results in underreporting of compliance breaches. The culture requirements touch on several aspects, ranging from the quality of training received to engaging with peers in the company: "*The culture of the organisation plays a major role, how the new employee when they joined the organisation got onboarded, how much training they got... Whether they got good training… how they have evolved over the time, how they learn from the peers. If they have learned the bad practice from the peers. They will follow them and then they will pass it on*" (E-13). Facilitating this change of mindset can prove in most cases difficult, as many employees have become accustomed to performing their roles and responsibilities in ways that befit their individual approach to tasks: "*Ultimately whatever you do has to work in cultures, and has to take advantage of cultures. Trying to get people to see things in the same way after 30 years of experiencing them differently is impossible*" (E-1). While creating these cultures was identified as being problematic, maintaining them was also identified as being a challenge most organisations stumble on: "*It's really hard to maintain a culture that you know works*" (E-6). Regardless, it was agreed by all experts that to forgo the development of a collaborative, open culture to promote any global data protection strategy would put it in severe jeopardy: "*Culture plays a really major role in the implementation. Any strategy will not work if the implementation is not right. That is the key thing to make it a success*" (E-13).

Conclusions, Limitations, and Future Works

The research questions addressed in this paper were: (i) *What KBDC mechanisms are required in developing a data compliance strategy for data-driven organisations?*; (ii) *What KBDC mechanisms are required in establishing a data compliance strategy for data-driven organisations?*; and (iii) *What KBDC mechanisms are required in committing to a data compliance strategy for data-driven organisations?* These questions were answered by implementing a-priori theory, and testing it through several judgment studies from the perspective of data governance and compliance experts. This research develops the literature in the still infant field of forming data compliance strategies through KBDC as a theoretical lens, which we argue is of particular importance to data-driven organisations that may be subject to several data regulations depending on their global presence. This study identifies 14 emergent themes across the three research questions outlined above, which represents the main contributions of this paper, and by extension, it offers several approaches to how the study's findings can be utilised in practice to assist these organisations in implementing a robust data compliance strategy inclusive of the differing regulations, while also offering several future research directions. Firstly, this research serves to identify the strategic value of KBDC by producing a conceptual data compliance strategy framework wheel for data-driven organisations (Fig. 1). The framework presented here therefore provides organisations with an effective roadmap to facilitate the creation of their data compliance strategy across three key areas: development, establishment, and commitment. Understanding these mechanisms allows for a more microscopic view of KBDC and, by extension, a more detailed appreciation to how these resources may be developed and managed. As the online global landscape becomes increasingly competitive, businesses are realising the need to differentiate themselves from their competitors, and while there are many sources of differentiation, more recently privacy design is being looked upon for its value to customers and resulting competitive advantage for businesses. Depending on how an organisation addresses these KBDC mechanisms to ensure consumer privacy, and based on how it prepares itself for additional laws, will indicate and decide the organisation's performance for years to come. Secondly, from a practical point of view, these are original results that reveal the importance of developing KBDC mechanisms within not only data-driven organisations, but any organisation that relies heavily on data. This research serves to identify the strategic value in forming mechanisms through the KBDC perspective, as it offers clarity on what resources an organisation possesses, the components they lack, the capability they require, and the realistic approaches needed for successful execution. This is important as the majority of experts who took part in this investigation were unfamiliar with the concept of KBDC to begin with. Through the conceptual framework presented herein, practitioners are now capable of understanding immediately the nature of KBDC, along with what mechanisms are required for each stage of strategy formulation. Thirdly, the introduction of KBDC into the analysis of data strategy formulation adds a level of complexity that has not yet been empirically examined, and as such provides a sound basis for further work. To that end, the next step would be to conduct focus groups with several managers to validate and refine the conceptual framework and explore what the experts think about the practicality and usefulness of such a tool. We would also encourage future studies to empirically explore this framework further through various lines of enquiry, including, but not limited to: intervention functions for adapting existing strategies (e.g., education, training, incentivisation, persuasion, and so on), policy categories (e.g., planning, provision, communication, and so on), behaviour change techniques (e.g., social rewards, support, instruction, demonstration, and so on), or content and implementation options. While we endeavoured to achieve the highest levels of validity, accuracy, and objectivity, as is true of any research, this study has several limitations which can be addressed by future research. Given the novel approach of this research, a relatively small population size of qualitative interviewees from data governance and regulatory compliance experts was pursued, which might present generalisability limitations. As a result, our understanding of KBDC and its influence was presented by experts with experience and exposure to data compliance and regulation policies and strategies. While this research offers an initial exploration, future studies are now advised to also capture the understanding of KBDC and its mechanisms from multiple perspectives, through large-scale quantitative investigations aimed at

larger population sizes. In addition, we also encourage future research to investigate KBDC mechanisms within other data environments, including, but not limited to data-driven business models, big data analytics, and decision making.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347,* 509-514.

Aiken, P., & Harbour, T. (2017). *Data strategy and the enterprise data executive: Ensuring that business and IT are in synch in the post-big data era*. Technics Publications.

Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: An analysis of the literature. *Journal of Decision Systems, 25,* 64-75.

Arora, P. (2019). General data protection regulation – A global standard? Privacy futures, digital activism, and surveillance cultures in the global south. *Surveillance & Society, 17,* 717-725.

Barrett, C. (2019). Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? *Scitech Lawyer, 15,* 24-29.

Beckett, P. (2017). GDPR compliance: Your tech department's next big opportunity. *Computer Fraud & Security,* 9-13.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Visions and voices on emerging challenges in digital business strategy. *MIS Quarterly, 37*(2), 633-661.

Brody, M., & Nielson, B. H. (2005). Privacy, data protection and information management compliance strategies for handling security breach notifications. *Banking and Financial Services Policy Report, 24,* 1-3.

Cheong, L. K., & Chang, V. (2007). The need for data governance: A case study. *ACIS 2007 Proceedings*, 100.

Chesbrough, H., & Rosenbloom, R. S. (2002). The role of the business model in capturing value from innovation: Evidence from Xerox Corporation's technology spin-off companies. *Industrial and Corporate Change, 11,* 529-555.

Côrte-Real, N., Oliveira, T., & Ruivo, P. (2017). Assessing business value of big data analytics in European firms. *Journal of Business Research, 70,* 379-390.

Desai, V. M. (2016). Under the radar: Regulatory collaborations and their selective use to facilitate organizational compliance. *Academy of Management Journal, 59,* 636-657.

Determann, L., & Gupta, C. (2018). Indian personal data protection act, 2018: Draft bill and its history, compared to EU GDPR and California privacy law. *UC Berkeley Public Law Research Paper*.

Diamond, M. (2019). Creating a California consumer privacy act action plan. *Journal of Internet Law, 22,* 12-22.

Dremel, C., Wulf, J., Herterich, M. M., Waizmann, J.-C., & Brenner, W. (2017). How AUDI AG established big data analytics in its digital transformation. *MIS Quarterly Executive, 16.*

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal, 21*, 1105-1121.

Erickson, A. (2018). Comparative analysis of the EU's GDPR and Brazil's LGPD: Enforcement challenges with the LGPD. *Brook. J. Int'l L., 44,* 859.

Feng, Y. (2019). The future of China's personal data protection law: Challenges and prospects. *Asia Pacific Law Review, 27,* 62-82.

Garthwaite, P. H., Kadane, J. B., & O'hagan, A. (2005). Statistical methods for eliciting probability distributions. *Journal of the American Statistical Association, 100,* 680-701.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59,* 703-705.

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal, 17,* 109-122.

Greenleaf, G., & Livingston, S. (2017). China's personal information standard: The long March to a privacy law.

Gürses, S. (2014). Can you engineer privacy? *Communications of the ACM, 57,* 20-23.

Hansen, A. M., Kraemmergaard, P., & Mathiassen, L. (2011). Rapid adaptation in digital transformation:

A participatory process for engaging IS and business leaders. *MIS Quarterly Executive, 10.*

Hansen, R., & Sia, S. K. (2015). Hummel's digital transformation toward omnichannel retailing: Key lessons learned. *MIS Quarterly Executive, 14.*

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data – A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management*, *36*(10), 1382-1406.

Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. *MIS Quarterly Executive, 15.*

Holotiuk, F., & Beimborn, D. (2017). Critical success factors of digital business strategy.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Mis Quarterly*, 19-33.

Illman, E., & Temple, P. (2019). California consumer privacy act: What companies need to know. *Bus. Law., 75,* 1637, 1640.

Janssen, M., van der Voort, H. & Wahyudi, A. (2017). Factors influencing big data decision-making quality. *Journal of Business Research, 70*, 338-345.

Kammler, F., Hagen, S., Brinker, J., & Thomas, O. (2019). Leveraging the value of data-driven service systems in manufacturing: A graph-based approach.

Knox, S., & Burkard, A. W. (2009). Qualitative research interviews. *Psychotherapy Research, 19,* 566-575.

Kohli, R., & Johnson, S. (2011). Digital transformation in latecomer industries: CIO and CEO leadership lessons from Encana Oil & Gas (USA) Inc. *MIS Quarterly Executive,* 10.

Kumari, V., & Chakravarthy, S. (2016). Cooperative privacy game: A novel strategy for preserving privacy in data publishing. *Human-Centric Computing and Information Sciences, 6,* 1-20.

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security, 6,* 323-331.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Loi, M., Heitz, C., Ferrario, A., Schmid, A., & Christen, M. (2019). Towards an ethical code for data-based business. 2019 6th Swiss Conference on Data Science (SDS), IEEE, 6-12.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.

Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering, 57,* 339-343.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mcafee, A., Brynjolfsson, E., Davenport, T. H., Patil, D., & Barton, D. (2012). Big data: The management revolution. *Harvard Business Review, 90,* 60-68.

Mcintosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2,* 2333393615597674.

Merrick, R., & Ryan, S. (2019). Data privacy governance in the age of GDPR. *Risk Management, 66,* 38-43.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93,* 96-105.

Morgan, D. L. (1997). *The focus group guidebook*. Sage Publications.

Nunan, D. (2020). *Research in the 2020s: From big data to bigger regulation.* UK, London, England: SAGE Publications Sage.

Oates, B. (2005). *Researching information systems and computing.* Sage Publications: Great Britain.

Palvia, P., Mao, E., Salam, A., & Soliman, K. S. (2003). Management information systems research: What's there in a methodology? *Communications of the Association for Information Systems, 11,* 16.

Patnaik, P. (2020, July 24). Who controls citizens' data? Personal data protection bill must empower an independent and robust data protection authority. *The Times of India*.

Pernot-Leplay, E. (2020). China's approach on data privacy law: A third way between the US and the EU? *Penn State Journal of Law & International Affairs, 8.*

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, 4*(1).

Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy: An experiment into the competitive

advantage of collecting less personal information. *Electronic Commerce Research, 13,* 423-455.

Royakkers, L., Timmer, J., Kool, L., & Van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology, 20,* 127-142.

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly, 61,* 294-308.

Shamim, S., Zeng, J., Khan, Z., & Zia, N. U. (2020). Big data analytics capability and decision making performance in emerging market firms: The role of contractual and relational governance mechanisms. *Technological Forecasting and Social Change, 161*.

Shamim, S., Zeng, J., Shariq, S. M., & Khan, Z. (2019). Role of big data management in enhancing big data decision-making capability and quality among Chinese firms: A dynamic capabilities view. *Information & Management, 56*(1).

Sharma, G. D., Yadav, A. & Chopra, R. (2020). Artificial intelligence and effective governance: A review, critique and research agenda. *Sustainable Futures, 2***.**

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 989-1015.

Svahn, F., Mathiassen, L., & Lindgren, R. (2017). Embracing digital innovation in incumbent firms: How Volvo cars managed competing concerns. *Mis Quarterly, 41*.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security,* 5-8.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28,* 1319-1350.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18,* 509-533.

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice, 6*(5), 100-110.

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. *European Journal of Information Systems*, *25,* 77-89.

Vidgen, R., Shaw, S., & Grant, D. B. (2017). Management challenges in creating value from business analytics. *European Journal of Operational Research, 261,* 626-639.

Voigt, P., & Von Dem Bussche, A. (2017). Enforcement and fines under the GDPR. *The EU General Data Protection Regulation (GDPR)*. Springer.

Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: Providing a competitive advantage for US companies. *American Business Law Journal, 56,* 287-344.

Wang, J., & Yu, W. (2017). Government performance in the eyes of business: An empirical study of smes in China. *Public Performance & Management Review, 40,* 701-721.

Webber, R. (2020). COVID-19 and race: Protecting data or saving lives? *International Journal of Market Research, 62,* 528-537.

Weiner, N. & Weisbecker, A. (2011). *A business model framework for the design and evaluation of business models in the internet of services*. 2011 Annual SRII Global Conference, 2011. IEEE, 21-33.

Wilson, K. J. (2017). An investigation of dependence in expert judgement studies with multiple experts. *International Journal of Forecasting, 33,* 325-336.

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy, 42,* 425-440.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22,* 45-55.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(1).

Yin, R. (2008). *Case study research: Design and methods* (4th ed.) London: Sage Publisher.

Zheng, S., Zhang, W., & Du, J. (2011). Knowledge-based dynamic capabilities and innovation in networked environments. *Journal of Knowledge Management*, *15*(6), 1035-1051.