The Digital Traveller: Data Ethics and Data Governance in Tourism and Hospitality

Journal:	*Journal of Consumer Marketing*
Manuscript ID	JCM-12-2020-4278.R2
Manuscript Type:	Regular Paper
Keywords:	digital privacy, data ethics, data governance, tourism, hospitality, COVID-19

The Digital Traveller: Implications for Data Ethics and Data Governance in Tourism and Hospitality

Abstract:

Purpose: Big data and analytics are being increasingly used by tourism and hospitality organisations (THOs) to provide insights and to inform critical business decisions. Particularly in times of crisis and uncertainty data analytics supports THOs to acquire the knowledge needed to ensure business continuity and the rebuilt of tourism and hospitality sectors. Despite being recognised as an important source of value creation, big data and digital technologies raise ethical, privacy, and security concerns. This conceptual paper suggests a framework for ethical data management in tourism and hospitality designed to facilitate and promote effective data governance practices.

Design/methodology/approach: The paper adopts an organisational and stakeholder perspective through a scoping review of literature to provide an overview of an under-researched topic and to guide further research in data ethics and data governance.

Findings: The proposed framework integrates an ethical-based approach which expands beyond a mere compliance with privacy and protection laws, to include other critical facets regarding privacy and ethics, an equitable exchange of travellers' data, and THOs ability to demonstrate a social license to operate by building trusting relationships with stakeholders.

Originality: This study represents one of the first studies to consider the development of an ethical data framework for THOs, as platform for further refinements in future conceptual and empirical research of such data governance frameworks. It contributes to the advancement of the body of knowledge in data ethics and data governance in tourism and hospitality and other industries, and it is also beneficial to practitioners, as organisations may use it as a guide in data governance practices.

Keywords: digital privacy, data ethics, data governance, tourism, hospitality, COVID-19

1. Introduction

The rapid development and adoption of technology represents a key megatrend and driving force in business (Kraus *et al.*, 2019), as new technologies enhance customer service performance, and enable organisations to conduct better research on customers, competitors, and the broader market environment (Foroudi et al., 2017). This tremendous impact of technology on business is ever more prominent in the tourism and hospitality industry (Yeoman, 2012, 2018; Yeoman and McMahon-Beattie, 2018), which provides the highest number of products and services sold online in most countries (Navío-Marco *et al.*, 2018). Technological developments not only create changes in consumer behaviour, but they also generate changes in the way tourism and hospitality organisations (THOs) interact with their customers, i.e., travellers (Yallop and Séraphin, 2020; Urquhart, 2019). Nowadays, business disruption is further fuelled by technological advances, as organisations in the tourism and hospitality sectors can use new ways afforded by technology to reach their customers, and as a result, reshaping ways of engagement with customers to aid service and convenience (Boumphrey, 2019; Yallop and Séraphin, 2020).

Moreover, the recent COVID-19 pandemic has generated a prevalent and severe disruption of THOs globally (Jamal and Budke, 2020). Hirt *et al.* (2020) suggest that a next wave of disruption will occur, with a significant change in customer behaviours and business models (Kraus *et al.*, 2019). Without doubt, the sudden changes in the way THOs need to rethink the way they do business to survive in times of crisis is hastening the existing wave of disruption. Indeed, a recent report advised that COVID-19 will create lasting changes in consumers' attitudes and behaviour which organisations will have to cater to (Stalenis *et al.*, 2020). Even more so, due to the severe impacts of the global COVID19 pandemic on the tourism and hospitality industry worldwide, these consumer behaviour changes will be felt more acutely, with organisations having to quickly adapt to these changes in order to survive and maintain

competitive advantage (Yallop and Aliasghar, 2020). More than being just a disruptive event, the outbreak of COVID-19 is also perceived as an opportunity to rethink, adapt, and alter practices in the industry (Gossling *et al.*, 2020; Lapointe, 2020; Séraphin, 2020).

Likewise, a series of key technological developments significantly impact tourism and hospitality and related sectors (Getz, 2012), and may also have an important role in ensuring business continuity and the rebuild of tourism and hospitality sectors post COVID-19, through adoption of technology innovation intended to support survival and recovery strategies in the sector (Nanni and Ulqinaku, 2020).

Indeed, recent travel and tourism industry reports suggest that in the next five years technological advances will have a significant impact, with big data and analytics being the most important technology to impact the industry (Bremmer, 2019; UNWTO, 2020). Certainly, in the tourism and hospitality industry, traveller data and information are crucial to organisations; data and data analytics are being increasingly used by organisations to provide insights and to inform critical business decisions (Yang *et al.*, 2019). More so, recent reports suggest that, due to the unprecedented challenge posed by the pandemic, the travel, tourism and hospitality sectors will witness two main transformation areas in which digital technologies will shape the future of the sectors, namely touchless travel and digital health passports, henceforth the rise of the "digital traveller" where more personal data and information, cryptographic data and even medical/health data may be required from travellers (Leong, 2020). These emerging digital technologies are being supported by digital systems such as the World Economic Forum's 'Known Traveller Digital Identity' initiative (WEF, 2020).

However, despite its many benefits, technology can also have negative impacts on consumers because it can jeopardise people's autonomy and can breach their rights (Blakesley and Yallop, 2019; Martin *et al.*, 2020; Wu *et al.*, 2019; Laczniack and Murphy, 2006). The

pledge of better services and improved quality brought by data-driven technologies comes with concerns regarding ethical practices of the entities to which consumers provide their data freely every day (Digital Future Society, 2019). Thus, technology has significant consequences for privacy and security (Blakesley and Yallop, 2019; Conger *et al.*, 2013; Culnan and Bies, 2003; Sarathy and Robertson, 2003) and, consequently, it has significant implications for any data governance frameworks developed and implemented by organisations in ensuring ethical practices. Moreover, technology experts are of the opinion that, because of the fast move towards more insightful, automated, and data-driven organisations, the importance of data ethics and governance will grow further in the future (Harvard Business Review Analytic Services, 2019).

Although privacy and security issues are relevant to a range of industries, they are particularly salient in the tourism and hospitality sectors, especially because in recent years tourism and hospitality products and services have become the largest category of products and services sold over the Internet in most countries (Navío-Marco *et al.*, 2018). Moreover, if compared to other sectors, the amount of consumer personal data involved in business operations is significantly larger in tourism and hospitality, a highly information-intensive industry (Tussyadiah *et al.*, 2019). Thus, not only do travellers need to process a significant amount of information (pre-trip planning, in-destination experiences, post-trip evaluation and data sharing), but they are often required to give up personal information in exchange for services to enable and enhance their travel experiences (e.g., booking processes, visa applications, access to discounts, etc.). The specific significance of consumer privacy research in tourism and hospitality has been recently stressed by Bahar *et al.* (2021) who emphasise the need for more research in this sector due to the sector's prominent particularities as a data-driven industry, with strong links with the digital environment (Bahar et al, 2021). In addition, although many service industries have been disrupted by digitalisation particularly during the

pandemic, tourism & hospitality consumers have been most strongly disrupted (Bahar et al., 2021), with Bart *et al.* (2005) also indicating the high information risks attached to travel sectors, for which data privacy is of utmost importance compared to most other industries and sectors (Bart *et al.*, 2005).

Against this backdrop, this study focuses on the issues pertaining to data ethics and data governance in the tourism and hospitality sector, an under-researched area, and the subsequent implications for consumer/traveller data. The paper's main objective is to develop a conceptual framework for ethical data management and data governance in tourism and hospitality so that ethical and security considerations are carefully thought of in the collection, storage and analysis of tourism and hospitality data and information, in the best interests of travellers/customers and all other stakeholders involved (i.e. THOs and their employees, government, authorities, industry associations, complementary industries and sectors, the general public, etc.). This is important, as data governance and tourists' privacy has somewhat slight coverage in the UNWTO Global Code of Ethics for Tourism, with the code pointing towards the fact that international tourists are not to be discriminated by any means compared to domestic tourists in terms of collected personal data and information, especially when stored electronically. In this context, the proposed framework can become a useful tool for the various actors of the tourism and hospitality industry, who, nowadays practically depend on operating with big data.

This research responds to recent calls for more conceptual studies in consumer data ethics and data governance in business (see Yang *et al*., 2019), tourism and hospitality (see Bahar *et al.*, 2021; Yallop and Séraphin, 2020; Yallop and Aliasghar, 2020;), and further conceptual research in generating a deeper understanding of business stakeholders' convergence in safeguarding consumer data (Martin *et al.*, 2020). This study contributes to the advancement of the body of knowledge in consumer data ethics and data governance by developing a holistic

ethical data management and data governance framework that expands beyond a mere compliance-based approach to an all-inclusive ethical and socially responsible approach to data governance. Moreover, the paper's contributions are aligned with the Marketing Science Institute's research priorities for 2022-2024 concerning the increasing importance of preserving consumers' privacy (MSI, 2020).

The framework developed in this paper seeks to guide THOs on ways to manage their data assets responsibly and maximise the value of big data, therefore, to facilitate and promote good practice regarding data. The development of a framework for ethical data management and data governance in tourism and hospitality is important, as the lack of a framework for good practice may limit the scope, quantity, and quality of research in a specific area, may lead to researchers' and practitioners' disengagement from the area (Canosa, *et al.*, 2018a, b), which in turn may also hinder the reliability and validity of research carried in the specific area (Khoo-Lattimore, 2015). Likewise, the development and application of sound frameworks and good practice in the industry may inform responsible education management, and therefore, may ensure the nurturing of responsible managers and practitioners (Séraphin and Yallop, 2020; Séraphin and Vo-Thanh, 2020; Visser, 2015). Beyond the tourism and hospitality realm, the original stakeholders framework developed in this paper has the aim to provide a platform for different organisations and policy makers to shape and refine privacy norms and policies to address digital privacy concerns in online services.

The framework does not provide an exhaustive account of all possible ethical considerations, but a scoping review of literature, which has the purpose to identify the scope and extent of existing research on a topic and to provide an exploratory overview of the topic, in this case data ethics and data governance (Rasoolimanesh *et al.*, 2020). Scoping reviews are increasingly used in the social sciences (Moher *et al*., 2015), including tourism studies, in order

to provide an overview of an under-researched topic and to guide further research in the area (Rasoolimanesh *et al.*, 2020).

Therefore, from a methodological point of view, this study employed a problem-focused approach (Gilson and Goldberg, 2015) based on a scoping and topic-centre review (Hammond and Wellington, 2013) of academic literature as well as business/industry literature and reports as means of guiding the development of a conceptual framework. Consequently, the conceptual model developed is based on existing knowledge and theory reviewed in this paper, by bridging existing theories, and broadening the scope of our thinking (Gilson and Goldberg, 2015) around data ethics and data governance. To conduct a scoping and topic-centre literature review, studies on data ethics and data governance were identified through a comprehensive web-search of relevant terms (e.g., data privacy, data ethics, data security, data breaches, data governance, data compliance, big data, data sharing) using several electronic databases (e.g., Business Source Complete (EBSCO), Passport, Emerald Fulltext, Web of Science, Google Scholar), other relevant industry and practice-orientated business and governmental reports (e.g., IBM, Gartner, ICO, PwC, European Commission, Privacy Commissioner), and a review of reference lists from the academic and industry articles identified. Predominantly, the search covered literature published in the last two decades (2000-2020) which reflects the growing interest in privacy issues due to the continued growth in the use of mobile internet devices (Blakesley and Yallop, 2019) and the subsequent implications to customer privacy (Akhter, 2014), and it focused on the contexts of digital consumers, marketing, and tourism and hospitality more specifically.

To our knowledge, this study represents one of the first studies to consider the development of an ethical data framework for THOs, as a platform for further refinements in future conceptual and empirical research of such data governance frameworks.

To achieve the study's objective the paper begins with a brief review of key theoretical concepts related to big data, digital privacy and security, personal data sharing, data ethics and data governance as the underpinnings of this study. It continues with the introduction and discussion of the proposed conceptual framework of data governance to then draw conclusions and direct towards further research avenues in data ethics and governance in tourism and hospitality.

2. Big data in tourism and hospitality

Since the 1990s, data and data analysis have been extensively used in business decision-making (Al-Ruithe *et al.*, 2019). An increased amount of structured and unstructured data is gathered and used by organisations to maintain and gain competitive advantage (Nunan and Di Domenico, 2013). This affluence of digital data (Barocas and Nissenbaum, 2014; Wang, 2013) is being created by consumers online by means of mobile devices use (Shilton, 2009), a wealth of data shared on social networking platforms which is available online (Nov, Naaman and Chen, 2010), and data deliberately gathered by THOs booking systems or systems of customer relations management (Yallop and Séraphin, 2020).

In volatile and uncertain business environments and, more specifically, in the current context of COVID-19, big data are increasingly required to acquire knowledge in the tourism and hospitality industry in order to reduce the risks associated with uncertainty and to support policy decisions in mitigating the effects of crises in tourism destinations (Williams and Baláz, 2015; Gallego and Font, 2020).

The concept of Big Data has been established because of the wealth of data and data processing on a large scale (Blakesley and Yallop, 2019). Big Data is defined by Mayer-Schönberger and Cukier (2013) as data collection done on a large scale to obtain new insights

and create value for markets and organisations. Big data refers to data obtained from several internal and external data sources and displays four key dimensions: (1) "volume" (the large volume of data that has been generated and stored), (2) "variety" (data can be sourced from a large number of structured, semi-structured, and unstructured data sources), (3) "velocity" (the speed at which data are generated and need to be processed in order to meet the demands), and (4) "veracity" (Laney, 2001; IBM, 2014a). "Veracity" is the fourth dimension, which was added to the other three dimensions to address issues relating to trust and uncertainty in the analysis of data (Ward and Baker, 2013).

Another significant characteristic of big data is "value", represented by the validity and usefulness of data. When data offers insights, it becomes a value differentiator and an important source of competitive advantage (Gupta and Gupta, 2016; Addo-Tenkorang and Helo, 2016). Big data is valuable to THOs, as they assist in improving business decisions, and in deriving research and analytics insight (IBM, 2014b; Fitzgerald *et al.*, 2016). In particular, the use of big data allows THOs to enable service personalisation, convenience, and generally, achieve competitive advantage (Evans, 2020; Yallop and Séraphin, 2020). At the same time, effective employment of big data analytics drives cost and process efficiencies, business strategy and change (MicroStrategy, 2018). Yallop and Séraphin (2020, p. 2) provided representative examples of how big data and analytics are being utilised in tourism and hospitality, from revenue management, marketing purposes, to customer experience and reputation management. More recently, due to the challenges posed by COVID-19, big data and analytics play a major part in forecasting in tourism and hospitality, for the purposes of early detection of reactivation of tourism markets, and monitoring of markets in real time to enable appropriate actions by adjusting THOs' strategies and policy decisions (Gallego and Font, 2020), and for timely decision-making to ensure health and safety (Sigala, 2020).

However, although big data is seen as valuable, in the academic literature there are also wider privacy and ethical issues about it (Blakesley and Yallop, 2019; Barocas and Nissenbaum, 2014; Richards and King, 2014; Román, 2007; Yallop and Séraphin, 2020; Petrescu *et al*., 2020; Frik and Gaudeul, 2020), along with issues about security (Nunan and Di Domenico, 2013), and data breaches (Mayer-Schönberger and Cukier, 2013), which have significantly increased in recent years in tourism and hospitality. These ethical concerns around personal data sharing, data privacy and security will be addressed next.

3. Digital privacy and data security in tourism and hospitality

Since the proliferation of the Internet, data privacy has been an important research topic in marketing. According to Martin and Murphy's (2017) comprehensive examination of privacy-related scholarly research in marketing, privacy has been commonly examined from two main perspectives: assessing consumer privacy concerns and depicting the factors that drive consumers' willingness to disclose information. Marketing research has also emphasised the influence of perceived data privacy on consumer outcomes (Eastlick et al., 2006; Fortes and Rita, 2016; Phelps et al., 2001), with main findings revealing that privacy issues significantly impact consumers attitudes and intentions towards organisations and brands.

Personal data is data that relate to a person who can be identified from those data or those data and other information (ICO, 2015). Privacy is a subjective term because it is context-dependent, i.e., dependent on "the characteristics of the environment in which an individual happens to be at a given time" (Masur, 2018, p. 312), and has been defined in various ways across different disciplines (Ioannou *et al.*, 2020), therefore lacking a common definition. Digital privacy definitions are also vague, scholars often having to resort to different theories to support its definition (Ashworth and Free, 2006). What remains certain though is that digital

privacy has become a rising concern due to the growth of social media, e-commerce and online surveillance termed as "surveillance capitalism" (Zuboff, 2015) or "data capitalism" (West, 2019), which is seen as a system of information accumulation by which organisations aim to anticipate and change consumer behaviours as a means to create revenue and market control (Zuboff, 2015; Blakesley and Yallop, 2019; Hall and Ram, 2019). Nevertheless, a clear and relevant definition of digital privacy is that provided by Clarke (1999), who describes digital privacy as people's interest in maintaining a personal space, without interference from other people or organisations. However, with the increase in online consumer activity and with organisations using the internet of things and data analytics to gain competitive advantage through product and service personalisation, recent consumer marketing research highlights important subsequent problems such as data privacy, security, and significant issues of personally identifiable data during the analytic procedures (Petrescu *et al*., 2020). Indeed, as Aguirre *et al*. (2016) suggested, organisations must use consumer data and information in a strategic manner to balance the personalisation-privacy paradox.

In tourism and hospitality service personalisation is essential (Volchek *et al.,* 2020; Morosan and DeFranco, 2015) – digital technologies and digital connectivity are the mechanisms driving these industries forward (Tanti and Buhalis, 2017; Volchek *et al.*, 2020) and so, to facilitate and ensure a high degree of service personalisation and convenience that allows THOs to gain competitive advantage, the collection of personal data is key. Collection of personal data that provide a good understanding of consumer attributes and lifestyles supports THOs in ensuring the provision of appropriate and desirable service products to their consumers. For this purpose, a wealth of personal data and information is being gathered by THOs, and many organisations have already evolved in their digital endeavours (WEF, 2020). However, as Volchek *et al.* (2020) pointed out, travellers' awareness of personalisation through use of their personal data to recognise their context and to filter out information that is not

relevant to this context, motivates travellers to pay more attention to privacy and security issues.

Data and information collected may include, for example, particulars of travellers' interests, identity attributes or personally identifiable information (PII) such as date and place of birth and physical characteristics, dependant family information, as well as additional data that THOs can use for marketing purposes, sales and customer analysis (Yallop and Séraphin, 2020). In an increasing online and digital world, such additional data also comprise lifestyle information (e.g., hobbies, travel history and preferences), location data and browsing habits. Further, technological advances have created more opportunities for THOs to collect travellers' data, such as automated check-in kiosks collecting biometric data at airports, real-time surveillance systems for safety and security purposes, and recent innovations in artificial intelligence (AI) have led to the use of automated systems such as intelligent personal assistants (robots) able to learn the interests and behaviour of travellers and respond appropriately (Tussyadiah *et al.*, 2020; Yallop and Séraphin, 2020).

Also, in Europe, tourism platforms such as Airbnb, Booking.com, Expedia, and TripAdvisor have recently signed a data-sharing deal with the European Commission, which claims to enable public authorities to better understand the development of the "sharing economy" (or else called the "collaborative economy" covering industries such as tourism, hospitality and transport, which represents a significant part of the European economy – 21% of EU citizens used a website or app to book accommodation in 2019) and use this data as evidence-based support for policy decisions and regulations (Hellard, 2020).

In addition, due to the risks posed nowadays by COVID-19, there is increased support for the effective sharing and managing of traveller's health information and other data, with digital identity solutions meant to assist organisations, health and government authorities in the

implementation of tracing processes intended to help monitor people movement. However, although such data initiatives are claiming to respect individual's anonymity and privacy laws (Pollina and Busvine, 2020; Hellard, 2020), data privacy experts point out that there are major risks to privacy and that sharing such sensitive data is problematic, and any new surveillance and contact tracing software solutions employed by organisations must be secure and must protect personal privacy (Brough and Martin, 2020; Macdonald, 2020; Pollina and Busvine, 2020).

Moreover, in a coronavirus-stricken world, undoubtedly, vaccination passports seem like a desirable solution needed to revive the tourism industry, which is estimating more than US$1 trillion in losses due to COVID-19 (UNWTO, 2020). A vaccination passport is likely to include the name and date of birth of the traveller, date and type of vaccinations, or details about a recent test or recovery, allowing consumers to travel, enter business establishments such as gyms, hotels, and restaurants, and attend events (Dare, 2021; Weissinger, 2021). It should provide a secure system that protects consumers' privacy. However, vaccination passports, as with any digital system, creates several challenges, including how best to ensure security and privacy, and to get consumers to trust the verification systems (Parry, 2021; Weissinger, 2021). And like with other COVID-19 tracing apps, people are concerned about government and private-sector data surveillance, as vaccine passports apps may link identity to personal health information, and may be used to establish detailed personal profiles, including movement patterns (Weissinger, 2021).

Commonly, the governance of individuals' personal data is the responsibility of national independent authorities. For example, in the UK, the Information Commissioner's Office (ICO) affords data protection to consumers online through the Data Protection Act (UK Government, 2018) and the General Data Protection Regulation (GDPR). The GDPR has a significant impact on international data flows far beyond the European Union (EU) and

provides for different tools and guidelines to transfer personal data between countries only if an adequate level of data protection is guaranteed. In EU countries data protection authorities oversee the enforcement of data protection laws, provide expert advice on data protection issues, and handle complaints regarding violations of the GDPR and the relevant national laws (European Commission, 2020). Similarly, in New Zealand the Office of the Privacy Commissioner (OPC) works to protect personal data through the recently revised Privacy Act 2020, which has the purpose to promote people's confidence that their personal data and information is secure and will be treated properly by organisations (Privacy Commissioner, 2020).

When sharing personal data and information online, travellers may have to overcome their data disclosure risks' perceptions. Organisations can reduce consumer concerns by encouraging trust (Frik and Gaudeaul, 2020), and studies investigating considerations that influence consumers' willingness to share data online suggest that key factors are trust (e.g., trusting the organisation (Blakesley and Yallop, 2019), hence the online service provided such as, for example, the online hotel app used; trusting the digital technologies used (Tussyadiah *et al.*, 2020)); consumers' perceived data sensitivity (Weydert *et al.*, 2020); consumers' preference for privacy (Hunter and Taylor, 2020), and the overall value of information disclosure (Morosan and DeFranco, 2015; Blakesley and Yallop, 2019). National independent authorities' efforts (such as the ICO) focus on generating trust in the manner personal data are collected, used, and shared online, and increasing accountability and transparency in the processing of data (McQuater, 2018; Blakesley and Yallop, 2019).

As noted, privacy in tourism and hospitality has been a main data issue and concern for both scholars (Ioannou *et al.*, 2020; Hall and Ram, 2019; Pizam, 2013) and organisations for the past few years. The number of data breaches is rising and affecting the security of customers' data (Ameen *et al.*, 2021). This concern has been exacerbated because of recent

high-profile data breaches (Armerding, 2018; PwC, 2016, 2017). A key example is the Marriott International data breach, a significant data breach that has impacted the organisation and its customers. This data breach affected approximately 500 million customers worldwide – personally identifiable information was compromised, and credit card data of over 100 million customers were stolen (Armerding, 2018; Yallop and Séraphin, 2020).

Recent industry surveys and reports have revealed that, worldwide, 49% of organisations expressed the view that the key concerns held by organisations are about data privacy and security (MicroStrategy, 2018). These concerns have become more evident at present due to the additional challenges posed by the global pandemic. Indeed, more recent research has identified that in the last two weeks of March 2020 alone the number of COVID-19-related cyber-attacks has increased significantly from a few hundred to as high as over 5,000. On average, more than 2,600 COVID-19-related cyber-attacks on Internet users (including phishing emails, malicious website domains, misleading "health and safety" emails, disinformation spreading viruses that can produce a range of damages to a system: ransomware, keyloggers or other types of personal information gathering and online scams) took place each day (Continuity Central, 2020). Similarly, 70% of business decision-makers found data security to be a difficult task, which is not surprising considering that a significant amount of data that organisations collect, generate and store is often sensitive or private client data (Masergy, 2020).

Since cyber-attacks have become a significant concern in tourism and hospitality, studies that addressed issues concerning data security and data breaches have focused on evaluating the impacts of data and information security issues on THOs and their customers (Chen and Jai, 2019; Kim *et al.*, 2013) and less on ways to avoid and pro-actively counteract such data security issues. For this reason, this study focuses on the development of an ethical data management framework and data governance for THOs. This is important because, from

previous studies, it becomes evident that if travellers perceive that the THO involved in the data breach has had a high level of responsibility in protecting their data and information, travellers' trust and their intention to re-visit the destination will decline substantially (Chen and Jai, 2019).

4. Data ethics and data governance

Data ethics defines the value judgements organisations make when gathering, analysing, and distributing data, and involves a comprehensive knowledge of data protection laws, and the appropriate use of new technologies (UK Government, 2018b). These parameters entail a thorough understanding by organisations of compliance requirements in relation to data use and management. Data ethics, security, and privacy represent a prime concern when collecting, sharing, storing, and utilising big data by organisations (Yang *et al.*, 2019). Key ethical challenges in the use of big data for organisational purposes are related to the boundary between public good and private good (data), privacy and confidentiality, transparency, equity of access; and informed use of information (Tam and Kim, 2018). With the increased trends in the use of big data, analytics, and personalisation, a key concern is the challenges big data present to maintaining privacy of personal data and information (Bennett, 2019). The answer is a strong data governance framework which is developed to increase the accuracy, integration, access, security, and management of data across the organisation, and to manage its digital assets (Yang *et al.*, 2019).

Data governance represents a set of policies and procedures implemented by organisations to manage data (Yallop and Séraphin, 2020), and it refers to the "exercise of authority and control over the management of data" (Abraham *et al.*, 2019, p. 424). Data governance frameworks are frameworks developed to manage data as an important strategic asset

(Abraham *et al.*, 2019), which offer the right sets of data and actionable insight for business decision-making (Riggins and Klamm, 2017). The key goal of data governance frameworks is to produce competitive advantage through a holistic approach to crucial organisational data (Abraham *et al.*, 2019).

Although the topic of data governance is rising in importance, with several studies and previous literature aiming to develop data governance frameworks in various disciplines and sectors, the topic is fragmented (Abraham *et al.*, 2019). Earlier scientific and practice-based studies and reports on data governance suggest that research and publications on traditional data governance approaches concentrate on specific aspects of data governance, with a strong focus on issues relating to the quality of data, data lifecycle, security, and compliance (Yang *et al.*, 2019; Abraham *et al.*, 2019; Ballard *et al.*, 2014; Otto, 2011; Tallon *et al.*, 2014) and less on privacy and ethical aspects of big data (Yang et al., 2019). Similarly, such previous research consists of literature reviews related to data governance (Abraham *et al.*, 2019; Brous *et al.*, 2016; Lee *et al.*, 2017; Rasoulli *et al.*, 2016), albeit these reviews focus on limited areas of data governance, such as cloud data governance (Al-Ruithe *et al.*, 2019) or agile capabilities of data governance (Lillie and Eybers, 2019), with limited focus on and/or consideration of other conceptual areas (Abraham *et al.*, 2019).

And so, while traditional frameworks for data governance have been studied before (i.e., frameworks that mainly focus on data quality, compliance, and the management of traditional structured data sets rather than unstructured, high-volume, high-variety and high-velocity data), Yang *et al.* (2019) contend that there is a dearth of big data governance frameworks in the literature, and the existing ones are limited as they fail to consider big data environments that attract major challenges in terms of ethical considerations around big data privacy, transparency, and other ethical aspects of data processing by organisations. Therefore, the development of a holistic ethical data management and data governance framework that, in

addition to compliance-based concerns also consider ethical and social responsibility issues more thoroughly, becomes important. In addition, studies in tourism and hospitality are yet to examine ethical ways of managing data and effective data governance frameworks that may be employed by THOs to ensure ethical data management practices. Although many service industries have been disrupted by online technology, the tourism and hospitality industry has been one of the earliest to be introduced to digital platforms, and one of the most strongly disrupted by digitalisation (Bahar et al, 2021). Researchers contend that data privacy is noticeably more important in tourism and travel than in other sectors, as the frequent practice of providing personal information required for travel reservations and other customer management procedures exacerbate information risk for customers (Bart et al, 2005). Consequently, since online integration and data privacy issues are highly prevalent in this industry, tourism and hospitality provides a rich context for research into the phenomena of data governance and data privacy.

This paper aims to examine ethical ways of managing data and effective data governance frameworks, with the intent to generate more debates and discussions around best ways to manage and govern data in THOs. This aspect becomes important, particularly in times of crisis and uncertainty due to COVID-19, when both organisations and travellers become that much more vulnerable and risk adverse, and at a time when digital privacy and ethics are top strategic technology trends (Panetta, 2018). As Janeway (2012) argued, under uncertainty, it is crucial to do the right things instead of doing things right. Indeed, as Yallop and Aliasghar (2020) note, particularly during challenging times of crisis such as the pandemic, organisations must focus on the increasing data privacy and security concerns and develop data governance frameworks that effectively safeguard stakeholders' data and information.

Furthermore, as pointed out by Panetta (2018) and Yallop and Séraphin (2020), discourses regarding privacy must be based on trust and ethics and should move from compliance-based

questions to questions with a more ethical connotation, demonstrating a stronger concern about whether the organisation is indeed doing the right thing or not, even more so during the pandemic. Hence, addressing the increasing concerns about privacy and security of travellers' data becomes important for THOs – they must further their focus on the development of effective frameworks for data governance that expand past a simple compliance with current data privacy laws in order to guarantee data security and protection for travellers and all other stakeholders.

Therefore, an effective data governance framework in tourism and hospitality would need to entail a holistic approach integrating good practice, not only in regard to data computing techniques and information assurance that drives efficient and competent business decisions (i.e. practices that comply in their entirety with data privacy and protection laws and policies), but also in relation to ethics (i.e. ethical practices). The next section of this paper proposes a framework for ethical data management and data governance in tourism and hospitality, a framework that, different from previous frameworks, incorporates an ethical-based approach and therefore expands beyond solely compliance-based approaches to data governance.

5. Proposed framework for ethical data management and data governance in tourism and hospitality

As noted earlier in this study, compliance with data privacy and protection laws is an imperative requirement for all THOs involved in the process of collection, storage, analysis and use of travellers' personal data. Good data governance enables THOs to meet their regulatory obligations in respect of compliance, ensuring travellers' online safety and security. However, an effective ethical-based approach in line with THOs strategic objectives is also essential in order to ensure that the processing and use of travellers' data and information in big data analytics that assist the THOs in maintaining and gaining competitive advantage, is

carried out in a fair, transparent, responsible, and ethical manner (Bennett, 2019; Abraham *et al.*, 2019). Overall, the proposed conceptual framework for ethical-based data management and data governance in THOs is captured in Figure 1 below.

[INSERT FIGURE 1 ABOUT HERE]

This proposed data governance toolkit seeks to expand a compliance-based approach to a broader (in scope and content) ethical-based approach that, in addition to compliance issues, takes into consideration prevalent ethical considerations around privacy, an equitable exchange of travellers' data and information and, equally important, THOs ability to build trust among their stakeholders in their procedures and business practices (i.e., social license). Our data governance framework is different from existing frameworks presented in previous literature as it is developed within a conceptual philosophy formulated around ethics and trust (not just quality and compliance) as key concepts and constructs of ethical organisational data strategies that lead into more ethical approaches to data management by organisations.

5.1. Compliance

Firstly, from a legal/compliance perspective, THOs must implement suitable procedures to comply with international and national legislations on data collection, storage, use and disclosure of data. For example, the electronic/online collection and disclosure of personal data and information may be an offence under cybercrime legislation. Likewise, internationally, the GDPR provides the legal standards for personal data privacy and data protection as the current basis of the privacy and data protection legal system in the EU (Ameen *et al.*, 2021), with extended repercussions globally, due to increasing international flows of data and information (Witzleb, 2020).

As highlighted by Masseno and Santos (2018), in line with GDPR regulations and principles around *lawfulness, fairness, and transparency*, THOs must be clear as to why data are being collected and how data will be used (in compliance with Art. 5, clause 1a of the GDPR). They must comply with the principle of *purpose limitation* (Art. 5, clause 1b) which prevents arbitrary reuse of personal data, therefore limiting organisations' ability to process data for other purposes than those originally intended. Also, due to the considerable amounts of consumer data collected, aggregated and analysed by organisations, the principle of *data minimisation* (in compliance with (Art. 5, clause 1c) requires THOs to establish what data are deemed necessary and relevant for processing, and not excessive. Furthermore, as specified by Art. 5, clause 1d of the GDPR, THOs must engage in *accurate* and *up-to-date processing* as errors in data processing may affect the quality of data and may attract legal responsibilities for harm/damage (Hoeren, 2018). THOs must also dispose of data that is no longer useful for commercial or legal purposes (Art. 5, clause 1e), and they must demonstrate compliance with all the GDPR principles and must keep records of their data processing activities (Art. 5, clause 2). Finally, THOs should adopt *privacy by design* approaches (Art. 25) which require them to program pre-emptive technological measures and systems aimed to address data protection and privacy concerns (Masseno and Santos, 2018; ICO, 2018).

5.2. Privacy and ethics

Secondly, more so, from an ethical perspective, it may not be sufficient for THOs to simply comply with data and privacy laws to guard them from unsatisfied travellers, which, in recent times, have become much more aware and sensitive about how organisations use their data and information (Panetta, 2018). Hence, alongside the protections given by the GDPR (ICO, 2018) and other international and national data protection laws, potential frameworks for ethical data

management should identify the methods used in data collection, what data is used for, who has access to data, and why they have access to it (Blakesley and Yallop, 2019).

Privacy and ethics must be at the forefront of any design of data governance frameworks (Panetta, 2018). In tourism and hospitality such frameworks must ensure that widespread ethical concerns around travellers' digital data and information that are collected in various structured and unstructured ways by THOs are dealt with to ensure travellers' safety and data security.

THOs should also be able to express to travellers the particular advantages they may anticipate from disclosing their data when they use THOs services and/or provide feedback about their services online (Blakesley and Yallop, 2019; Yallop and Séraphin, 2020). Even more so, the COVID-19 pandemic is expected to accelerate the shift in consumer beliefs and attitudes, with consumers now having to balance expectations for privacy and autonomy with government and organisations, pushes for increased transparency and control. Hence, heightened levels of consumer questioning what data is being held on them and how this data is used should be expected (Manton, 2020). For this reason, THOs will need to make data decisions and create data strategies that will give travellers command over the information they choose to share, whilst explaining in which way this information can be utilised to the benefit of others (Manton, 2020). Likewise, these issues are directly linked to travellers' expectations for a fair and equitable exchange of their personal data and information.

Certainly, the use of consumers' personal data by THOs is indeed increasingly needed to drive performance in the sector and for competitive advantage as it provides greater insight into travellers' behaviour. However, these insights must not be obtained whilst violating travellers' privacy, instead THOs should aim to achieve both objectives – valuable data insights as well as privacy and data protection/security – by adopting ethical and fair data decision processes (Smith *et al.*, 1996; Yallop and Séraphin, 2020).

5.3. Equitable exchange of data and information

As noted, today, consumers are much more aware that their data and information is increasingly valuable to organisations (Panetta, 2018). In a growing digital space and business environment, most consumers recognise and accept that internet browsing, digital services and technologies are heavily monitored (Blakesley and Yallop, 2019). On the other hand, previous research surrounding equity in exchange and online service transactions suggests that consumers tend to evaluate the type and volume of personal data required of them to provide in exchange for services in general, and that they perceive the exchange fair if the *locus* of control of data and information shared resided with them (Milne and Culnan, 2004; Ashworth and Free, 2006; Min and Kim, 2015). Also, previous studies indicate that often, in service transactions, the motivations of customers and organisations providing the service are often conflicting, and recommend "goal congruence" measures to aim to achieve parity in exchange, which seeks to remove, albeit not entirely, opportunism (Jap and Anderson, 2003).

Several studies have highlighted the fact that transparency about the use and protection of consumers' data reinforces trust (Morey *et al.*, 2015; Bennett, 2019). This is particularly important in tourism and hospitality as travellers' trust in the respective THO that offers them the service may significantly decline if they perceive that the THO does not take appropriate measures to protect their personal data and information (Chen and Jai, 2019).

Moreover, due to the nature of the tourism and hospitality industry, THOs may be required to exchange travellers' data and information with other key stakeholders, such as government and local authorities, industry associations and other industry participants (such as access providers, e.g. aviation, cruises, etc.), and other complementary industries (such as businesses and representative organisations involved in industries that facilitate tourism, e.g. tertiary education, event organisers, etc.) (Tourism Australia, 2015). It is vital that a fair and ethical

exchange of travellers' data and information amongst all these stakeholders is ensured by THOs as key element of their data governance systems designed to protect their travellers' privacy and data security. As such, network partnerships in data sharing, digital technologies employed and ethical responsibilities between THOs and their stakeholders need to be based on trusting relationships (Tussyadiah *et al.*, 2020; Blakesley and Yallop, 2019; McQuater, 2018).

Specifically, in challenging times such as the COVID-19 pandemic, if THOs or any other third party requests any other information that does not sit within boundaries of current data privacy laws (for instance sensitive medical data and information, travel history and other personal details), then there should be suitable legal and ethical reasons for such requests. At the same time, THOs would need to put in place appropriate measures to manage the added ethical risks encountered by travellers, and the possible security and reputational risks that THOs are confronted with, especially when collecting, sharing, and storing sensitive traveller data and information.

5.4. Social license

The shift to a more digitised society over the past years (which has been felt more acutely in recent times due to the COVID-19 pandemic and its impacts that have seen a rapid reduction in social contact) has meant that organisations in tourism and hospitality sectors need to question more generally their license to know, discover and use travellers' data and information for strategic purposes. In other words, the need to build trust between THOs, travellers and other stakeholders becomes increasingly important, i.e., trusting relationships which in turn lead to the THOs' ability to demonstrate a social license to operate.

The concept of *social license* is not a new concept *per se*. Over the past few years however, the term "social license to operate" (SLO) has grown in popularity (Gehman *et al.*, 2017),

becoming an imperative aspect in industries and sectors that require support from local communities (Gupta and Kumar, 2018), such as tourism and hospitality, as THOs have the opportunity to make a real impact and positive difference to these communities. Commonly, organisations refer to "social license to operate" (SLO) to suggest that their activities are considered legitimate in the eyes of society. SLO is defined as an ongoing acceptance and approval of the organisation's business practices by its stakeholders and the larger public and community, as contractual grounds for the legitimacy of its business activities (Demuijnck and Fasterling, 2016). This approach delivers an extended outlook on social considerations and responsibilities of THOs solely related to accepted societal norms and standards, and ingrained cultural considerations. It entails a wider and more comprehensive approach to the use of big data and analytics, specifically the collection, storage, use and sharing of travellers' data and information. In their quest for success and competitive advantage, THOs must secure and preserve trust in their relationships with travellers, and they must display highly ethical organisational values to ensure that customers regard them as trustworthy (Gupta and Kumar, 2018; Yallop and Séraphin, 2020; Panetta, 2018).

Particularly with the wider acceptance and use of vaccination passports in the COVID-19 pandemic and post-pandemic, gaining consumers' approval and trust in THOs business practices becomes paramount. These organizations should consider travellers' concerns regarding privacy violations, government/private surveillance, the potential abuse of data collected and consumers' distrust in vaccination passport apps (Zhang *et al.*, 2021). To increase consumers' trust THOs should implement strong internal controls and safeguards to prevent staff from accessing any personal data without ethical process (e.g., third-party approval, the four-eyes principle – i.e., two individuals being required to complete the process, documentation, and alerts to affected individuals (Zhang *et al*., 2021). In addition, THOs need to consider ethical societal concerns around pandemic inequities, in that the benefits of

vaccination passports will not be distributed equitably, therefore, to ensure that some consumers' groups will not be disadvantaged in accessing THOs products and services (Asi, 2021; Kofler and Baylis, 2020). While vaccination passports are a premise of returning to normality and may become inevitable, they should include welfare and health exceptions (Hassoun and Herlitz, 2021) which THOs should consider and develop business practices that do not exacerbate consumer inequities.

Finally, it is important that THOs recognise the value of other key elements that are comprised in a comprehensive approach to data governance (as seen in Figure 1), namely an extension of legal/compliance matters to a wider assessment of other ethical aspects, such as individual ethical issues relating to travellers' digital privacy and ethics (confidentiality, transparency, equity of access, and informed use of information), and fair and equitable exchanges of data and information amongst all stakeholders, as this may negatively impact travellers/consumers' privacy and security. In the era of digital transformation, organisations need a framework for data governance that ensures consumer data is used for value creation, not only in accordance with legal requirements, but also meeting consumers' expectations. THOs must create a culture that recognises consumer data as an asset and must establish mechanisms that prevent the abuse or misuse of sensitive consumer data (e.g., gender, race, address, health status, personal identification data, etc.) that they collect for business decisions, marketing, or service creation and provision (Janssen et al, 2020).

Furthermore, the elements within the proposed data governance framework must be viewed by THOs as inter-connected elements that guide ethical data management practices and behaviour.

5.5. Framework implementation induced consumer benefits

The implementation of the proposed holistic framework of data governance creates significant benefits to THOs and, most importantly, to their key stakeholder, the consumers, as it enables trusting relationships between the two parties. Undoubtedly, the extended approach (from a mere compliance-based approach to a more ethical and socially responsible data governance) will enhance THOs ability to respond in a more ethical manner to consumers' concerns about personal data and information.

From a data compliance point of view, consumers will be confident that the THOs they share data with are aware and adhere to national and international data laws which ensure fairness and transparency. Firstly, consumers' main benefits will consist of choice and control. More specifically, they will be able choose what data they share with THOs, while, at the same time, will be in control of their shared data. Secondly, consumers will have access to their stored data, they will be able to require their personal information from THOs, and they will also be entitled to ask for their data to be deleted. Thirdly, according to latest data compliance laws, consumers will need to be informed in case of data breaches. Any such occurrence will need to be rapidly notified to consumers, who will have to be able to decide on certain operations to be carried out by affected THOs regarding their consumers' data.

Just as important, from an ethical point of view, the proposed framework ensures that travellers/consumers' privacy rights will be respected, and THOs adopt a truly ethical business stance, seeking ongoing measures to protect their customers' interests regarding privacy through fair and ethical exchanges of consumer data, and demonstrating a social and ethics license to operate, through increased trust that they are doing the right thing by their consumers.

Clearly, an ethical data management and data governance framework which allows THOs to have access to consumers' data and enable them to provide a more personalised and efficient

service based on the information consumers choose to provide, would ultimately be a great benefit to consumers/travellers.

6. Conclusion

In an increasingly digital world big data and analytics have a vital role in business decision-making in tourism and hospitality. Over the last years tourists have become increasingly aware about service personalisation practices used by THOs through use of their personal data, hence more aware and sensitive about data privacy and security issues (Panetta, 2018; Chen and Jai, 2019). THOs must put in place appropriate data governance frameworks that ensure consumers' data protection. Such frameworks, as the one proposed in this study, need to expand further than a mere compliance with current data privacy and protection legislation, entailing a more ethical and responsible approach to secure data and to offer protection for travellers and all other stakeholders. In the current climate of the COVID-19 pandemic this issue becomes critical as an increased number of data breaches and cyber-attacks have been reported globally (Armerding, 2018; Continuity Central, 2020).

Thus, this study suggested a framework for ethical data management and data governance in THOs that, alongside legal and compliance issues, involves ethical considerations in building trusting relationships with customers and stakeholders. Consequently, THOs need to ensure travellers' privacy and data security and to place travellers in control of the data and information they choose to disclose. Furthermore, because the nature of tourism activities may require THOs to share travellers' data with other stakeholders, it is vital for them to ensure an equitable and ethical exchange of data and information that places tourists' rights to privacy and data security at the forefront of big data decisions. Equally important, THOs need to have high ethical organisational standards and values in their pursuit of building strong, long-term relationships based on trust, with travellers and other stakeholders.

The suggested strategy for a more ethical approach of data management in THOs is in line with the conceptual philosophy of this study which is articulated around the topic of ethics, and may be expressed through Motivation, Opportunity and Ability (MOA), terms which are also at the basis of an eponymous model. Indeed, the MOA model highlights factors that either support or inhibit engagement and participation of individuals or organisations with something or someone (Jepson *et al.*, 2013): *Motivation* is what pushes an organisation to do something, and it is typically based on expected benefits. *Opportunity* is about the engineering put in place to facilitate the involvement with or implementation of a process and requires the support of leaders and/or good governance. Finally, *ability* includes awareness, experience, knowledge, skills, and accessibility to implement a strategy (Jepson *et al.*, 2013). Ability is central as without *ability*, the other two factors are not feasible (Jepson *et al.*, 2013). The framework developed in this study confirms that each of these factors is equally important. The motivation to protect travellers' autonomy, rights, personal privacy, and security is evident (Blakesley and Yallop, 2019; Culnan and Bies, 2003; Laczniack and Murphy, 2006; Martin *et al.*, 2020; Sarathy and Robertson, 2003; Wu *et al.*, 2019). However, Gallego and Font (2020) question the ability of THOs to achieve their objectives, especially in times of crisis such as the COVID-19 pandemic, which, subsequently, impacts opportunities. Therefore, it is imperative to address these latter points, i.e., opportunities (the work carried out by THOs to facilitate the implementation of ethical data management and data governance) and ability (increased awareness and 'know-how' in designing and implementing ethical frameworks for data management). Particularly under the current challenging circumstances due to COVID-19, the successful application of the framework developed in this study would lead to the achievement of Sustainable Development Goal 9 (Industry innovation and infrastructure); and Sustainable Development Goal 17 (Partnership for the goals) (UNDP, 2020).

Also, it is important to acknowledge that the implementation of this framework by THOs might involve, for some, a change in their set of values, and this change can only be achieved with the support of the leadership team and good (corporate and data) governance. At the same time, building customer trust is vital. Several measures will support THOs in building trusting relationships with customers and their stakeholders such as: (a) an awareness about regulations (from the GDPR to other international and national data protection laws, particularly when operating internationally); (b) training of employees in data governance and using data experts to design data governance frameworks that ensure data security and protection effectively; (c) demonstrating full transparency in data decisions; (d) empowering travellers by developing data strategies that will give travellers control of the information they choose to share, whilst explaining in which way this information may be utilised to benefit others; and (e) adopting 'privacy by design' approaches, with decisions relating to frameworks' design situated in the applicable local and global contexts. Certainly, the current context of the pandemic will have substantial repercussions on data decisions, and THOs decisions in general.

Paradoxically, the COVID-19 pandemic provides a favorable context for changing the currently accepted development model based solely on growth. The ethical behavior of THOs in relation to tourists in terms of ensuring personal data privacy and security will lead to an increased level of trust, which, in turn, will lead to satisfied and loyal tourists. Thus, ethical data management and sound data governance frameworks will become a source of competitive advantage.

Future research directions should consider extended research into the governance of data in tourism and hospitality particularly relating to studies that describe the actual practice and identify a set of effective operational tools for data governance, privacy, and security issues. Equally important, the perspective of travellers' and THOs' representatives should be studied, with the objective to further refine the proposed framework, as they are involved directly in the

application of such framework and/or are its main beneficiaries. Finally, the proposed framework and resulting knowledge may be transferable and applicable to other online services and related business contexts. Further conceptual and empirical studies could be conducted in other service industries to identify and examine potential similarities and differences in organisations' practices of dealing with consumer privacy in a lawful and ethical manner.

7. References

Abraham, R., Schneider, J., and vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49, 424-438.

Addo-Tenkorang, R., and Helo, P.T. (2016). Big data applications in operations/supply-chain management: A literature review. *Computers and Industrial Engineering*, 101, 528–543.

Aguirre, E., Roggeveen, A. L., Grewal, D., and Wetzels, M. (2016). The personalization-privacy paradox: implications for new media, *Journal of Consumer Marketing*, 33(2), 98-110.

Al-Ruithe, M., Benkhelifa, E., and Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, 23(5-6), 839-859.

Akhter, S.H. (2014). Privacy Concern and Online Transactions: The Impact of Internet Self-Efficacy and Internet Involvement, *Journal of Consumer Marketing*, 31 (2), 118-125.

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J., and Choudrie, J. (2021) Keeping customers'data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce, *Computers in Human Behavior*, 114, 106531, ahead-of-print, https://doi.org/10.1016/j.chb.2020.106531

Armerding, T. (2018). The 18 biggest data breaches of the 21st Century, available at: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (accessed 25 October 2019).

Ashworth, L., and Free, C. (2006). Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, 67(2), 107-123.

Asi, Y. M. (2021). Vaccine passports may be on the way – but are they a reason for hope or a cause for concern? *The Conversation*, available at: https://theconversation.com/vaccine-passports-may-be-on-the-way-but-are-they-a-reason-for-hope-or-a-cause-for-concern-156534

Bahar, V. S., Nenonen, S., & Starr Jr, R. G. (2021). From channel integration to platform integration: Capabilities required in hospitality. *Industrial Marketing Management*, 94, 19-40.

Ballard, C., Compert, C., Jesionowski, T., Milman, I., Plants, B., Rosen, B., and Smith, H. (2014). Information governance principles and practices for a big data landscape, IBM Redbooks, available at: http://refhub.elsevier.com/S0268-4012(19)30078-7/sbref0310 (accessed 10 August, 2020).

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study, *Journal of Marketing*, 69(4), 133-152.

Barocas, S., and Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM,* 57(11), 31-33.

Bennett, S. (2019). Big data, privacy and information governance: Incorporating an ethical-based assessment. *Governance Directions,* 71(5), 244-254.

Blakesley, I.R., and Yallop, A.C. (2019). What do you know about me? Digital privacy and online data sharing in the UK insurance sector. *Journal of Information, Communication & Ethics in Society*, 18(2), 281-303.

Boumphrey, S. (2019). Megatrends: Disruptors – What does it take to disrupt a market? Euromonitor International, available at: http://www.portal.euromonitor.com (accessed 23 October 2019).

Bremmer, C. (2019). The voice of the industry: Travel. Euromonitor International, available at: http://www.portal.euromonitor.com (accessed 23 October 2019).

Brough, A. R. and Martin, K. D. (2020). Consumer privacy during (and after) the COVID-19 pandemic, *Journal of Public Policy & Marketing*, DOI: 10.1177/0743915620929999

Brous, P., Herder, P., and Janssen, M. (2016). Governing asset management data infrastructures. *Procedia Computer Science*, 95, 303–310.

Conger, S., Pratt, J. H. and Loch, K. D (2013). Personal information privacy and emerging technologies, *Information Systems Journal*, Vol. 23, 401-417.

Canosa, A., Graham, A., and Wilson, E. (2018a). Reflexivity and ethical mindfulness in participatory research with children: What does it really look like? *Childhood*, 25(3), 400-415.

Canosa, A., Graham, A., and Wilson, E. (2018b). Child-centred approaches in tourism and hospitality research: methodological opportunities and ethical challenges. In *Handbook of Research Methods for Tourism and Hospitality Management*. Edward Elgar Publishing.

Chen, H.S., and Jai, T.-M. (2019). Cyber alarm: Determining the impacts of hotel's data breaches messages. *International Journal of Hospitality Management*, 82, 326-334.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60-67.

Continuity Central (2020), High levels of COVID-19 based cyber-attacks seen in March but overall levels are down, available at: https://www.continuitycentral.com/index.php/news/technology/5017-high-levelsof-covid-19-based-cyber-attacks-seen-in-march-but-overall-levels-are-down

Culnan, M.J., and Bies, R.J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues,* 59(2), 323-342.

Dare, T. (2021). Before we introduce vaccine passports we need to know how they'll be used, The Conversation, available at: https://theconversation.com/before-we-introduce-vaccine-passports-we-need-to-know-how-theyll-be-used-156197

Digital Future Society (2019) *Toward better data governance for all: Data ethics and privacy in the digital era*. Available at https://digitalfuturesociety.com/report/toward-better-data-governance-for-all/

Demuijnck, G., and Fasterling, B. (2016). The Social License to Operate. *Journal of Business Ethics*, 136 (4), 675–685.

Eastlick, M. A., Lotz, S. L., and Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59(8), 877-886.

European Commission (2020). What are Data Protection Authorities (DPAs)? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (accessed 5 August 2020).

Evans, N. (2020). *Strategic management for tourism, hospitality and events*, 3rd Edition, Routledge, Abingdon.

Fitzgerald, C., McCarthy, S., Carton, F., O'Connor, Y.O., Lynch, L., and Adam, F. (2016). Citizen participation in decision-making: can one make a difference? *Journal of Decision Systems*, 25(sup1), 248-260.

Foroudi, P., Gupta, S., Nazarian, A. and Duda, M. (2017). Digital technology and marketing management capability: achieving growth in SMEs. *Qualitative Market Research*, 20(2), 230-246.

Fortes, N., and Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, 22(3), 167-176.

Frik, A., and Gaudeul, A. (2020). A measure of the implicit value of privacy under risk, *Journal of Consumer Marketing*, 37(4), 457-472.

Gallego, I. and Font, X. (2020). Changes in air passenger demand as a result of the COVID-19 crisis: using Big Data to inform tourism policy. *Journal of Sustainable Tourism*, https://doi.org/10.1080/09669582.2020.1773476

Gehman, J., Lefsrud, L.M., and Fast, S. (2017). Social license to operate: Legitimacy by another name? *Canadian Public Administration*, 60(2), 293-317.

Getz, D. (2012). Event studies. *Theory, research and policy for planned events*. Routledge.

Gilson, L. L. and Goldberg, C. B. (2015). Editor's comment: So, what is a conceptual paper? *Group & Organization Management*, 40*(2)*, 127-130.

Gossling, S., Scott, D., and Hall, C.M. (2020) Pandemics, tourism and global change: A rapid assessment of COVID-19. *Journal of Sustainable Tourism*, doi.org/10.1080/09669582.2020.1758708.

Gupta, U.G., and Gupta, A. (2016). Vision: a missing key dimension in the 5V Big Data framework. *Journal of International Business Research and Marketing*, 1(3), 50-56.

Gupta, S., and Kumar, A. (2018). Social licence to operate: A review of literature and a future research agenda. *Social Business*, 8(2), 187-203.

Hall, C.M., and Ram, Y. (2019). Protecting privacy in tourism – a perspective article. *Tourism Review*, 75(1), 76-80.

Hammond, M., & Wellington, J. (2013). *Research methods. The key concepts*. London: Routledge.

Harvard Business Review Analytic Services (2019). An inflection point for the data-driven enterprise, available at: https://hbr.org/resources/pdfs/comm/snowflake/AnInflectionPoint.pdf (accessed 10 August 2020).

Hassoun, N., and Herlitz, A. (2021). How to Make 'Immunity Passports' More Ethical Requirements that travelers be vaccinated must be implemented in a humanitarian way. *Scientific American*, available at: https://www.scientificamerican.com/article/how-to-make-immunity-passports-more-ethical/ (accessed 28 February 2021).

Hellard, B. (2020). Tourism platforms sign data-sharing deal with EU, available at: https://www.itpro.co.uk/policy-legislation/data-governance/354933/tourism-platforms-sign-data-sharing-deal-with-eu (accessed 10 August 2020).

Hirt, M., Smit, S., Bradley, C., Uhlaner, R., Mysore, M., Atsmon, Y., and Northcote, N. (2020). Getting ahead of the next stage of the coronavirus crisis, April 2, 2020, McKinsey & Company, available at: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/getting-ahead-of-the-next-stage-of-the-coronavirus-crisis?cid=other-eml-alt-mip-mck&hlkid=da6132784e504d26b73ba152c8f8a3fe&hctky=11662083&hdpid=d52f8189-6d6f-4fd8-87ad-51442a8b1801 (accessed 10 August 2020).

Hoeren, T. (2018). Big Data and Data Quality, in Hoeren, T., Kolany-Raiser, B. (Eds.) *Big Data in Context - Legal, Social and Technological Insights*, Springer.

Hunter, G. L., and Taylor, S. A. (2020). The relationship between preference for privacy and social media usage, *Journal of Consumer Marketing*, 37(1), 43-54.

IBM (2014a). The four V's of big data, available at: https://www.ibmbigdatahub.com/infographic/four-vs-big-data (accessed 10 August 2020).

IBM (2014b). Extracting business value from the four V's of big data, available at: https://www.ibmbigdatahub.com/infographic/extracting-business-value-4-vs-big-data (accessed 10 August 2020).

ICO (2015). Key definitions of the data protection act. The Information Commissioner's Office (ICO), London, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/ (accessed 27 August 2020).

ICO (2018). Guide to the General Data Protection Regulation (GDPR), available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (accessed: 10 August, 2020).

Ioannou, A., Tussyadiaha, I., and Lu Y. (2020). Privacy Concerns and Disclosure of Biometric and Behavioral Data for Travel. *International Journal of Information Management*, 54, https://doi.org/10.1016/j.ijinfomgt.2020.102122 (ahead-of-print).

Jamal, T., and Budke, C. (2020). Tourism in a world with pandemics: Local-global responsibility and action. *Journal of Tourism Futures*, 6(2), 181-188.

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, 37(3), 101493.

Janeway, W. (2012). *Doing Capitalism in the Innovation Economy: Markets, Speculation and the State*. Cambridge: Cambridge University Press.

Jap, S.D., and Anderson, E. (2003). Safeguarding interorganizational performance and continuity under ex post opportunism. *Management Science*, 49(12), 1684-1701.

Jepson, A., Clarke, A., and Ragsdell, G. (2013). Applying the motivation-opportunity-ability (MOA) model to reveal factors that influence inclusive engagement within local community festivals: The case of UtcaZene 2012. *International Journal of Event and Festival Management*, 4(3), 186-205.

Khoo-Lattimore, C. (2015). Kids on board: methodological challenges, concerns and clarification when including young children's voices in tourism research. *Current Issues in Tourism*, 18(9), 845-858.

Kim, H.-B., Lee, D.-S., and Ham, S. (2013). Impact of hotel information security on system reliability, *International Journal of Hospitality Management*, 35, 369-379.

Kraus, S., Palmer, C., Kailer, N., Kallinger, F. L., & Spitzer, J. (2019). Digital entrepreneurship: A research agenda on new business models for the twenty-first century, *International Journal of Entrepreneurial Behavior & Research*, 25(2), 353-375.

Kofler, N., and Baylis, F. (2020). Ten reasons why immunity passports are a bad idea. Restricting movement on the basis of biology threatens freedom, fairness and public health. *Nature*, 581, 379-381.

Laczniak, G.R., and Murphy, P.E. (2006). Marketing, consumers and technology. *Business Ethics Quarterly*, 16(3), 313–321.Laney, D. (2001). 3D data management: controlling data volume, velocity and variety, February 6th, 2001, available at: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (accessed 10 August 2020).

Lapointe, D. (2020). Reconnecting tourism after COVID-19: The paradox of alterity in tourism areas. *Tourism Geographies*, 22(3), 633-638.

Leong, C. (2020). Here's what travelling could be like after COVID-19. World Economic Forum, Agenda, available at: https://www.weforum.org/agenda/2020/05/this-is-what-travelling-will-be-like-after-covid-19/ (accessed 10 August 2020).

Lillie, T., and Eybers, S. (2019). Identifying the constructs and agile capabilities of data governance and data management: A review of the literature. IDIA 2018, CCIS, 933, 313–326.

Macdonald, N. (2020). Could NZ use mobile phones to trace the contacts of Covid-19 cases?, March 25th, 2020, available at: https://www.stuff.co.nz/national/health/coronavirus/120518745/could-nz-use-mobile-phones-to-trace-the-contacts-of-covid19-cases (accessed 10 August 2020).

Manton, H. (2020). Coronavirus: Global change accelerators. WGSN, March 23rd, 2020, available at: https://www.wgsn.com/blogs/coronavirus-global-change-accelerators/ (accessed 10 August 2020).

Martin, K., Shilton, K., and Smith, J. (2019). Business and the ethical implications of technology: Introduction to the symposium. *Journal of Business Ethics*, 160, 307-317.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155.

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L. Stewart, D. W., Walker, B. A., Wang, Y. and Weaven, S. K. (2020). Data privacy in retail, *Jornal of Retailing*, Vol. Ahead-of-print, https://doi.org/10.1016/j.jretai.2020.08.003

Masergy (2020). 2020 UCaaS and CCaaS market trends report: Security and network are top demands, available at: https://www.masergy.com/white-paper/2020-idg-ucaas-and-ccaas-market-trends-report-security-and-network-are-top-demands (accessed 10 August 2020).

Masseno, M.D., and Santos, C. (2018). Privacy and Data Protection Issues on Smart Tourism Destinations - A First Approach. *Intelligent Environments*, 23 298-307.

Masur, P.K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

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

McQuater, K. (2018). Increase in data protection complaints. ResearchLive available at: www.research-live.com/article/news/increase-in-data-protection-complaints/id/5041443 (accessed 10 August, 2020).

MicroStrategy (2018). 2018 Global State of Enterprise Analytics Report, available at: https://www.microstrategy.com/getmedia/50ea9c13-feb7-4b9a-b976-8b04ca39abb2/Global-State-of-Enterprise-Analytics-Report-MicroStrategy_2018 (accessed 25 October 2019).

Milne, G.R., and Culnan, M.J. (2004). Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15-29.

Min, J., and Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, 66(4), 839-857.

Moher, D., Stewart, L., & Shekelle, P. (2015). All in the family: Systematic reviews, rapid reviews, scoping reviews, realist reviews, and more. *Systematic Reviews*, 4(1), 183–194. https://doi.org/10.1186/s13643-015-0163-7

Morey T, Forbath T., and Schoop A (2015). Customer data: designing for transparency and trust. *Harvard Business Review*, May, available at: https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (accessed 10 August 2020).

Morosan, C., DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, 47, 120-130.

MSI (2020) *Research priorities 2022-2024*, https://www.msi.org/wp-content/uploads/2020/09/MSI-2020-22-Research-Priorities-final.pdf

Nanni, A., and Ulqinaku, A. (2020). Mortality threats and technology effects on tourism. *Annals of Tourism Research*, May 3, 2020: 102942, https://doi.org/10.1016/j.annals.2020.102942 (in press).

Nov, O., Naaman, M., and Chen, Y. (2010). Analysis of participation in an online photo-sharing community: A multidimensional perspective. *Journal of the American Society of Information Science and Technology*, 61(3), 555-566.

Navío-Marco, J., Ruiz-Gómez, L. M., and Sevilla-Sevilla, C. (2018). Progress in information technology and tourism management: 30 years on and 20 years after the internet. *Tourism Management*, 69, 460-470.

Nunan, D., and Di Domenico, M.L. (2013). Market research and the ethics of big data. *International Journal of Market Research*, 55(4), 2-13.

Panetta, K. (2018). Gartner Top 10 Strategic Technology Trends for 2019, October 15, 2018, available at: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/ (accessed 10 August 2020).

Parry, D. (2021). How would digital COVID vaccine passports work? And what's stopping people from faking them? *The Conversation*, available at: https://theconversation.com/how-would-digital-covid-vaccine-passports-work-and-whats-stopping-people-from-faking-them-156032

Petrescu, M., Krishen, A., and Bui, M. (2020). The internet of everything: implications of marketing analytics from a consumer policy perspective, *Journal of Consumer Marketing*, 37(6), 675-686.

Phelps, J. E., D'Souza, G., and Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.

Pizam, A. (2013). Editorial: Hotel online privacy. *International Journal of Hospitality Management*, 35, A1.

Pollina, E., and Busvine, D. (2020). European mobile operators share data for coronavirus fight.
Reuters, available at: https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2 (accessed 10 August 2020).

Privacy Commissioner (2020), The Privacy Act, available at: https://privacy.org.nz/privacy-act-2020/privacy-act-2020/ (accessed 20 August 2020).

PwC (2016). Cyber and data security in the hotel industry, available at: https://www.pwc.com/m1/en/publications/documents/cyber-and-data-security-in-the-hotel-industry.pdf (accessed 17 October 2019).

PwC (2017). Cyber security and data privacy in the hotel industry, available at: https://www.pwc.com.cy/en/publications/assets/cyber-security-and-data-privacy-in-the-hotel-industry-january-2017.pdf (accessed 20 October 2019).

Rasoolimanesh, S.M., Ramakrishna, S., Hall, C.M., Esfandiar, K., and Seyfi, S. (2020). A systematic scoping review of sustainable tourism indicators in relation to the sustainable development goals. *Journal of Sustainable Tourism*, https://doi.org/10.1080/09669582.2020.1775621 (ahead-of-print).

Rasouli, M.R., Trienekens, J.J., Kusters, R.J., and Grefen, P.W. (2016). Information governance requirements in dynamic business networking. Industrial Management & Data Systems, 116(7), 1356–1379.

Richards, N.M., and King, J.H. (2014). Big data ethics. Wake Forest Law Review, 49(2), 393-432.

Riggins, F. J., and Klamm, B. K. (2017). Data governance case at KrauseMcMahon LLP in an era of self-service BI and Big Data. *Journal of Accounting Education*, 38, 23-36.

Román, S. (2007). The ethics of online retailing: a scale development and validation from the consumers' perspective. *Journal of Business Ethics*, 72(2), 131-148.

Sarathy, R., and Robertson, C.J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, 46(2), 111-126.

Séraphin, H. (2020). COVID-19: An opportunity to review existing grounded theories in event studies. Journal of Convention and Event Tourism, doi: 10.1080/15470148.2020.1776657 (ahead-of-print).

Séraphin, H, and Yallop, A.C. (Eds.), (2020). *Overtourism and tourism education. A strategy for sustainable tourism futures.* Routledge, London.

Séraphin, H., and Vo-Than, T. (2020). Investigating the Application of the Principles for Responsible Management Education to Resort Mini-Clubs. *The International Journal of Management Education*, 18(2), 100377.

Shilton, K. (2009). Four billion little brothers? Privacy, mobile phones and ubiquitous data collection. *Communications of the ACM*, 52(11), 48-53.

Sigala, M. (2020). Tourism and COVID-19: impacts and implications for advancing and resetting industry and research. *Journal of Business Research*, 117, 312-321.

Smith, H.J., Milberg, S.J., and Burke, S.J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.

Stalenis, G., Hodgson, A., and Boumphrey, S. (2020). The impact of Coronavirus on the global economy, Euromonitor International, available at: http://www.portal.euromonitor.com (accessed 10 August 2020).

Tallon, P.P., Ramirez, R.V., and Short, J.E. (2014). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, 30(3), 141–177.

Tam, S.-M., and Kim, J.-K. (2018). Big data ethics and selection-bias: An official statistician's perspective. *Statistical Journal of the IAOS*, 34, 577-588.

Tanti, A., and Buhalis, D. (2017). The influences and consequences of being digitally connected and/or disconnected to travellers. *Information Technology & Tourism*, 17, 121–141.

Tourism Australia (2015). Risk management policy & procedure, available at: https://www.tourism.australia.com/content/dam/assets/document/1/6/x/6/p/2002561.pdf (accessed 10 August 2020).

Tussyadiah I., Li S., and Miller G. (2019). Privacy protection in tourism: Where we are and where we should be heading for. In: Pesonen J., Neidhardt J. (Eds.), *Information and Communication Technologies in Tourism*, 278-290, Springer Verlag, Berlin.

Tussyadiah I., Zach, F.J., and Wang, J. (2020). Do travellers trust intelligent service robots? *Annals of Tourism Research*, 81, 102888, DOI:10.1016/j.annals.2020.102886

UK Government (2018a). The data protection act (2018), available at: www.gov.uk/data-protection (accessed 10 August 2020).

UK Government (2018b). Guidance: Data Ethics Framework, available at: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework (accessed 10 August 2020).

UNDP (2020). Sustainable development goals, available at: https://www.un.org/sustainabledevelopment/sustainable-development-goals/ (accessed 10 August 2020).

UNWTO (2001), Global Code of Ethics for Tourism. For Responsible Tourism, available at https://webunwto.s3.eu-west-1.amazonaws.com/imported_images/37802/gcetbrochureglobalcodeen.pdf

UNWTO (2020). Supporting jobs and economies through travel & tourism. Call for action to mitigate the socio-economic impact of COVID-19 and accelerate recovery, available at: https://webunwto.s3.eu-west-1.amazonaws.com/s3fs-public/2020-04/COVID19_Recommendations_English_1.pdf (accessed 10 August 2020).

UNWTO (2020). World Tourism Barometer, vol. 18, No. 3, June 2020, Madrid, available at https://doi.org/10.18111/wtobarometereng

Urquhart, E. (2019). Technological mediation in the future of experiential tourism. *Journal of Tourism Futures*, 5(2), 120-126.

Visser, W. (2015). *Sustainable Frontiers. Unlocking Change through Business, Leadership and Innovation*, Greenleaf Publishing, Sheffield.

Volchek, K., Law, R., Buhalis, D., and Song, H. (2020). Exploring ways to improve personalisation: The influence of tourism context on service perception. *e-Review of Tourism Research*, 17(5), 737-752.

Ward, J.S., and Baker, A. (2013). Undefined by data: a survey of big data definitions, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.705.9909&rep=rep1&type=pdf (accessed 10 august 2020).

Weissinger, L. (2021). Vaccination passport apps could help society reopen – first they have to be secure, private and trusted, The Conversation, available at: https://theconversation.com/vaccination-passport-apps-could-help-society-reopen-first-they-have-to-be-secure-private-and-trusted-157219

West, S.M. (2019). Data capitalism: redefining the logics of surveillance and privacy. *Business & Society*, 58, 20-41.

Weydert, V., Desmet, P., and Lancelot-Miltgen, C. (2020). Convincing consumers to share personal data: double-edged effect of offering money, *Journal of Consumer Marketing*, 37(1), 1-9.

Williams, A.M., and Baláz, V. (2015). Tourism risk and uncertainty: Theoretical reflections. *Journal of Travel Research*, 54(3), 271–287.

Witzleb, N. (2020). Data privacy: stricter European rules will have repercussions in Australia as global division grow, *The Conversation*, available at: https://theconversation.com/data-privacy-stricter-european-rules-will-have-repercussions-in-australia-as-global-divisions-grow-142980 (accessed: 27 August, 2020)

World Economic Forum (WEF) (2020), Known Traveller Digital: Identity Specifications Guidance, March 2020, available at https://www.weforum.org/whitepapers/known-traveller-digital-identity-specifications-guidance (accessed: 5 June, 2020).

Wu, P.F., Vitak, J., and Zimmer, M.T. (2020). A conceptual approach to information privacy research. *Journal of the Association for Information Science and Technology*, 71(4),485-490.

Yallop, A.C., and Aliasghar, O. (2020). No busines as usual: A case for data ethics and data governance in the age of coronavirus, Online Information Review, https://doi.org/10.1108/OIR-06-2020-0257 (ahead-of-print).

Yallop, A.C., and Séraphin, H. (2020). Big Data and Analytics in Tourism and Hospitality: Opportunities and Risks. *Journal of Tourism Futures*, doi:10.1108/JTF-10-2019-0108 (ahead-of-print).

Yang, L., Li, J., Elisa, N., Prickett, T., and Chao, F. (2019). Towards big data governance in cybersecurity. *Data-Enabled Discovery and Application*, 3(10) DOI:10.1007/s41688-019-0034-9.

Yeoman, I. (2012). *2050: Tomorrow's tourism*. Channel View Publications, Bristol.

Yeoman, I., and McMahon-Beattie, U. (2018). The future of luxury: mega drivers, new faces and scenarios. *Journal of Revenue and Pricing Management*, 17(4), 204-217.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89.

Zhang, B., Weissinger, L., Himmelreich, J., McMurry, N., Li, T. C., & Kreps, S. E. (2021). Building robust and ethical vaccination verification systems. Brookings TechStream, available at: https://www.brookings.edu/techstream/building-robust-and-ethical-vaccination-verification-systems/

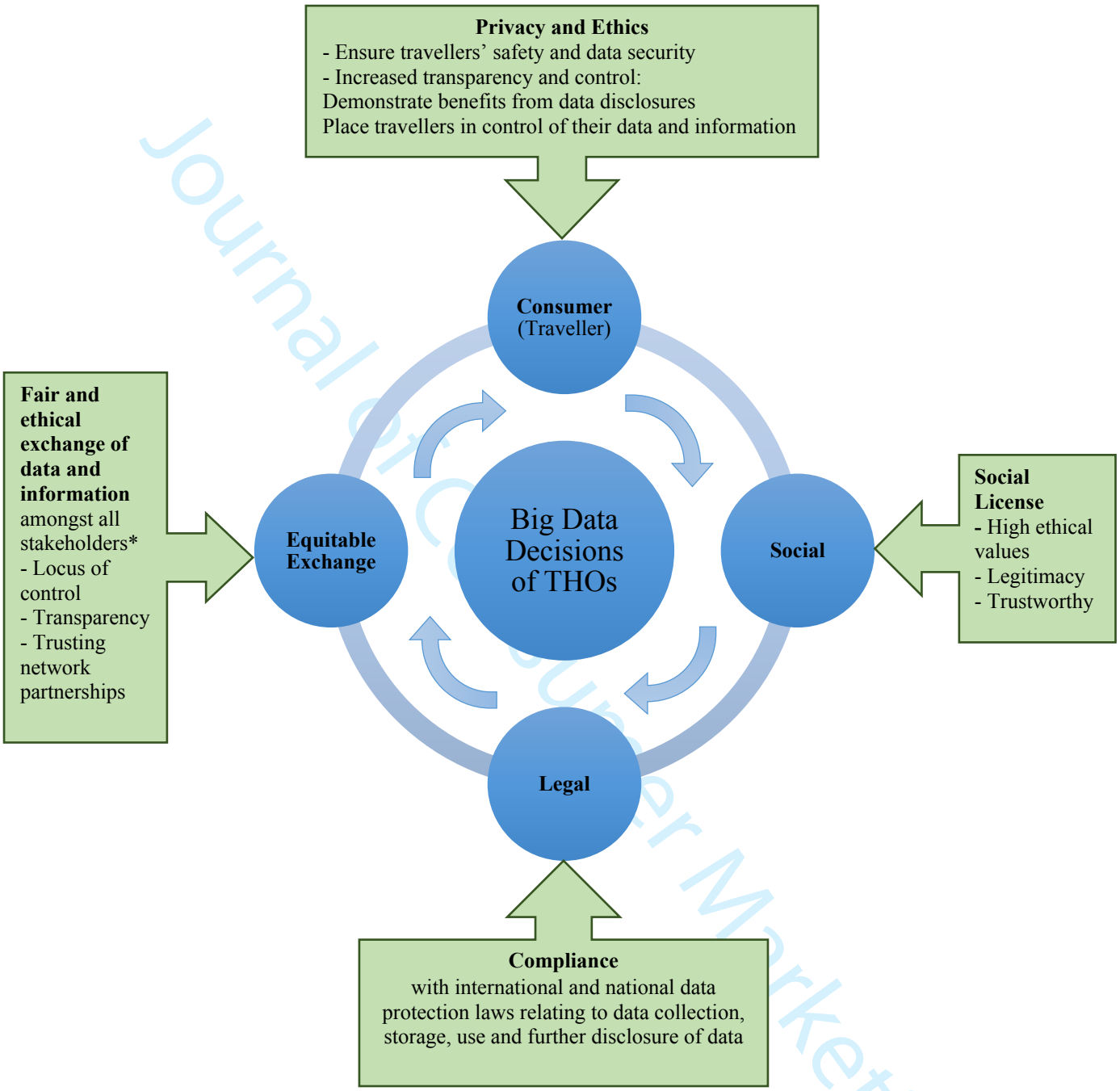

Figure 1: Proposed framework for ethical data management and data governance in tourism and hospitality organisations (THOs)

*Stakeholders: Travellers / Tourists; Government / Local authorities; Industry associations; Complementary industries

Source: The authors

JOURNAL OF CONSUMER MARKETING

Author Response Form

Revisions for Manuscript ID JCM-12-2020-4278.R1

Second review of: The Digital Traveller: Data Ethics and Data Governance in Tourism and Hospitality

Dear Dr Charles Jebarajakirthy and team of Guest Editors,
(*Guest Editors, Journal of Consumer Marketing*)

Thank you for the opportunity to revise this manuscript. We are confident that the team will see that the reviewers' comments steered further improvements in this revision.

Revisions from Reviewer 1: The main issue raised by R1 is that they do not see the contribution this paper makes to the consumer/marketing literature, and hence to this Special Issue in consumer privacy. We respectfully have to disagree that a paper addressing consumer privacy issues in tourism and hospitality is not relevant to consumer marketing literature, particularly for a Special Issue that calls for research on privacy concerns, especially during a pandemic. This industry and its consumers implicitly have been the most impacted by the pandemic and digital privacy issues, due to the industry's highly information-intensive characteristics (Tussyadiah et al., 2019) (even more so with the current need for stricter personal identification and vaccination passports), prominent particularities as a data-driven industry with strong links to the digital environment (Bahar et al., 2021), and an industry for which data privacy is of utmost importance compared to most other service industries (Bart et al., 2005).

Second, our paper engages with a representative range of consumer/marketing literature involving consumer privacy issues (which is also recognised by Reviewer 2), a good range published in the *Journal of Consumer Marketing* and other highly regarded marketing journals such as *Journal of Marketing*, *Journal of the Academy of Marketing Science, Journal of Interactive Marketing, Journal of Public Policy & Marketing, International Journal of Market Research*. Furthermore, a comprehensive search on the Web of Science of key marketing journals (i.e. *European Journal of Marketing, Industrial Marketing Management, International Journal of Research in Marketing, Journal of Interactive Marketing, Journal of International Consumer Marketing, Journal of Marketing, Journal of Marketing Research*) reveals a good number of publications (88 articles) focused specifically on tourism/hospitality/travel which, in itself, demonstrates the importance given to research in these sectors; whilst the body of marketing literature focused on consumer privacy has been evolving in the last years, albeit it is still limited, hence we welcomed this Special Issue as timely.

Last, but not least, our paper has been specifically developed with this Special Issue's main goals in mind, which are to "enable online service providers/data collecting organisations, and

policy makers to re-design, refine, and develop privacy policies to address online users' privacy concerns thereby facilitating online services", hence the original stakeholders approach we applied in the development of the framework proposed in our paper, which can serve as useful platform for further research in other service industries and related business contexts.

Even so, we endeavoured to satisfy reviewer 1 by reinforcing the rationale of our paper and including even more relevant consumer/marketing literature related to consumer privacy and further engaging with previous conversations and debates published in the *Journal of Consumer Marketing* and other significant marketing journals, as noted above. We have also corrected all other minor issues highlighted by the reviewer.

Revisions from Reviewer 2: R2 proposes two main (related) improvements which we made in the revised paper, i.e., to clarify what other papers we compare ourselves against in the development of the framework and how the framework is different from other frameworks of data governance.

Please, find the detailed response in the following tables. The first column (in black) includes the unredacted comments from the reviewing team, and the second column (blue) has a detailed response. When a change in the manuscript was required, the second column includes the page number and the edits in italics. (Changes in the manuscript are also in blue).

We would like to thank you again for the opportunity and the attention.

Reviewer 1

Comments to the Authors

Reviewer 1	Response
Thank you for allowing me to read this updated version of the manuscript. I appreciate the revisions the authors have made. Please see my comments above.	Thank you for your time to review our paper and your comments.
1. Originality: I find little contribution to the consumer marketing literature. The same concerns I had in the first draft remains. I find this manuscript more suitable for Emeralds JHTT or another more computer information type journal.	We are afraid that we have to disagree. Our research is focused on consumer privacy and ethical data management (it is not research on technological/technical/IT issues that would render publication in a technology/computer information journal). The paper engages considerably with consumer/marketing literature, drawing on, and contributing to recent debates published in the Journal of Consumer Marketing (JCM) and other top-tier marketing journals such as Journal of Marketing, Journal of the Academy of Marketing Science, Journal of Interactive Marketing, Journal of Public Policy & Marketing, International Journal of Market Research. A focus on tourism & hospitality is not uncommon in consumer/marketing literature, on the contrary, there is an array of literature focused on these sectors published in reputable marketing journals, and we engaged with a good range of this literature in our paper, including recent JCM publications (see Petrescu *et al.*, 2020, p. 11; Aguirre et al., 2016, p. 11; Frik and Gaudeul, 2020, p. 14; Hunter and Taylor, 2020 and Weydert et al., 2020, p. 14; and Akhter, 2014, p. 7). Regarding privacy concerns in online services, although many service industries have been disrupted by digitalisation particularly during the pandemic, tourism & hospitality consumers have been most strongly disrupted (see Bahar et al., 2021, published in Industrial Marketing Management), with Bart et al., 2005 (published in Journal of Marketing) also indicating the high information risks attached to travel sectors. To reflect this, we added the following arguments further justifying the focus of our paper (these have been included in addition to the arguments made in the earlier version of the paper which cited

works of Navío-Marco *et al.*, 2018; Tussyadiah *et al.*, 2019, which also justify the focus on T&H, see p. 4):

Page 4-5: The specific significance of consumer privacy research in tourism and hospitality has been recently stressed by Bahar et al. (2021) who emphasise the need for more research in this sector due to the sector's prominent particularities as a data-driven industry, with strong links with the digital environment (Bahar et al, 2021). In addition, although many service industries have been disrupted by digitalisation particularly during the pandemic, tourism & hospitality consumers have been most strongly disrupted (Bahar et al., 2021), with Bart et al. (2005) also indicating the high information risks attached to these travel sectors, for which data privacy is of utmost importance compared to most other industries and sectors (Bart et al., 2005).

Also, the paper has been specifically written to fit the Special Issue in consumer privacy, which, as noted in the call for papers, seeks to publish work that provides a platform for "**organisations and policy makers to re-design, refine, and develop privacy policies to address online [digital] privacy concerns in online services**". The original stakeholders framework developed in our paper does precisely that, and we have now emphasised this in the paper:

Page 6: Beyond the tourism and hospitality realm, the original stakeholders framework developed in this paper has the aim to provide a platform for different organisations and policy makers to shape and refine privacy norms and policies to address digital privacy concerns in online services.

So, we would like to respectfully point out that focusing consumer privacy research on tourism & hospitality should not mean the study has no relevance to consumer/marketing literature published in marketing journals. Rather, the specific industry focus may inform and provide a useful avenue and platform for further research in other service industries and related business contexts:

Page 30: Finally, the proposed framework and resulting knowledge may be transferable and applicable to other online services and related business contexts. Further conceptual and empirical

	studies could be conducted in other service industries to identify and examine potential similarities and differences in organisations' practices of dealing with consumer privacy in a lawful and ethical manner.
2. Relationship to Literature: I appreciate the authors attempt to include more marketing/ consumer oriented references.	Thank you. Indeed, the paper benefited from the addition of more consumer marketing literature to strengthen the rationale and contribution.
3. Methodology: While I appreciate that the authors now state on p. 16 lines 28-40 that ethical data management and data governance have been studies in a range of disciplines but yet in tourism and hospitality - I don't find this a compelling reason for the need of a THO specific framework.	We note that the key concerns raised here are not necessarily linked to methodological rigor / methods, but rather, once again, concerns about the need for a tourism & hospitality focus in the ethical data management framework developed. As we explained earlier, we made further revisions to justify the focus (see point 1. Originality above), and we are confident that we have managed to further clarify the importance of a T&H framework. *Page 17: Although many service industries have been disrupted by online technology, the tourism and hospitality industry has been one of the earliest to be introduced to digital platforms, and one of the most strongly disrupted by digitalisation (Bahar et al, 2021). Researchers contend that data privacy is noticeably more important in tourism and travel than in other sectors, as the frequent practice of providing personal information required for travel reservations and other customer management procedures exacerbate information risk for customers (Bart et al, 2005). Consequently, since online integration and data privacy issues are highly prevalent in this industry, tourism and hospitality provides a rich context for research into the phenomena of data governance and data privacy.*
4. Results: I still see limited contributions of this framework.	We included the following paragraphs to better emphasise the need and contribution of this framework for data governance. *Page 17: Earlier scientific and practice-based studies and reports on data governance suggest that research and publications on traditional data governance approaches concentrate on specific aspects of data governance, with a strong focus on issues relating to the quality of data, data lifecycle, security, and compliance (Yang et al., 2019; Abraham et al., 2019; Ballard et al., 2014; Otto, 2011; Tallon et al., 2014)*

	and less on privacy and *ethical aspects of big data (Yang et al., 2019).* *And so, while traditional frameworks for data governance have been studied before (i.e., frameworks that mainly focus on data quality and the management of traditional structured data sets rather than unstructured, high-volume, high-variety and high-velocity data), Yang et al. (2019) contend that there is a dearth of big data governance frameworks in the literature, and the existing ones are limited as they fail to consider big data environments that attract major challenges in terms of ethical considerations around big data privacy, transparency, and other ethical aspects of data processing by organisations.* *Therefore, the development of a holistic ethical data management and data governance framework that, in addition to compliance-based concerns also consider ethical and social responsibility issues more thoroughly, becomes important.* *Page 5: This is important, as data governance and tourists' privacy has somewhat slight coverage in the UNWTO Global Code of Ethics for Tourism, with the code pointing towards the fact that international tourists are not to be discriminated by any means compared to domestic tourists in terms of collected personal data and information, especially when stored electronically. In this context, the proposed framework can become a useful tool for the various actors of the tourism and hospitality industry, who, nowadays practically depend on operating with big data."* *Page 25: In the era of digital transformation, organisations need a framework for data governance that ensures that* consumer *data and information is used for value creation, not only in accordance with legal requirements, but also meeting* consumers' *expectations. THOs* must *create a culture* that recognises consumer *data* as *an asset and* must *establish mechanisms that prevent the abuse or misuse of sensitive* consumer *data* (e.g., *gender, race, address, health status, personal identification data, etc.)* that *they collect for business decisions, marketing, or service creation and provision (Janssen et al, 2020).*
5. Practicality and/or Research implications: Blue font is smaller than the black font. I do appreciate the added	Correction made to font size. Thank you.

section 5.5 on p. 24-25 which discuss consumer benefits.	
6. Quality of Communication: Minor p. 2 line 13 rebuilt should be rebuild p. 4 line 39 that travelers should be should be do travelers p. 4 line 56 should be consumer/traveler data remove spaces. Also on p. 6 p. 6 lines 20-22 developed is repeated. p. 6 What is scoping - explain. What is ICO - page 13. What are the covid-19 cyber attacks, p. 14 give examples.	Thank you for the constructive comments. We have now corrected all the highlighted minor issues and did a careful full proofread of the paper. We explained what scoping reviews are: *Page 6: ...scoping review of literature has the purpose to identify the scope and extent of existing research on a topic, and to provide an exploratory overview of the topic, in this case data ethics and data governance (Rasoolimanesh et al., 2020). Scoping reviews are increasingly used in the social sciences (Moher et al., 2015), including tourism studies, in order to provide an overview of an under-researched topic and to guide further research in the area (Rasoolimanesh et al., 2020).* ICO (now on p. 14) stands for Information Commissioner's Office and the full term was introduced earlier on page 13. Examples of types of cyber-attacks have been included: *Page 15: ... phishing emails, malicious website domains, misleading "health and safety" emails, disinformation spreading viruses that can produce a range of damages to a system: ransomware, keyloggers or other types of personal information gathering and online scams.*

Reviewer 2

Comments to the Author

Reviewer 2	Response
Dear authors, I found your approach and changes insightful. I have two more comments in the "originality" and "results" section just to make the paper more transparent (e.g. when clarifying what other papers you compare yourself against. Overall the paper reads well in my view and provides compelling ideas.	Thank you very much for your positive comments. We believe the paper has been considerably strengthened following your useful recommendations during the review process and we thank you.
1. Originality: Contemporary and relevant topic that can help guide the practice of big data management. The rational for the creation of the framework (p 16 second paragraph i.e. studies are not present in the tourism industry) can be stronger - maybe enrich it with the ethical based vs compliance based concept you have introduced in other sections of the paper (e.g. p 5).	Thank you very much for this suggestion. We have now added additional arguments which we believe strengthen the rationale for the framework developed. *Page 17: Earlier scientific and practice-based studies and reports on data governance suggest that research and publications on traditional data governance approaches concentrate on specific aspects of data governance, with a strong focus on issues relating to the quality of data, data lifecycle, security, and compliance (Yang et al., 2019; Abraham et al., 2019; Ballard et al., 2014; Otto, 2011; Tallon et al., 2014) and less on privacy and ethical aspects of big data (Yang et al., 2019). Similarly, such previous research consists of literature reviews related to data governance (Abraham et al., 2019; Brous et al., 2016; Lee et al., 2017; Rasoulli et al., 2016), albeit these reviews focus on limited areas of data governance, such as cloud data governance (Al-Ruithe et al., 2019) or agile capabilities of data governance (Lillie and Eybers, 2019), with limited focus on and/or consideration of other conceptual areas (Abraham et al., 2019).* *And so, while traditional frameworks for data governance have been studied before (i.e., frameworks that mainly focus on data quality, compliance, and the management of traditional structured data sets rather than unstructured, high-volume, high-variety and high-velocity data), Yang et al. (2019) contend that there is a dearth of big data governance frameworks in the literature, and the existing ones are limited as they fail to consider big data environments that attract major challenges in*

	terms of ethical considerations around big data privacy, transparency, and other ethical aspects of data processing by organisations. Therefore, the development of a holistic ethical data management and data governance framework that, in addition to compliance-based concerns also consider ethical and social responsibility issues more thoroughly, becomes important.
2. Relationship to Literature: A good variety of practitioner, policy and academic sources.	Thank you.
3. Methodology: The information provided for the methodological rationale for the paper is good.	Thank you.
4. Results: The additions on the distinctiveness of the framework are interesting, still not fully convincing. Could you make more clear what are the other similar frameworks that you compare your against when writing that you follow not only a compliance perspective but an ethical one? Are there other similar frameworks or you generally refer to papers discussing similar issues?	We trust that the detailed explanation of the framework's rationale (as above, p. 17) may benefit in clarifying how our framework is different compared to existing ones (i.e., frameworks that focus mainly on data quality and compliance and less on ethics and trust; with examples from literature). However, we also added the following sentence to reenforce this difference in the results section (section 5): *Page 20: Our data governance framework is different from existing frameworks presented in previous literature as it is developed within a conceptual philosophy formulated around ethics and trust (not just quality and compliance) as key concepts and constructs of ethical organisational data strategies that lead into more ethical approaches to data management by organisations.*
5. Practicality and/or Research implications: Yes, adequately discussed and thought that the consumer implications section that was added was well developed.	Thank you, we appreciate your comments.
6. Quality of Communication: I find the paper well written with clear and logical argument.	Thanks again! We appreciate the comments made.