Configuring The Internet of Things (IoT): A Review and Implications for Big Data Analytics

Susan P. Williams
University of Koblenz-Landau
williams@uni-koblenz.de

Catherine A. Hardy
University of Sydney
catherine.hardy@sydney.edu.au

Patrick Nitschke
University of Koblenz-Landau
nitschke@uni-koblenz.de

Abstract

Big data analytics is emerging as a key initiative in the IoT field as data grows at unprecedented scale and depth. However, considerable uncertainty remains about how organizations are using big data analytics to capitalize on IoT. In this paper we argue that there is a need for a more refined depiction of the relationship between IoT and big data analytics as it tends to be linked by technological and economic viewpoints. Three principal claims are made. Firstly, there is a pressing need to clarify the characteristics configuring and shaping the discourses around IoT. We find that IoT is characterized as a complex, (more than) technological, multi-scale and multi-level information infrastructure that is emergent and uncertain. Secondly, the unique characteristics of IoT are challenging governance capabilities in big data analytics. Thirdly, the impact of IoT through big data analytics for building 'sustainable futures' raises questions about responsible research and innovation.

1. Introduction

The Internet of Things (IoT) has been identified as one of the key drivers in a new technological revolution that is "fundamentally changing the way we live, work and relate to one another" [68:1]. The "seamless integration of the physical and digital worlds through networked sensors, actuators, embedded hardware and software will change industrial models" [77:4] enabling the delivery of new products and services in domains as diverse as urban design [54, 80], manufacturing [29], health [61], agriculture [10] and government [11]. Ongoing developments in the Internet of Nano-Things (IoNT) and Industrial Internet of Things (IIoT), as an example, are accelerating the number of connected devices [18]. It is estimated that by 2025, IoT will create an annual economic impact of USD 2.7 trillion to USD 6.2 trillion [42:51] and that by 2030 "8 billion people and maybe 25 billion active "smart" devices will be interconnected and interwoven by one single huge information network" [51:240]. Further, the "seamless integration of the physical and digital worlds" [77:4] and the increase in embedded technologies brought about through IoT is also accelerating the convergence between operational technologies (OT) that work in real-time on physical systems such as manufacturing and control systems, and information technologies (IT) that support information processing, communication and decision-making to improve the management of business resources.

Big data analytics is rapidly emerging as a key initiative in the IoT field as data grows at an unprecedented scale and depth with the proliferation of smart and sensor devices [8, 16, 40, 45, 53]. Some commentators go as far as to say that big data analytics is driving the "next wave of IoT innovation" [53:64] and making IoT "pertinent to the world" [2:vii] by offering more effective ways for managing and analyzing "notoriously messy" IoT data [45]. Others view IoT initiatives as a disruptor to data and analytics [22], influencing the adoption and implementation of "new and different types of data and analytics technologies and techniques" [20]. Whilst the potential transformational effects of IoT and big data analytics are widely acknowledged, considerable uncertainty remains about these concepts and how organizations are using big data analytics to "capitalize" on IoT [62] to deliver social and economic value [25].

In this paper, we argue that there is a need for a more refined depiction of the relationship between IoT and big data analytics. The paper is not intended to be a comprehensive literature review, but an exploratory essay drawing selectively on literatures in computer science, IT and information systems (IS). Three principal claims are made. Firstly, the two fields of IoT and big data analytics tend to be "linked

URI: https://hdl.handle.net/10125/60020
ISBN: 978-0-9981331-2-6

and bound together" primarily by technological and economic viewpoints [66]. Calls have been made for broadening the scope and diversity of research to assist in bringing greater understanding to issues of a non-technical nature that are related to the emergence of IoT [62]. The big data analytics field is already making advances in developing characteristics and research agendas that include behavioral, design and an economic focus [1, 25]. It is argued that there is a pressing need to clarify the characteristics configuring and shaping the discourses around IoT as the field is still in its infancy and is technology focused [79]. Further, conceptual clarity is a precondition for effectively integrating knowledge between fields [60]. The term 'field' is used here in a conceptual sense rather than to represent professional fields of practice [38] as IoT and big data analytics encompasses a variety of emerging professions and industry groups.

The second claim is that the unique characteristics of IoT are challenging existing governance capabilities in the field of big data analytics [3, 21] and more widely [78]. In a recent survey of CIOs and CTOs, security, privacy, implementation/integration complexity, cost/funding concerns and potential risks and liabilities were cited as the top five barriers to IoT success [22]. IoT presents greater risks due to the complexity and distribution of IoT systems [21]. As IoT is a relatively young and still evolving technology infrastructure, the consequences it brings for individuals, organizations, industries and nations and, in particular, the future implications and requirements for effectively managing and governing IoT are still being shaped. Further, the "synecdoche use" of the *digital* governance term across the fields of IoT, big data analytics and digital development more broadly requires clarification [19]. Floridi [19] argues that in using the digital governance term care must be taken to ensure that other normative matters, namely digital ethics and digital regulation, are understood as separate and overlapping to avoid confusion. Based on the characterization of IoT we examine the implications for governance and in doing so: identify areas requiring further attention for research and practice; and bring further clarity in how the governance term is used.

The final claim is that the shifts in IoT discourses towards more complex systems, the inclusion of social, cultural, political and economic issues and the consequent involvement of multiple stakeholders, are opening the field to a much wider landscape of social and environmental concerns, broadly classified as sustainability. To date research has largely been focused on developing sustainable technology solutions [50] and IoT as a disruptive technology and new source of digital data with the potential to transform business models and industries [14, 34, 49, 63]. The impact of IoT through big data analytics for building "sustainable futures" and "sustainable lifestyles" in areas such as energy management, healthcare, manufacturing, emergency management [62], the environment [39] and smart cities [27] is uncertain and dynamic. Yet, in following Floridi's [19] argument we should "resist" the "distracting narrative" of disruption not because it "is wrong" but "it is superficially right." The pace of technological innovation is no doubt impacting business and society. However, there is a more fundamental question in need of answering in terms of the "kind of mature information societies we want to build" directing attention from "digital innovation" to the "governance of the digital" [19]. The imperative for expanding the boundaries of IS research beyond organizational and managerial impacts is not new [75]. However, more recently social inclusion researchers have posited that IS scholars have a moral obligation to investigate digital platforms to "reveal biases coded in their designs that promote exclusionary practices and prevent equitable work opportunities" and in doing so "propose new and creative designs solutions" that are "sensitive to the values that foster social inclusion and deter exclusion" [75]. This raises questions about responsible research and innovation, which we explore in the context of our characterization of IoT.

The argument is presented in three parts. First, we clarify how big data analytics is viewed in the context of this paper. Second, we examine critical discourses in IoT. Our review is necessarily partial and limited. IoT is notable for its ubiquity across domains and applications and is a dynamic and contested space. Hence, framing the boundaries of the field is a challenge as no singular discourse can define the field. However, there are certain powerful discourses operating in the field that are explored to develop a characterization of IoT. Third, we examine the implications for governance based on this characterization. Finally, we explore questions about responsible research and innovation in IoT and big data analytics followed by the conclusion.

2. Representing big data analytics: An overview

Definitions and labels related to big data, analytics, big data and analytics and big data analytics (to name a few) have evolved over time with technological changes and from different vantage points [1, 14, 16]. For example, Chen et al

[14] classified *(big) data analytics* as one of five "critical technical areas" contributing to *business intelligence and analytics*, the others being text analytics, web analytics, network analytics and mobile analytics. Others have used the labels *big data & analytics* or *big data analytics* to describe the platform that captures and processes large volumes and varieties of data at high velocity and the methods or techniques for revealing patterns, trends and insights to improve business decisions [16, 25]. Much of the literature in this space may be characterized by "its many speculations and opinions" as well as its emphasis on "opportunities afforded by big data technologies" [25]. Whilst still in its nascent stages there have been responses to calls more recently for a more "socio-technical characterization" directing attention towards how organizations are deriving value from big data analytics [25]. In the context of this essay, we adopt the broader socio-technical characterization of big data analytics.

In the IoT field big data and analytics is identified as a function and requirement for IoT [3] providing 'large' scale data management and computational technologies for analysis [66]. In addition, it is also viewed as a challenge of IoT [40, 56] and has similar challenges relating to matters such as privacy and security, data quality, interoperability and business value concerns [3, 56]. A number of reviews of *big IoT data analytics* have been conducted recently in technology related fields such as computer science, engineering and IT [see for e.g. 9, 16, 40, 45, 53]. Whilst useful, these reviews tend to present a mechanistic view and technological focus, with limited attention to the human, organizational and social aspects.

3. Internet of Things (IoT) Configurations

The field of IoT has a strong base in technology-related fields such as computer science, engineering and IT. Bibliometric [46], and scientometric studies [64] and other extensive reviews [43, 48, 74] of the IoT literature have been conducted. In this section, we examine definitions and discourses surrounding IoT. Several studies have presented in-depth analyses and definitions of IoT [6, 30, 32, 44]. It is not our intention in this article to derive a universal definition of IoT. Rather, we examine the characteristics configuring and shaping the discourses around IoT in keeping with the first claim of our argument.

3.1 IoT – complex (more than) technology

Efforts to define IoT frequently begin with a technology focus to describe what IoT is. IoT is typically defined as "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [31:6] and as "a network of items-each embedded with sensors-which are connected to the Internet" [30]. The focus in these definitions is on the software and hardware that enables the embedding of sensors and other technologies into physical things and the protocols, standards and platforms that enable the connection and coordination of "smart" things.

Atzori et al [6] reviewed the various definitions presented in the academic literature and identify three different groupings of definitions of IoT technologies: a "things-oriented" vision, an "Internet-oriented vision" and a "semantic-oriented vision". The things-oriented vision focuses first on the things themselves at the atomic level of sensors, actuators and smart objects, and gives attention to the methods for registering, tracing and awareness (in terms of locations, status etc.) of these objects [6, 7]. The Internet-oriented vision focuses on the networking aspects of IoT that enable vast numbers of heterogeneous, constrained objects to be connected together. Enabling them to communicate with each other and with other systems, and to function in low-power and low bandwidth environments [6, 7]. The semantic-oriented vision focuses on the ways that vast networks of heterogeneous objects and the data that they are creating can be controlled and managed from a technical viewpoint. Semantic technologies and information-centric networking architectures are required to simplify and handle the scale and scope of these vast networks of things and the processes to organize and coordinate search, retrieval, storage and analysis of the vast volumes of data being generated, transported and consumed [6, 7]. The three visions identified by Atzori et al. point to a deep, complex and evolving ecosystem involving many different technologies and stakeholders, including sensor and device manufacturers, network, telecommunications and middleware providers, IoT platforms and service providers, end-users and consumers of IoT services. IoT technology architectures are still evolving [7], as are the standards and protocols for ensuring IoT quality of service delivery [71]. For example, standards and protocols for object naming, authentication, operation of low-power wireless networks, security and privacy [6].

Other definitions of IoT look beyond technology and ask not only, what is IoT? but also, what does IoT enable and for whom? The International Telecommunication Union adopts a broader view of IoT that includes its purpose, defining it as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and

virtual) things based on existing and evolving interoperable information and communication technologies" [32:1]. IoT infrastructure is more than just the technology that it is built upon, it is a vast, complex and evolving system, comprising many millions of nodes, connected across multiple ecosystems with diverse standards and protocols that is enabling the development of a wide range of operations (sensing, actuating, monitoring, controlling, data capture), within and between multiple domains of application and situations of use. It is in essence, a new information infrastructure [26, 47]. An information infrastructure (II) has been "characterized by openness to number and types of users (no fixed notion of 'user'), interconnections of numerous modules/systems (i.e. multiplicity of purposes, agendas, strategies), dynamically evolving portfolios of (an ecosystem of) systems and shaped by an installed base of existing systems and practices (thus restricting the scope of design, as traditionally conceived)" [47]. This characterization of an II can clearly be applied to the emerging IoT information infrastructure (IoT-II) and raises interesting challenges about the nature of, and requirements for IoT governance in such a diverse ecosystem of technologies, users, purposes and practices. Monteiro et al. [47:576] also reason that II's are "typically stretched across space and time: they are shaped and used across many different locales and endure over long periods (decades rather than years)" a characteristic of IoT-II to which our attention now turns.

3.2 IoT – multi-scale and multi-level

In addition to crossing multiple domains and industries, IoT is also visible across multiple dimensions or scales (e.g. spatial, temporal, data, technology architecture, jurisdictional, governance etc.) and at differing levels of abstraction (e.g. atomic, local, regional, global). The IoT-II can be examined at the micro-, atomic level of a single sensor through to the macro-level of a massively connected and integrated, global network of smart things and at all levels in between. In a world where physical and digital things come together, these digitally material artefacts take up a defined position in Cartesian space; a single sensor is attached to a specific tree in a given forest, physical location matters. The data that is captured by a single sensor, may subsequently be shared or aggregated across multiple spatial, temporal and jurisdictional levels and applied to different uses or purposes, increasing the scale and level complexity of IoT and amalgamating data to a point where the exact physical location of the sensor is less important to the purpose at hand. In the scenario presented below (illustrated in Figure 1) we examine the complex and interconnected nature of IoT Information Infrastructures. We begin with a single scale, the data scale and follow the scenario of a homeowner who installs a home weather station provided by a provider of smart home solutions. We follow a single point of data across various levels in the IoT-II from the micro-level of the homeowner with her single weather station, through the meso-level and macro-levels, where other stakeholders, with different data needs and intentions appear. Our aim is to use the scenario to consider the different scale and cross-scale issues that are shaping the IoT-II.

Despite being a very small point in the overall dataset, the data gathered by the single home weather station at a single location and point in time, has a potential impact on a global scale and for a much longer period of time.

Although the example follows just one data stream captured in one IoT domain, it illustrates that moving between scales and levels the data requirements, data consumers, data uses, spatial and temporal reach and scope are changing; raising the potential for challenges to the contextual integrity of the data and its use. The complexity of interactions between different dimensions and levels brings potential challenges for the management and governance of IoT; as the interests and intentionality of stakeholders at one level may not easily be translated or interpreted at other levels. Useful theoretical and analytical insights into ways of accounting for the multi-scale complexity of IoT and for governance in a multi-level world may be drawn from research into scale and cross-scale dynamics conducted in the field of human-environment systems [cf. 12, 13, 23, 72]. Cash et al [12:1] argue that understanding scale and cross-scale dynamics is increasingly important in complex worlds and that failure to take transboundary problems into account has led to many examples of policy failure in human-environment systems. They identify common scale challenges where cross-scale and cross-level interactions threaten to undermine the resilience of a human-environment system. These challenges are equally likely to occur in the multi-level, multi-scale IoT-II illustrated above, where different communities of interest, technological ecosystems and vested interests may overlap, conform and conflict. Formulating approaches to IoT governance may thus require transdisciplinary research approaches that focus attention on the interplay between scales and across levels and represent the theoretical and practical imperatives of different communities.

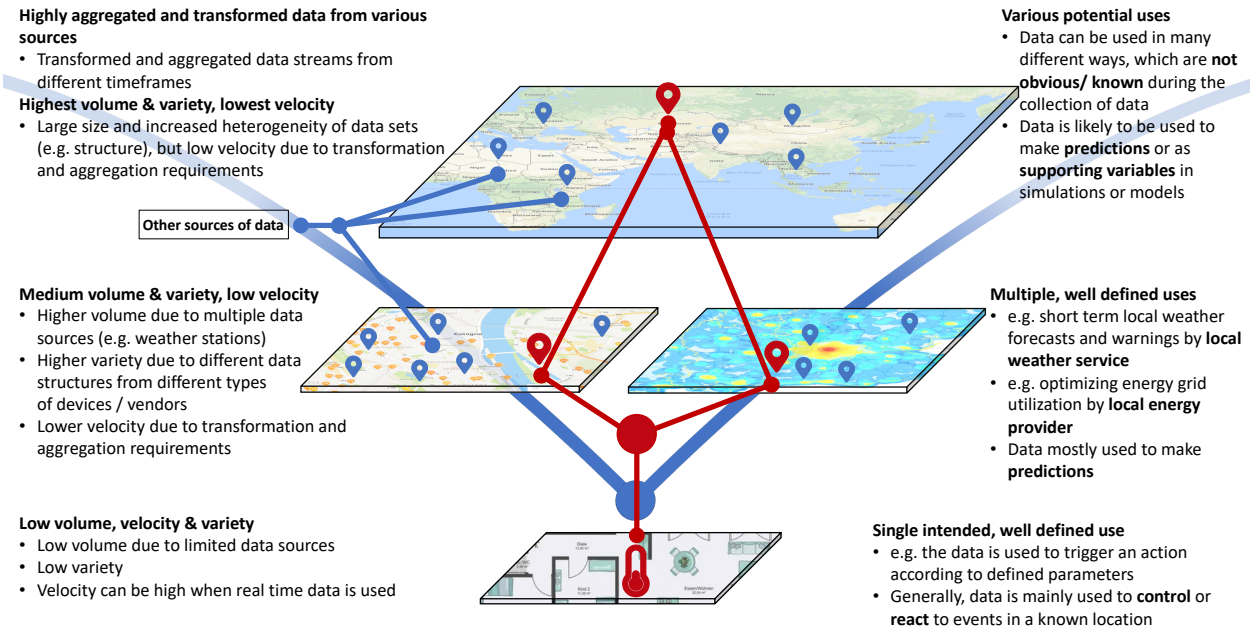

Figure 1. IoT information infrastructure: multi-scale, multi-level

Scenario of IoT Use and Data Requirements

A homeowner installed a home weather station on her balcony to make her home smarter and to control her heating costs. The weather station measures weather data (air temperature, humidity, rainfall etc.), which is used to trigger actions in other sensors and actuators she has installed in her apartment. For example, when outside temperatures reach a pre-specified minimum value a signal is sent to an actuator that automatically closes the windows to save energy. The weather data is captured at the local level of her apartment, a relatively small and clearly bounded 'patch' of the IoT-II. For the required actions to be meaningful, the data being created and acted upon must be available in real-time and the data structures pre-specified. Temperature sensor values and alert levels are defined in degrees Celsius and transferred in JSON format as specified by the smart home solutions provider. The sensor data can then be consumed by the smart window actuator and viewed by the homeowner on her smart phone through a dashboard provided by the smart home solution provider.

The smart home solutions provider aggregates readings from the weather stations of many individual customers in the region. This aggregated spatial data is managed and owned by the smart home solutions provider who sells it to third parties who have very different uses for the data and different data requirements. For example, one use of the data is made by a local weather service, which provides weather warnings to farmers and local councils in the region, such as impending frost events that could damage crops or require roads to be gritted to prevent ice forming. The weather service requires readings from many weather sensors in a region. The data must be in a structured format, individual data points still matter although data coverage may be uneven depending on where individual sensors are located. The region and the boundaries of the region may be imprecise. Whereas the owner of a single weather station only has access to the single readings of her weather station, the weather service combines multiple data-streams along with their geo-locations to visualize weather events (e.g. as frost maps) in near real-time. Another use of the regional data is made by the local energy provider who uses the data in their energy supply prediction models. For example, a sudden cold snap might increase energy consumption by households; by predicting these weather events the energy provider can buy or generate additional energy to manage peak demand or participate in the energy commodity market. The energy provider is interested in data at an aggregate level (for example, city block or the area covered by a specific electricity sub-station) and uses retrospective data to train the predictive models, and real-time data for taking decisions about immediate energy supply. The weather service, the energy supplier and the manufacturer each have a use for the data but with different motivations and end goals and varying data requirements.

At an even higher level the data from multiple regions is aggregated and used by a national weather bureau for weather forecasting and for informing decisions about water saving measures in extended hot and dry periods. Over a longer timeframe a global climate research institute aggregates multiple data sets to feed large scale weather and long-term climate monitoring models and inform climate change policymakers. These activities cover larger areas, and require data from multiple data suppliers, each with potentially different data formats, bound by diverse data sharing agreements and subject to different jurisdictional requirements. The volume and variety of data is much higher at this level as it is aggregated from potentially millions of sensors in different sensor networks. Now the interest of the data consumer is on longer time series of data for guiding future climate change policy, rather than the original purpose of using real-time sensor data at a single point in space to trigger an action to close an apartment window.

3.3. IoT – emergent and uncertain

IoT is frequently characterized as a disruptive technology with the potential to transform organizations [58] and industries [52]; to re-shape value chains [57] and having impact locally, nationally and globally [33, 52, 73]. Porter and Heppelmann [57:67] argue that IoT has the potential to "drive yet another wave of value-chain based productivity improvement" that will "reshape industry structure" and "redefine industry boundaries". At a national level the US National Intelligence Council has identified IoT as one of the six most disruptive civil technologies likely to impact US national power in coming years [73]. The OECD has similarly identified IoT as having "profound implications for all aspects and sectors of the economy, the largest impacts are expected in the healthcare sector, the manufacturing sector, network industries and local government" [52:80].

However, there is considerable uncertainty about these future scenarios and the scale, nature, timing and impact of potential disruptions. The US National Intelligence Council considered the likely impact of IoT on aspects of national power along two major axes: timing of development, that is, whether disruption would occur slowly or rapidly; and depth of penetration, whether IoT would be restricted to niche applications or be ubiquitous in effect. From this analysis, they developed four scenarios for how IoT might evolve towards 2025, along with the potential opportunities and risks that could arise [73:27–28]. The outcome shows multiple possible trajectories and futures for IoT and many unknown factors. The International Telecommunications Union (ITU) also examined the future impact of IoT and envisages high complexity and diversity. Whilst identifying IoT's potential to address various global challenges, such as delivering power, water and sanitation services and managing megacities and natural hazards, ITU concludes that "IoT opportunities are not equally distributed between and within countries" and unlocking the potential of IoT requires significant cooperation between a wide range of stakeholders from different industries and levels of government [33]. Similarly, the OECD identifies potential interoperability issues due to persisting technology uncertainties relating to competing technology standards, technology platforms and applications and has further concerns regarding the costs of IoT, the skills and knowledge required and the potential for social inequality to widen for those nations that cannot keep up [52:82].

In this section, we have identified three different ways that IoT is being characterized; the implications of these characterizations are examined in the following sections.

4. Implications: governance and sustainability

Our characterization shows IoT as (more than) technology, multi-scale and multi-level, and emergent and uncertain. The discussion that follows examines how these characteristics are materially implicated in big data analytics in terms of governance and responsible research and innovation.

4.1 Implications for Governance

Data governance is at the centre of IoT and big data analytics governance. Challenges relating to the effective governance of transactional data, master data and analytical data are further amplified in the IoT-II, at the physical edge, platform and enterprise level. The number and distributed nature of sensor and smart devices, the related volumes of data generated, and the multiple formats and standards that need to be supported present additional challenges, including decisions as to whether existing information infrastructure capabilities may be leveraged or new investments are required to ensure that platforms can scale with need and integrate with business applications at multiple levels [59].

The distributed nature of the IoT-II also presents vulnerabilities and governance challenges in a number of areas relating to security, privacy, data quality, data retention, standards and policy. The nature of these risks and vulnerabilities are not necessarily new to the big data analytics field or the IS community more broadly, with common security principles centered on confidentiality, integrity and availability. However, the "surface for attacks" in IoT-II increases security risks due to the broad external ecosystem in which it is embedded and presenting governance challenges as it is outside of the IT organization's control [59]. Further, organizations operating in the industrial IoT (IIoT) and converging IT and OT settings are faced with additional challenges since "most industries have developed and managed OT and IT as two different domains, maintaining separate technology stacks, protocols, standards, governance models and organizational units" [5]. In the OT domain, safety awareness rather than security awareness has traditionally been the focus [4]. The principle of availability is shared between the IT/OT domains. However, facilitating an integrated approach will also require integrity and confidentiality matters to be

considered each presenting unique circumstances in IoT-II.

The scale and pace at which IoT technologies are generating, collecting and streaming data also introduces data integrity and availability challenges brought about with sporadic connectivity of things and network reliability issues [21]. Assuring the integrity of data of every event generated in IoT is not practical. IoT data collected from multiple sources and their synchronization may present data inconsistency problems. For example, reading event data from a sensor done independently of other data is different to the serial consistency required when comparing it with data from previous readings or the full consistency required when combining data from multiple streams and needing the full context of that data within each stream [24]. Further, data generated from IoT structured, for example, to minimize resource consumption may not be consistent with formats, terminologies or have the metadata of 'traditional' data types with business applications or what is referred to as 'semantic inconsistencies' [21].

While some loss of data in the pipeline may be tolerated from a data consistency perspective [24], this may not be the case in a security context. For example, the operation of critical infrastructures such as power plants, energy grids or transportation could lead to costly downtimes or an environmental catastrophe if critical data was unavailable [21]. Further, the loss of data generated and analyzed about individuals through for example wearable devices may result in reputational damage and liabilities due to commercial confidentiality agreements and privacy regulations relating to the protection of personal identifiable information (PII) [21]. Finally, with constant streams of data the decision to keep everything to satisfy regulations and policies relating to data retention may not be sustainable. Against this backdrop is the question of who owns IoT data, the person who created it, the manufacturer of the sensors collecting the data and/or the owners of the platforms aggregating and analyzing the data [69].

As seen in the above discussion governance processes are "complexly constituted" [19]. Whilst it is widely recognized that innovative and collaborative approaches to governance will be required, there is currently limited guidance as to how this can be achieved. Structures, processes and mechanisms that are well established in the fields of IT and data governance may still provide useful guidance as they are underpinned by similar principles of integrity, confidentiality and availability. However, we argue that as IoT is transboundary, engagement with multiple stakeholders outside of (inter)organizational structures is required. Further meanings and interpretations of values and principles may differ across the multiple scales and levels of IoT. What does stakeholder engagement mean in these contexts? We argue that there is a need for theoretical and empirical development into the *governability* of IoT and big data analytics. The field of interactive governance (IG) [see for e.g. 37] may offer useful guidance, examining, broadly speaking, how the properties of a system to be governed, namely its *diversity, complexity, dynamics* and *scale*, the ability of actors to *participate* and the responsiveness of different governance modes (e.g. hierarchical, self or co-governance) make, in this case, IoT more or less *governable*.

Further the IoT and big data analytics governance terrain is peppered with work that is separate and related to *law and regulations* and *ethics*. Governance may comprise policies and guidelines that overlap with *regulations*. For example, the EU General Data Protection Regulation (GDPR) means that data and analytics leaders need to comply with privacy requirements whilst at the same time meeting demands for more autonomous access to data [17]. Or, the complexity of developing standards for multiple 'things' at multiple scales and levels requiring the coordination of different standards bodies to address the range of concerns from the data format itself to global infrastructures [55]. Coupled with this are *ethical* matters relating to the generation, recording, processing, distribution, sharing and use of data, the algorithms that process and analyze the data and corresponding *practices* and *infrastructures*, including codes, standards and responsible innovation [19]. As an emerging technology, the question for IoT is not simply in terms of attempting to anticipate unforeseen circumstances, a limitation of top-down risk based models of governance, but also to become more responsive to societal needs [36], where our discussion now turns under the umbrella term of responsible research and innovation.

4.2 Responsible Research and Innovation

As discussed above, the design, management and governance of complex and emerging IoT information infrastructures presents a 'grand challenge' as it traverses different scales, levels and involves diverse stakeholders, with different, potentially conflicting intentions, motivations, ethical frames and data needs.

Further, the emergent and uncertain characteristic of IoT raises possibilities for unknown or unintended consequences [73] and uneven or unequitable access

to IoT resources [52]. This presents the "dilemma of control" [15]; where the negative consequences of decisions made today become expensive, difficult or impossible to reverse in the future when they are embedded into the social and economic fabric of the global IoT information infrastructure. Researchers, policy makers and practitioners are required to adopt responsible research and innovation (RRI) approaches [35, 67] to ensure that future risks or negative outcomes of IoT can, as far as possible, be anticipated and prepared for during the technology design and policy making processes surrounding IoT development. RRI is presented as "a meta-responsibility that aims to shape, maintain, develop, coordinate and align existing and novel research and innovation processes, actors and responsibilities with a view to ensuring desirable and acceptable research outcomes" [70]. This requires that designers and researchers consider the future consequences of their design decisions and place greater emphasis on technology assessment and foresight studies [28, 41]. By doing so, to incorporate ethics and reflexivity into the design process [35, 65] and explicitly address matters of sustainability and equitable access to IoT systems, products and services [76].

5. Conclusion

In this paper we frame the field of IoT as (more than) technology, multi-scale and multi-level and emergent and uncertain. Our purpose was not to provide a comprehensive literature review of the field, but rather to examine the multiplicity and fluidity of views and practices through critical discourse to begin laying a theoretical and methodological foundation for advancing research in big IoT data analytics. In doing so we draw attention to a number of issues and examine research implications arising from them by the foregoing discussion. IoT is not simply constituted by technologies, but also by the principles of configuration by which these technologies are organized. The contours of the IoT field are necessarily fluid and contingent as it is a developing field. By providing a more 'malleable' framing of the IoT field rather than a singular conception that presents a simplified picture, we recognize IoT as a complex empirical reality. By undertaking this interdisciplinary review, we have charted a path that provides concepts and dimensions that does not exhaustively catalogue all conceptualizations available but provides an anchor to a research agenda and stimulates debate in the emerging field of IoT and big data analytics.

6. References

[1] Abbasi, A., S. Sarker, and R. Chiang, "Big Data Research in Information Systems: Toward an Inclusive Research Agenda", *Journal of the Association for Information Systems 17*(2), 2016, pp. I–XXXII.

[2] Acharjya, D.P., and M.K. Geetha, eds., *Internet of Things: Novel Advances and Envisioned Applications*, Springer International Publishing, Cham, 2017.

[3] Ahmed, E., I. Yaqoob, I.A.T. Hashem, et al., "The role of big data analytics in Internet of Things", *Computer Networks 129*, 2017, pp. 459–471.

[4] Alaybeyi, S.B., *2018 Strategic Roadmap for Integrated IT and OT Security*, Gartner ID: G00345734, 2018.

[5] ATOS, "The convergence of IT and Operational Technology", 2012.

[6] Atzori, L., A. Iera, and G. Morabito, "The Internet of Things: A survey", *Computer Networks 54*(15), 2010, pp. 2787–2805.

[7] Atzori, L., A. Iera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm", *Ad Hoc Networks 56*, 2017, pp. 122–140.

[8] Bodapati, S., and A. Akila, "Framework of cloud well-being tactics intended for guarding data", *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE (2017), 611–618.

[9] Bossé, É., and B. Solaiman, *Information Fusion and Analytics for Big Data and IoT*, Artech House, Norwood, MA, 2016.

[10] Brewster, C., I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, "IoT in Agriculture: Designing a Europe-Wide Large-Scale Pilot", *IEEE Communications Magazine 55*(9), 2017, pp. 26–33.

[11] Brous, P., and M. Janssen, "Advancing e-Government Using the Internet of Things: A Systematic Review of Benefits", In E. Tambouris, ed., *Electronic Government (EGOV 2015) Lecture Notes in Computer Science*. 2015, 156–169.

[12] Cash, D.W., W.N. Adger, F. Berkes, et al., "Scale and Cross-Scale Dynamics: Governance and Information in a Multilevel World", *Ecology and Society*, 2006.

[13] Cash, D.W., W.C. Clark, F. Alcock, et al., "Knowledge systems for sustainable development", *Proceedings of the National Academy of Sciences 100*(14), 2003, pp. 8086–8091.

[14] Chen, H., R.H.L. Chiang, and V.C. Storey, "Business intelligence and analytics: from big data to big impact", *MIS Quarterly 36*(4), 2012, pp. 1165–1188.

[15] Collingridge, D., *The social control of technology*, The Open University Press, Milton Keynes, GB, 1980.

[16] Dey, N., A.E. Hassanien, C. Bhatt, A.S. Ashour, and S.C. Satapathy, eds., *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, Springer International Publishing, Cham, CH, 2018.

[17] Edjal, R., *Survey Analysis: Data Management Is Pressed Between Support for Analytics – and Data Governance, Risk and Compliance*, Gartner ID: G00351994, 2018.

[18] Ezz El-Din, H., and D.H. Manjaiah, "Internet of Nano Things and Industrial Internet of Things", In D.P. Acharjya and M.K. Geetha, eds., *Internet of Things: Novel Advances and Envisioned Applications*. Springer International Publishing, Cham, 2017, 109–123.

[19] Floridi, L., "Soft Ethics and the Governance of the Digital", *Philosophy & Technology 31*(1), 2018, pp. 1–8.

[20] Friedman, T., *Survey Analysis: Internet of Things Requires Expanded Data and Analytics Capabilities*, Gartner ID: G00273608, 2017.

[21] Friedman, T., and S. Judah, *Data Risks in the Internet of Things Demand Extensive Information Governance*, Gartner ID: G00273608, 2017.

[22] Ganguli, S., and T. Friedman, *IoT Technology Disruptions: A Gartner Trend Insight Report*, Gartner ID: G00331334, 2017.

[23] Gibson, C.C., E. Ostrom, and T.K. Ahn, "The concept of scale and the human dimensions of global change: a survey", *Ecological Economics 32*(2), 2000, pp. 217–239.

[24] Greenwald, R., and K. Guttridge, *The Challenge of Data Consistency and Its Impact on IoT Design*, Gartner ID: G00323867, 2017.

[25] Günther, W.A., M.H. Rezazade Mehrizi, M. Huysman, and F. Feldberg, "Debating big data: A literature review on realizing value from big data", *The Journal of Strategic Information Systems 26*(3), 2017, pp. 191–209.

[26] Hanseth, O., E. Monteiro, and M. Hatling, "Developing Information Infrastructure: The Tension Between Standardization and Flexibility", *Science, Technology, & Human Values 21*(4), 1996, pp. 407–426.

[27] Hashem, I.A.T., V. Chang, N.B. Anuar, et al., "The role of big data in smart city", *International Journal of Information Management 36*(5), 2016, pp. 748–758.

[28] Havas, A., and K.M. Weber, "The role of foresight in shaping the next production revolution", In *The Next Production Revolution*. OECD Publishing, Paris, 2017, 299–324.

[29] Hermann, M., T. Pentek, and B. Otto, "Design Principles for Industrie 4.0 Scenarios", *2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE (2016), 3928–3937.

[30] IEEE, "The Internet of Things" the Connected Revolution.", *The Institute*, 2014.

[31] INFSO D.4 Networked Enterprise, R.I.G.. Micro, Nanosystems, and EPoSS, *Internet of Things in 2020 A ROADMAP FOR THE FUTURE*, Berlin, 2008.

[32] ITU, "Overview of the Internet of Things", 2012. https://www.itu.int/rec/T-REC-Y.2060-201206-I

[33] ITU, "Measuring the Information Society Report 2015", 2015. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

[34] Ives, B., J.A. Rodriguez, and B. Palese, "Enhancing Customer Service through the Internet of Things and Digital Data Streams", *MIS Quarterly Executive 15*(4), 2016, pp. 279–297.

[35] Jirotka, M., B. Grimpe, B. Stahl, G. Eden, and M. Hartswood, "Responsible research and innovation in the digital age", *Communications of the ACM 60*(5), 2017, pp. 62–68.

[36] Konrad, K.E., H. van Lente, C. Groves, and C. Selin, "Performing and Governing the Future in Science and Technology", In U. Felt, R. Fouché, C.A. Miller and L. Smith-Doerr, eds., *The Handbook of Science and Technology Studies, Fourth Edition*. MIT Press, 2016, 465–493.

[37] Kooiman, J., "Interactive governance and governability", In J. Edelenbos and I. van Meerkek, eds., *Critical Reflections on Interactive Governance, Self-organization and Participation in Public Governance*. Edward Elgar Publishing, Cheltenham, UK, 2016, 29–52.

[38] Krause, M., "How fields vary", *The British Journal of Sociology 69*(1), 2018, pp. 3–22.

[39] Maksimovic, M., "Greening the Future: Green Internet of Things (G-IoT) as a Key Technological Enabler of Sustainable Development", In N. Dey, A.E. Hassanien, C. Bhatt, A.S. Ashour and S.C. Satapathy, eds., *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Studies in Big Data*. Springer International Publishing, Cham, 2018, 283–313.

[40] Marjani, M., F. Nasaruddin, A. Gani, et al., "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges", *IEEE Access 5*, 2017, pp. 5247–5261.

[41] Markus, M.L., and K. Mentzer, "Foresight for a responsible future with ICT", *Information Systems Frontiers 16*(3), 2014, pp. 353–368.

[42] MGI, *Disruptive Technologies: Advances That Will Transform Life, Business and the Global Economy*, 2013.

[43] Middha, K., and A. Verma, "Internet of things (IoT) architecture, challenges, applications: a review", *International Journal of Advanced Research in Computer Science 9*(1), 2018, pp. 389–393.

[44] Minerva, R., A. Biru, and A. Rotondi, *Towards a definition of the Internet of Things (IoT)*, 2015.

[45] Minteer, A., *Analytics for the Internet of Things (IoT): intelligent analytics for your intelligent devices*, Packt Publishing, Birmingham, UK, 2017.

[46] Mishra, D., A. Gunasekaran, S.J. Childe, T. Papadopoulos, R. Dubey, and S. Wamba, "Vision, applications and future challenges of Internet of Things", *Industrial Management & Data Systems 116*(7), 2016, pp. 1331–1355.

[47] Monteiro, E., N. Pollock, O. Hanseth, and R. Williams, "From Artefacts to Infrastructures", *Computer Supported Cooperative Work (CSCW) 22*(4–6), 2013, pp. 575–607.

[48] Muralidharan, S., A. Roy, and N. Saxena, "An Exhaustive Review on Internet of Things from Korea's

Perspective", *Wireless Personal Communications 90*(3), 2016, pp. 1463–1486.

[49] O'Leary, D.E., "Exploiting Big Data from Mobile Device Sensor-Based Apps: Challenges and Benefits", *MIS Quarterly Executive2 12*(4), 2013, pp. 179–187.

[50] Ochs, T., and U. Riemann, "Smart Manufacturing in the Internet of Things Era", In N. Dey, A.E. Hassanien, C. Bhatt, A.S. Ashour and S.C. Satapathy, eds., *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Studies in Big Data*. Cham, 2018, 199–217.

[51] OECD, "Data-Driven Innovation: Big Data for Growth and Well-Being", 2015.

[52] OECD, "Science, Technology and Innovation Outlook", 2016.

[53] Patel, P., M. Intizar Ali, and A. Sheth, "On Using the Intelligent Edge for IoT Analytics", *IEEE Intelligent Systems 32*(5), 2017, pp. 64–69.

[54] Perera, C., A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by Internet of Things", *Transactions on Emerging Telecommunications Technologies 25*(1), 2014, pp. 81–93.

[55] Perkins, E., *Securing the Internet of Things*, Gartner ID: G00300281, 2017.

[56] Perumal, K., and M. Manohar, "A Survey on Internet of Things: Case Studies, Applications, and Future Directions", In D.P. Acharjya and M.K. Geetha, eds., *Internet of Things: Novel Advances and Envisioned Applications. Studies in Big Data*. Springer International Publishing, Cham, 2017, 281–297.

[57] Porter, M.E., and J.E. Heppelmann, "How smart, connected products are transforming companies", *Harvard Business Review*, 2014, 60–88.

[58] Porter, M.E., and J.E. Heppelmann, "How smart, connected products are transforming companies", *Harvard Business Review*, 2015, 96–114.

[59] Proctor, P.E., and R. Wagner, *Special Report: Cybersecurity at the Speed of Digital Business*, Gartner ID: G00315580, 2017.

[60] Repko, A.F., *Interdisciplinary research: process and theory*, Sage Publications, Thousand Oaks, 2012.

[61] Riazul Islam, S.M., Daehan Kwak, M. Humaun Kabir, M. Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey", *IEEE Access 3*, 2015, pp. 678–708.

[62] Riggins, F.J., and S.F. Wamba, "Research Directions on the Adoption, Usage, and Impact of the Internet of Things through the Use of Big Data Analytics", *2015 48th Hawaii International Conference on System Sciences*, IEEE (2015), 1531–1540.

[63] Robson, K., L.F. Pitt, and J. Kietzmann, "APC Forum: Extending Business Values through Wearables", *MIS Quarterly Executive 15*(2), 2016, pp. 167–177.

[64] Ruiz-Rosero, J., G. Ramirez-Gonzalez, J. Williams, H. Liu, R. Khanna, and G. Pisharody, "Internet of Things: A Scientometric Review", *Symmetry 9*(12), 2017, pp. 301.

[65] Russ, T., *Sustainability and design ethics*, CRC Press, Boca Raton, USA, 2010.

[66] Sabitha Malli, S., S. Vijayalakshmi, and V. Balaji, "Real Time Big Data Analytics to Derive Actionable Intelligence in Enterprise Applications", In N. Dey, A.E. Hassanien, C. Bhatt, A.S. Ashour and S.C. Satapathy, eds., *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Studies in Big Data*. Springer International Publishing, Cham, 2018, 99–121.

[67] von Schomberg, R., "A Vision of Responsible Research and Innovation", In R. Owen, J. Bessant and M. Heintz, eds., *Responsible Innovation*. John Wiley & Sons, Ltd, Chichester, UK, 2013, 51–74.

[68] Schwab, K., *The Fourth Industrial Revolution*, Crown Business, Cologny/Geneva, 2016.

[69] Shea, S., "The great IoT data ownership debate", 2018. https://internetofthingsagenda.techtarget.com/feature/The-great-IoT-data-ownership-debate

[70] Stahl, B.C., "Responsible research and innovation: The role of privacy in an emerging framework", *Science and Public Policy 40*(6), 2013, pp. 708–716.

[71] Tambotoh, J.J.C., S.M. Isa, F.L. Gaol, B. Soewito, and H.L.H.S. Warnars, "Software quality model for Internet of Things governance", *2016 International Conference on Data and Software Engineering (ICoDSE)*, IEEE (2016), 1–6.

[72] Termeer, C.J.A.M., A. Dewulf, and M. van Lieshout, "Disentangling Scale Approaches in Governance Research: Comparing Monocentric, Multilevel, and Adaptive Governance", *Ecology and Society 15*(4), 2010, pp. 29.

[73] The National Intelligence Council, "Disruptive Civil Technologies Six Technologies With Potential Impacts on US Interests Out to 2025", *National Intelligence Council 59*(April), 2008, pp. 48.

[74] Tiwari, V., "Study of Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", *International Journal of Advanced Research in Computer Science 7*(7), 2016, pp. 65–84.

[75] Trauth, E., K.D. Joshi, and L.K. Yarger, "ISJ Editorial", *Information Systems Journal*, 2018.

[76] Walsham, G., "Are we making a better world with ICTs? Reflections on a future agenda for the IS field", *Journal of Information Technology 27*(2), 2012, pp. 87–93.

[77] WEF, "Deep shift: technology tipping points and societal impact", *World Economic Forum*, 2015.

[78] Wentworth, S., "Internet multi-stakeholder governance", *Journal of Cyber Policy 2*(3), 2017, pp. 318–322.

[79] Whitmore, A., A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends", *Information Systems Frontiers 17*(2), 2015, pp. 261–274.

[80] Zanella, A., N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things Journal 1*(1), 2014, pp. 22–32.