Journal of Information Technology (2018)
© 2018 Association for Information Technology Trust All rights reserved 0268-3962/18
www.palgrave.com/journals

Open

Research Article

Mapping the values of IoT

Razvan Nicolescu[1], Michael Huth[1], Petar Radanliev[2], David De Roure[2]

[1]Department of Computing, Imperial College London, Huxley Building, 180 Queen's Gate, South Kensington Campus, London SW7 2AZ, UK;
[2]Oxford e-Research Centre, 7 Keble Road, Oxford OX1 3QG, UK

Correspondence:
R Nicolescu, Department of Computing, Imperial College London, Huxley Building, 180 Queen's Gate, South Kensington Campus, London SW7 2AZ, UK.
Tel: +44 (0) 2075948242;
Fax: +44 (0) 2075948932
E-mail: r.nicolescu@imperial.ac.uk

Abstract

We investigate the emerging meanings of "value" associated with the Internet of Things. Given the current political economy, we argue that the multiple meanings of "value" cannot be reduced to a single domain or discipline, but rather they are invariably articulated at the juxtaposition of three domains: social, economic, and technical. We analyse each of these domains and present domain challenges and cross-domain implications – drawing from an interdisciplinary literature review and gap analysis across sources from academia, business, and governments. We propose a functional model that aggregates these findings into a value-driven logic of the emerging global political economy enabled by digital technology in general and IoT in particular. These conceptual contributions highlight the critical need for an interdisciplinary understanding of the meaning of "value", so that IoT services and products will create and sustain such concurrent meanings during their entire lifecycle, from design to consumption and retirement or recycling.

Journal of Information Technology (2018). https://doi.org/10.1057/s41265-018-0054-1

Keywords: internet of things; political economy; social, economic, and technical values

Introduction

Internet of Things (IoT) technology has been placed at the vanguard of future digital applications for more than a decade now. Developed around end devices that have the "mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing" (ITU-T, 2012), IoT came to represent complex systems and systems of systems that promise further transformations of the digital economy. Such developments would connect individuals, organizations, and devices in ways that can transform capitalist economies radically, for example, by stimulating collaborative economies, restructuring supply chains, eliminating middlemen, and lowering fixed costs significantly.

It has been argued that IoT will soon become the ubiquitous technology par excellence (GOS, 2014; McKinsey, 2015; Gartner, 2017) with the potential to evolve into Internet of Services and Internet of People. IoT technology promises to revolutionize a broad range of applications in basically all domains of life, from education and health to farming and the aeronautic industry. However, many of the benefits and potential challenges of harnessing the IoT are not yet fully known. Concerns are raised about how developments of IoT technologies would add to the unresolved technical or social issues identified in related domains such as distributed computing and data analytics (Crawford *et al.*, 2014) or crypto-currencies and FinTech systems (Scott, 2016). International standards (e.g. NIST, 2016) and regulations (GDPR, 2016) struggle to make sense of, and keep pace with, the complex challenges posed by IoT. The mass adoption of IoT technology seems to depend on the success of this technology to address the relative reticence of consumers and most market segments to actually embrace products and services enabled by IoT (Thierer, 2015).

This article probes these challenges by discussing the concept of "value" as pertaining to IoT from three different perspectives: social, economic, and technical. This analysis maps out the meaning of "value" in these three perspectives, presents a functional model of IoT derived from this investigation, and argues for the need to consider multidisciplinary methods in developing IoT products and services. Neglect of such an integrative approach would impede, if not prohibit, harnessing the great potential benefits of IoT.

The meaning of value in the space of IoT-connected devices

There is no simple or universal definition of the concept behind the term "value", especially when addressing a dynamically evolving topic such as IoT. The most notable attempts to record and discuss the concept of "value" are perhaps formalized by economists and made popular by the industry and finance sectors. The dominant classic theories of values can be grouped in a labour theory of value, which saw value as being somehow simply generated during the process of productive labour (Smith, 1904 [1776]; Ricardo, 1821 [1817]; Marx, 1906 [1867]). In this paradigm, value formation depended on the availability and the particular dispositions of a handful of key resources, such as land and production means, the processes of commoditization, and commodity exchange. Other theories of value such as the subjective theories of value (Jevons, 1871; Menger, 1871; Walras, 1874) in mainstream economics and the developments around the notion of "value proposition" widely used in the business and management literature show the multitude of viewpoints and approaches to advancing the economic understanding of "value".

Throughout the second half of the twentieth century, the political economy in the West was significantly influenced by Polanyi's (2001[1944]) theory that saw economic value as an abstraction placed at the intersection between the *formal* economy and the *substantive* economy. The *formal* represented the conceptual and normative economy, and the *substantive* represented the practical economy – a relatively simple and organic model for economists, businesses, and the general public alike.

It has been argued that, by the late twentieth century, leading capitalist economies started to focus increasingly more on the formal and abstract aspects of the economy (Carrier and Miller, 1998). For example, the emergence of personal finance products or derivatives markets began to gradually move people away from the structures of the conceptual economics.

On the other hand, social scientists showed that in many societies people use economic value as a vehicle to make sense of different aspects of their lives and sometimes navigate between otherwise incommensurable regimes of value, such as in the case of personal insurance and art markets (e.g. Zelizer, 1987, 1997). In this context, anthropologist Miller (2008) argued for an understanding of value that starts from the way people actually use and conceptualize value. We find this approach particularly helpful to bridge the problematic differences between various domains, transformations, and interpretations of value.

We here apply this approach to value in the IoT space. IoT is spanning across a multitude of geographies, political and economic systems, and cultural norms and practices. It is not the scope of this paper to account for this diversity in relation to IoT. Rather, the paper focuses on the current developments in Western Europe and the USA. It raises concerns that are relevant for this geographical space but that might not be as important in other parts of the world. Nevertheless, the paper highlights principles and insights that may be applied globally.

In refining the above working definition of IoT, the term "IoT" can mean different things to different actors. The values associated with IoT do not merely vary with the more obvious technological, economic, and political factors, but also with behavioural patterns and cultural practices across individuals, communities, and demographics. Research has shown that adoption and appropriation of new digital technologies can represent the outcome of subtle and profound cultural processes that are often unanticipated by producers and policy makers (Silverstone and Hirsch, 1992; Dourish, 2003; Williams *et al.*, 2005). In particular, the design of computing systems and algorithms struggles to keep up with the pace of changes in societal knowledge, populations, and cultural values (e.g. Friedman and Nissenbaum, 1996; Friedman *et al.*, 2008), and the cyber-physical nature of the IoT makes these efforts even more challenging.

We probe these challenges to the concept of "value" as pertaining to IoT through three analytical lenses: social, economic, and technical. These three viewpoints are neither clear-cut nor mutually exclusive, as most mature IoT solutions represent a composition of specific developments that impact and draw from all three viewpoints. Rather, it is the juxtaposition of the social, economic, and technical perspectives that allows for a finer analysis of the processes that, together, create an IoT product or service. Therefore, we conceptualize value as a dynamic process of negotiation between the *theoretical* understanding of "value" as proposed by science and supported, for example, by formal economic systems, and the *use* of values as proposed by industry and sometimes arbitrated by end users themselves. While the limits of a single notion of "value" and approaches for its circumvention are relatively well known and documented (e.g. Anderson *et al.*, 2014), a study on the meaning of "value" in a multidisciplinary perspective of IoT does not yet exist, to the best of our knowledge.

At a higher analytical level, this article focuses on the relationship between current IoT developments and the creation and nurturing of their value. This relationship is continuing and is often dialectical in nature. So, a broader interpretation of value is needed, we argue, to address such a dynamically evolving topic and to balance out mainstream industrial developments with academic research, since each of these domains tends to focus on advancing understanding of different aspects of IoT, such as its cyber-physical nature, the interconnection of IoT systems, or their integration with incumbent and emerging technologies (Stankovic, 2014; NIST, 2016). We will therefore typically use value (without quotes) to grasp the wealth of meanings of this term in the different domains, rather than "value" (with quotes) as a conceptual term within a given taxonomy.

From a technical point of view, cyber-physical systems involve a permanent two-way translation between sensor values and semantically meaningful activities. However, this viewpoint does not make very clear how IoT would make valuable contributions to the overall changes in technology, economy, and societies at large. Instead, we argue that the process of creating and understanding value in IoT has to be interdisciplinary in order to make it available, more transparent, easy to understand and meaningful to larger populations. This approach would develop IoT systems that are economically viable and trustworthy for engineers, regulators, and the general public – where such acceptability may also be a function of local social and institutional culture.

Outline of article

The rest of the article is organized as follows. In "Motivation and methodology" section we present the motivation for this article and the methodology we used in research. In "The new political economy enabled by IoT" we propose a functional model for the IoT ecosystem that aggregates the different findings of our research into a value-driven logic of the emerging global political economy. In "The social viewpoint" to "The technical viewpoint" sections, we examine – respectively – the social, the economic, and the technical viewpoints of values in IoT as proposed by industries and academic research. Each of these sections follows from the review material and is structured into a state-of-the art review and a summary of main challenges, gaps, and further implications in the IoT space. We present the main challenges at a higher analytical level that aims to summarize and focus the previous discussions into key take-away points. The concluding section summarizes our findings and discusses their implications for current and future IoT technology.

Motivation and methodology

The motivation for this article comes from the increased sense that digital technology and IoT, in particular, are currently pushing our societies to accept challenges that do not have absolute solutions, and to transform these challenges into questions about how we order our world (Mayer-Schönberger and Cukier, 2013, p. 184). Researchers argue for greater interaction between technical domains (Stankovic, 2014) and between technical domains and social sciences (Kaplan, 2017). For example, "[m]ost AI researchers naturally focus on solving some immediate problem, but in the coming decades a significant impediment to widespread acceptance of their work will likely be how well their systems abide by our social and cultural customs" (Kaplan, 2017, p. 38). The work we report here is responding to the need to understand and situate the values related to IoT technology in a broader social, economic and technical context.

It has been argued that ethnographic and discourse approaches to technology use and technology development are invaluable to the construction of science and its representation (e.g. David, 2005, pp. 73–89). This points to the need to understand and develop digital technology as dialectics between – on the one hand – control and sociality and – on the other hand – increased autonomy and human freedom.

Our methodology

We responded to all these objectives by first mapping developments, opportunities, and challenges related to the harnessing of economic value in IoT. The data collection and analysis process of this article follows the principles for systematic literature review (e.g. Brereton *et al.*, 2007) applied to the IoT space. We performed a detailed literature review in three main areas: technical, economic and social. This was an iterative process that used a range of primary and secondary sources, from academic publications to governmental, business and consultancy reports. Data collections and analysis were performed by the authors and checked for validity and breadth by two other reviewers. Our interdisciplinary research considered the way different disciplines and institutions analysed mutually understand, accept and inform each other, rather than act as independent "reference disciplines" and contributions (e.g. Glass *et al.*, 2004). We then surveyed a range of risk assessment methodologies associated with economic value in the IoT space. We also followed and reflected on current debates and national strategies in high-priority domains, such as education, health care and the digital skills market. Finally, we identified the challenges and gaps in IoT and focused our subsequent research on these challenges, gaps and further implications as main criteria for selecting which findings to present in this paper.

The new political economy enabled by IoT

The literature on governance of socio-technical systems suggests that in modern industrial societies, individuals and social relations are embedded in economic actions (Granovetter, 1985) and in complex institutional environments (e.g. Hollingsworth and Boyer, 1997; Hollingsworth *et al.*, 2002; Powell and DiMaggio, 1991) in ways that dialectically shape each other. It has been argued that the recent spectacular advancement in digital and social technologies may lead to the increased understanding of information, data and culture as "public goods" (Benkler, 2003), the growth of activism connected to the political economy tradition (Mosco, 2008), and the democratization of innovation and creativity on the emerging "Collaborative Commons" – based less on the expectation of financial reward and more on the desire to advance social well-being (Rifkin, 2014). These processes also involve important developments in terms of assuring fair (Van Dijk, 2005) and unbiased (Nakamura, 2002) access to infrastructures and services across populations in ways that can involve the creation of a "transcultural political economy" (Chakravartty and Zhao, 2008).

In this context, IoT technology seems to add a supplementary level of abstraction to economic and social relations. We use a taxonomy informed by the evolution of ICTs (information and communications technology) into cyber-physical systems (CPS) that have notions and capacity to sense physical environment and the drive to relate logical and physical phenomena to each other. IoTs can be seen as the more ambitious evolution on this chain towards aggregating cyber-physical systems and systems of systems. However, unlike the more popular digital technologies – such as mobile Internet, ubiquitous computing, and portability – IoT technologies are developed simultaneously in different environments, at different levels of society, and often with conflicting scopes. Individual entrepreneurs, small communities, areas of the public sector, and large organizations from major industries (some of them with leading roles in the Second and Third Industrial Revolutions) form a rather diverse IoT ecosystem. The current prominence of IoT is due to the combination of three relatively recent technologies: broadband internet, big data, and smart services. We will discuss how these three technologies have shaped the current values associated with IoT.

The swift success of Internet broadband in the late 1990s and early 2000s represented not simply a consequence of technological advancements, but also a particular combination of regulatory decisions, deployment of critical infrastructure, support from industry finances, commercial expediency, complex control of upstream pricing policies, and short-term technical benefits (Wu, 2003; Krämer and Wiewiorra, 2012; Deshpande, 2013). However, Internet broadband capabilities did not really change the basic pricing models and methods for existing services, such as content distribution networks (CDNs), and peer-to-peer (P2P) content distribution technologies (He *et al.*, 2012). Rather, the new network resources and service pricing were used as effective tools to prompt technical progress, support quality of service (QoS) improvement, and enhance network efficiency. In this context, broadband Internet facilitated solid economic growth (Litan and Rivlin, 2001; Gillett *et al.*, 2006; Czernich *et al.*, 2011) and changed work environment and practices (Bloom and Van Reenen, 2007; Crandall *et al.*, 2007). The cheaper and increasingly more accessible information led to the emergence of a whole range of social and economic values based on fast-acquired knowledge that was transparent and global in nature.

"Big data" refers to major technological and economic advancements in distributed computing, cloud computing, and data generation and analytics. In early 2000s, these advances started to broaden the scope and target of advanced enterprise information technologies, such as enterprise resource planning (ERP), supply chain management (SCM), and customer relationship management (CRM) systems, which have been continually improved over the previous decades (Brynjolfsson *et al.*, 2011). Thus, big data created unprecedented economic value for businesses to innovate business models, products, and services (e.g. McKinsey, 2011; Tambe, 2014). At the same time, most end users started to enjoy the new values brought by big data, which included increased convenience in work and leisure experiences, cloud-based collaborative computing (e.g. Dropbox, Google Drive), and various personalized services (e.g. Amazon, Netflix). However, these values were not uniformly distributed across markets (Shapiro and Varian, 1999) and populations, which accelerated biases (Nakamura, 2002) and divides (Van Dijk, 2005) within society.

Finally, the smartphone revolution was facilitated by advancements in big-data technology that changed existing paradigms in mobile communication and personal computing. Two main perpetrators of these changes, Apple and Google, have set up innovative service ecosystems where several third parties, mainly app developers, hardware suppliers, telecom operators, and key users cooperated systematically with spectacular back-end infrastructures to create useful and attractive services in a relatively short period of time (Constantinou, 2015). Apple and Google created business models that retained most of the value created within their unique ecosystems and that acted as a "network effect" to drive a critical mass of users and key market differentiators. Notably, the "app gap" simply could not be filled by the major incumbent players such as Nokia and Blackberry and by new rivals such as Microsoft. The smartphone revolution innovated in terms of business and user values also because it allowed for the coexistence of services of different scales and purposes, such as big social media and ecommerce providers and smaller developers of free or open-source code.

In early 2010s, IoT emerged as a technology with great disruptive potential, capitalizing on the advances in broadband communication, distributed computing, and smart mobility. However, to a large extent IoT is tributary to the current digital innovations that happen in the technologically advanced societies. These particular economic and social conditions might be conducive for major businesses and for some segments of the public sector, but they are unequally understood and accessed by members of the public and across geographies. These issues simply make IoT not attractive enough for most consumers. Business plans built on the technical capabilities of IoT tend to justify these capabilities rather than innovate for a wider range of populations. For example, controlling one's household systems from the smartphone is not a free and useful service in and of itself. In many domains, IoT is currently struggling to build convincing value propositions devised from the composition of values associated with the social, economic, and technical viewpoints. We offer here the grounds on which an interdisciplinary exploration of the meanings of "value" in IoT can occur.

A functional model for IoT

Figure 1 depicts the model that informs and structures the research presented in this article. At the highest functional level, the current IoT ecosystems could be represented as the juxtaposition of two main spaces that we call, respectively, micro-sphere and macro-sphere. The micro-sphere represents the ensemble of IoT-related things that are visible and recognizable to the average citizen, such as home sensors and wearables. The macro-sphere represents the ensemble of IoT-related devices and processes that are usually accessible primarily to higher-level entities, such as large businesses, corporations, and governments, but also to relatively few highly skilled individuals. The inputs and outputs are parts of a larger system of feedbacks in which technological, economic, and social forces mutually constitute each other and co-evolve. Figure 1 illustrates a snapshot of this dynamic system. For example, the "Requirements" in the right-hand side of Figure 1 represent forces that are part of bigger feedback mechanisms at work in the three perspectives we discuss: the social, the economic, and the technical viewpoints.

In this model, most of the computational effort, the service integration, and the various business flows are enabled exclusively within the macro-sphere. The IoT micro-sphere corresponds to the proliferation of personal computing, mobile communication, and more smart and distributed applications. For example, in the case of Internet, the micro-sphere subsumes the radical innovation enabled by the relatively loose specification of a network architecture (Roscoe, 2006) and the specific increase in individual autonomy reported in the USA (Rainie and Wellman, 2012), while the macro-sphere represents the space where large incumbent and emerging industries use Internet technology to transform business processes and propositions.

What is characteristic for the IoT is the complementarity, interdependence, and co-evolution of the two spheres. For example, innovation in start-up cultures (micro-sphere) needs the infrastructure and support of bigger industrial players and the public sector (macro-sphere). At the same time, major players in the macro-sphere need the levels of flexibility and risk-taking that start-ups can provide and internalize when needed. On the other hand, small businesses, organizations, and research professionals can produce services to balance out the possible social and economic disruptions that might happen in the macro-sphere. This mutual reinforcement

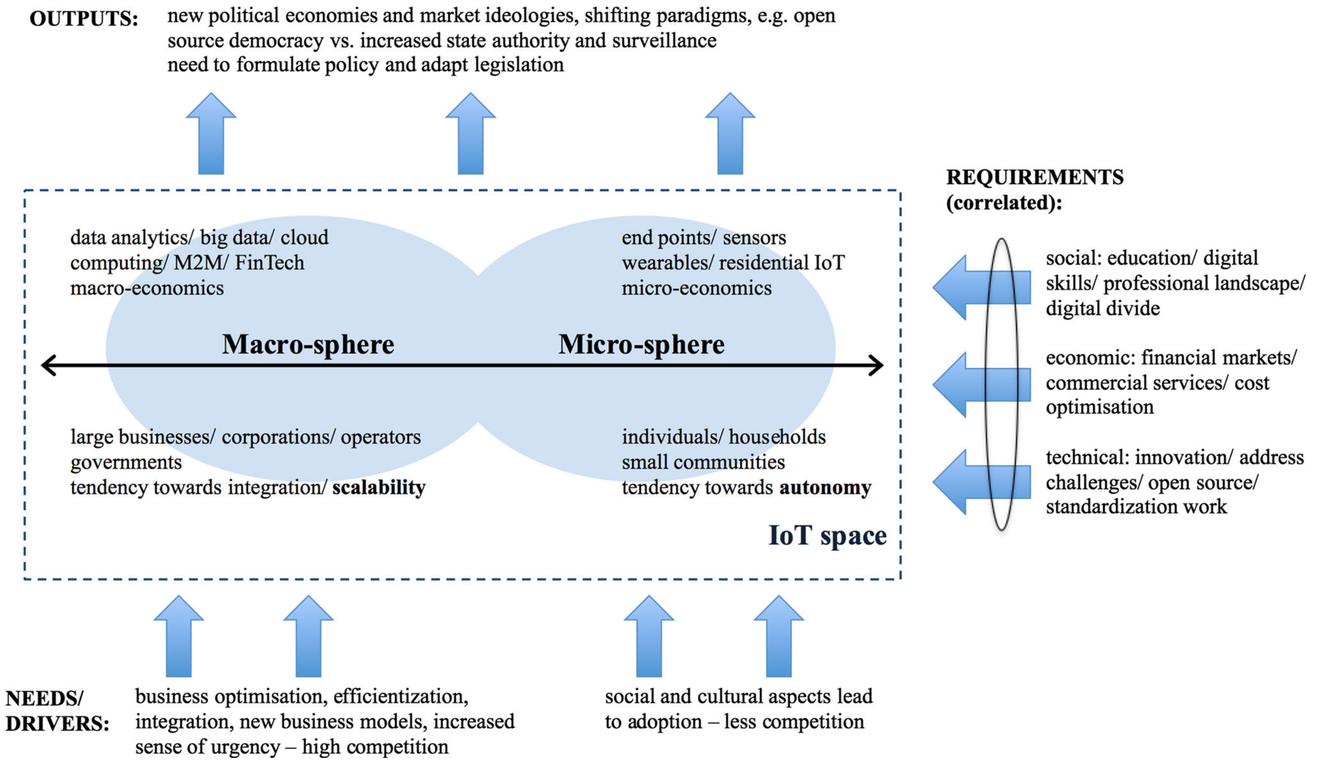

Figure 1 A high-level functional model of IoT ecosystems, showing the interaction and cross-dependencies of two major domains we call macro-sphere and micro-sphere.

between the two spheres is part of the bigger and intrinsic process of cooperation between the (usually) voluntary markets and the (usually) coercive and powerful Western capitalist states (Hollingsworth and Boyer, 1997).

Where the micro-sphere and the macro-spheres intersect, there are different intermediate spaces currently taking shape. These “meso-spheres” would correspond to the needs that are dialectically built at the organizational and community level. The different forces in Figure 1 represent emergent properties that materialize at a level of the social system that transcends individual organizations. Likewise, social and cultural aspects in Figure 1 typically are features that are related to levels of social organization and can thus transcend individual organizations. This discussion is informed by the work on the role markets and organizations have to manipulate information impactedness and opportunism (Williamson, 1975), the possible contractual organizations of economic exchange (Williamson, 1981), and the role and limitations that bounded rationality has in exchanging and processing information (Simon, 1957), especially under uncertainty conditions (Radner, 1968).

The functional model in Figure 1 does not follow any classical segmentation, such as markets into industrial, business, and consumer segments, and domains into public and private. For example, most IoT services for the consumer market are actually created within the macro-sphere and imply complex mechanisms to exchange personal data within an information value chain that could easily span across several economic sectors. Rather, in our functional model actors from one sphere can complement actors and services in the other sphere. Therefore, a major challenge for the IoT community is to be able to build systems that scale efficiently within and between these two spheres. This corresponds to the challenge for IoT businesses to address a specific “vertical” niche versus providing a broad “horizontal” platform (McKinsey, 2015, p. 120).

Our research shows that the proliferation of IoT technologies and related applications, as well as the growing needs for seamless system interconnection and interoperability, typically leads to the organization of the IoT-capable infrastructure into ecosystems that overlap and cooperate with one another. This pushes most implementation efforts in IoT towards the macro-sphere. Thus, promoters of technology focus on service ecosystems, end-point ecosystems, or on more specialized ecosystems such as those for autonomous cars or smart cities. This gap is represented by the existence of relatively little research on the social impact of IoT, including transformations in terms of social values that this technology enables in different contexts. Notable exceptions can be found in product design and in the field of human–computer interaction.

The social viewpoint

The political economy – enabled by spectacular advancements in digital technologies, pervasive computing, and communications – has shifted the conventional understanding of the terms “value” and “economics”, their exchange and circulation; see, for example, the proliferation of crypto-currencies and developments in the field of distributed autonomous organizations (DAO). At the same time, it took decades for computing to be recognized as “something having a history, rather than just being permanently in a state of improvement" (Fuller, 2008, p. 7). In the case of IoT, research shows that present IoT technology similarly lacks essential cultural and social sensitivity, including inclusion and (re)distribution of digital resources. We structure the main findings of our mapping exercise for the social viewpoint in three main subsections.

The social limits to technological advancements

Although science, technology, and society arguably inherit a common core of problems and methods (e.g. Latour, 1987), the current IoT market is pretty much driven by technology itself. This drive is supported by a number of growing adjacent disciplines and specializations, such as user experience, human–computer interaction, design informatics, and digital anthropology. What these disciplines share is a particular attention directed towards a broad range of social values that go well beyond technological and economic discussions. For example, anthropologists Miller *et al.* (2016) have shown that the use of social media in nine different global contexts is neither influenced by technology itself (which is similar across most sites) nor by the local economic conditions (which can be very different), but rather by the social use of this particular technology in each of the communities studied. The authors suggest that it is the sustained exercise of particular values related to social relations, education, aspirations, and happiness that continuously change social media as a technology.

There is an important body of research on the challenges computing systems and algorithms face to accommodate the diversity of human values and behaviour. Research shows that many computer algorithms implicitly or explicitly comprise essential value judgements (Kraemer *et al.*, 2011). This means that designers of algorithms who accept different value judgements may have a rational reason to design algorithms and products differently or are oblivious to such differences having undesirable impacts. The ethical implications of algorithms (e.g. Kraemer *et al.*, 2011; Mittelstadt *et al.*, 2016), cloud computing (De Bruin and Floridi, 2016), and information transparency (Turilli and Floridi, 2009) are crucial for the present social transformations driven by digital technologies, yet these implications are modest and uneven in practice. Even if designers of technology can transfer their ethical views into the technology itself, adopters of technology might simply not share these ethical values. For example, communities that emphasize cooperation and collaboration as core values can reject technologies designed to reward individualistic and competitive behaviour, even when these values are embedded in ICTs in ways that are rather opaque for users.

Research shows that IoT currently tends to become a utility with increased sophistication in sensing, actuation, communication, control, and in creating knowledge from vast amounts of data (Stankovic, 2014, p. 8). This has disruption potential for the existing models of IoT, for example, by challenging the existing data-silo architectures that have limited transversal communication or by exploring new sources of economic value in emerging ecosystems (e.g. Pang *et al.*, 2015). This dynamics can result in qualitatively different consumption patterns and lifestyles from those imagined by the designers and perpetrators of technology. In this context, alignment of technological development with social and cultural values in the IoT space should be considered in terms of social and cultural variations across populations. Support for social sensibility requires adaptive control and design to incorporate human behaviour that is essentially changing over time and space.

This discussion points to the more general challenge to increase the transparency and human understanding of different pieces of technology that are seen by many human agents as black boxes. Presenting and explaining IoT data to non-digital natives and the capacity of IoT systems to collaborate with humans in meaningful and safe ways are key to establishing trust in this technology. This perspective is close to the current efforts to explaining and making AI models more transparent and manageable (e.g. DARPA, 2016; Ribeiro *et al.*, 2016; Wang *et al.*, 2016).

Social diversity and inclusion

Many IoT solutions are currently developed to address an idealized type of end consumer and ignore possible important variations, including those in geography and community. Such an approach represents a challenge for IoT solutions that aim at reaching multiple different consumer markets. This raises the issue of social interpretation of data as a key component in complex systems and as an important simplified sub-class of social computation. While a television set may be universally acceptable and usable for a diverse global population, it is questionable whether IoT solutions such as those that support smart cities can attain similar universal status. Technology platforms may well be installable in different cities and their cultural spaces, but it is not clear at all whether local communities would adopt such productization or whether they will prefer platforms that reflect local culture, history, or other specific value-centric factors.

Moreover, end users are faced with an unprecedented collapse of what they perceive as very distinct, if not opposite, spheres such as public versus private, autonomy versus dependence, privacy versus sociality, or specialization (vertical market) versus non-specialization (horizontal markets). For individuals, these traditionally opposed categories have very different social and cultural meanings, and – for that matter – correspond to clearly distinct economic values. Traditionally, businesses know how to render these meanings into value points or market values, or they go on and adjust business propositions in order to be consistent with the social and cultural interpretations. In contrast, IoT-enabled solutions often have unclear economic value in terms of their meaning and perceived utility to end users. For example, the value that retail customers co-create with IoT technology increases with their familiarity and ability to use IoT technology and decreases with their technology anxiety and their need for personal interaction (Balaji and Roy, 2016). The analysis of such processes is critical to understanding the social consequences of mass adoption of IoT and the implications to different populations, such as those with very different social and economic backgrounds.

We suggest that such an analysis should be applied to each IoT product, service, or platform. Security concerns, for example, do not simply vary with the criticality of end applications, but may have different value points for each category of consumers and community. We thus identify an important gap between the way IoT technology is designed to function and the way consumers actually perceive and appropriate it. We believe that understanding this gap would help the IoT industry deliver products that are more meaningful and valued by people.

Changes in the professional landscape facilitated by IoT

Almost 90 years ago, economist John Maynard Keynes famously predicted that widespread technological unemployment is "due to our discovery of means of economising the use of labour outrunning the pace at which we can find new uses for labour" (Keynes, 1931, p. 360). Current estimations show that large-scale development of IoT systems and spectacular advancement in computing will create important changes in the professional landscape. In a recent report, the World Economic Forum estimates that 65% of the children that start primary school today will end up working in jobs that do not yet exist (WEF, 2016). In the UK, the Bank of England predicts that up to 15 million jobs could be at risk of automation in the medium term because of advances in Artificial Intelligence and Robotics (Haldane, 2015). In a recent report, the World Economic Forum shows that a major part of the global industry expects that around 5 million jobs will be cut between 2015 and 2020, also as a result of technological changes that would happen between 2015 and 2017. The top four changes are, respectively, mobile internet and cloud technology, advancement in computing power and big data, new energy supplies and technologies, and the Internet of Things (WEF, 2016).

The digitization of work processes and environments is expected to mean that a double-figure percentage of the total employments are at risk in the next 20 years in the UK and USA (e.g. Frey and Osborne, 2017). Technological unemployment is already happening in both routine and non-routine manufacturing tasks (e.g. Brynjolfsson and McAfee, 2011). These developments happen in a context in which many jobs are based on building trust or rapport with other people (Kaplan, 2017). Therefore, value consists not simply in technology itself but also in the way people valorise their actual work and the social relations enabled by work.

In the UK, the challenges to secure digital skills (DCMS, 2016) overlap with more systemic problems of the British labour market. For example, economists showed a trend over the past decades towards polarization of the UK labour market: with growing employment in high-income cognitive jobs and in low-income manual occupations, while in the middle-income routine jobs employment falls dramatically (Goos and Manning, 2007). Efforts to increase digital literacy skills should therefore start from the systemic problems when aiming to reduce the economic and social inequalities.

In this context, IoT poses supplementary challenges to future digital markets and consumers. Application developers, for example, currently face a lack of support to bring IoT-enabled services to their full potential (Mineraud *et al.*, 2016, p. 10). Research suggests that primitives for querying the data stream catalogues and for fusing and aggregating data should be available to developers in order to speed up and simplify cross-platform development of data-centric IoT applications. Importantly, the General Data Protection Regulation (GDPR) will become law in 2018, requiring that data controllers are compliant with strict privacy controls. These are other examples of transversal gaps that cross multiple domains and articulate concurrent notions of value.

It is argued that the associated social disruptions will be significant in the short term, as technologically driven labour market transitions would take considerable time, while domains such as Artificial Intelligence and Robotics will accelerate the pace of automation (Kaplan, 2017). But industries argue that new technology and innovation will create more jobs. While this may well be true, the issue will be how well the workforce will cope with leaving traditional roles and learning new skills for future job roles. This represents a complex social and cultural process to appropriate new technical requirements and undertakes professional reconversion and possibly physical relocation. Implementing such changes while maintaining the social contract of some economies can be challenging, especially for existing small and medium businesses and for parts of the public sector.

Main findings pertaining to the social viewpoint

The main challenges and gaps in the current IoT landscape with major social implications are:

Disruptive technology should not mean social disruption

The impact of IoT and related technology on the existing social contract or citizen rights in different international and national contexts is understudied. National and international legal systems and policies should consider balancing out the economic advantages brought by IoT technology with social rights.

Securing the digital skills required by proliferation of IoT

Coherent and inclusive educational strategy would reduce "digital divides" across communities and professional groups. Training in coding and in developing IoT technology can start from the age of seven, say, while new study subjects that focus on creative and social intelligence, as something least likely to be replicated by conventional algorithms, should be set up (Frey and Osborne, 2017). The British Computer Society's Computing at School group is already active in that space, as are similar such groups in other territories.

Collaboration with human agents

Many IoT systems are required to collaborate with humans, which includes learning and reacting to unpredictable, unexpectedly absent or malicious human behaviour in a meaningful and safe way. We do not know how to quantify the values of such collaborations at design, implementation, and assurance stages.

Integrating multiple social values into a complex socio-technical system is challenging

Social and cultural values can be competing with each other when they are considered outside their typical context, e.g. on a global scale, and may depend on issues that are not directly addressed by the IoT technology, such as local governance and ethical aspects considered at different social or professional levels.

Social adoptability of technology
IoT technology promises to improve crucial aspects of everyday life, which most people do not necessarily associate with economic value. Social adoptability, acceptability, and social integration represent key values that determine economic value of IoT. However, we currently do not understand this relation well enough.

Understanding the value and gaps between individuals' privacy and IoT systems that process personal data
This may be partially addressed by regulations such as EU's GDPR and the EU-US Privacy Shield framework. However, it is unclear whether the principles of GDPR can be mapped onto current ICT and IoT systems.

Lack of legal and regulatory clarity
Legal rights, including ownership rights, accountability, and liability are still to be defined and reinforced in IoT ecosystems, particularly since territorial law may act as a potential obstacle to global IoT integration.

Current lack of adoption
There are issues pertaining to trustworthiness, public opinion, understanding the social benefits, and commoditization of IoT technology. The consideration of routines and human or social group-centric behaviour in domestic settings, as currently considered in the design process, should be extended to other social contexts.

The economic viewpoint

Financial markets are now technology-centric. This context shapes the way humans bring value and justify their own meanings of "value" to these markets. An employee may offer value by his or her ability to find, process, interpret, and deliver data. But that same individual may also increase their sense of self-consciousness in relation to managing personal data, which might have complex and unpredictable consequences.

Economic strategies

Many of the benefits of IoT have public or quasi-public character, for example the benefits of smart transportation and smart city technologies on environmental quality and on public safety. This raises considerable challenges for finding business models to finance investments in such technologies. The service models associated with enabling healthier, safer, and greener environments in urban and work contexts are still in their infancy (e.g. NIST, 2017a). Businesses and the public agencies that run large IoT live demonstrators currently struggle to find ways to recover the operating costs for IoT-enabled services. This is often the case when the benefits brought by IoT are studied in a top-down approach, while it is not clear to what extent the general public would be happy to actually pay for smarter services. In some areas, platform businesses have been able to internalize such externalities and build sustainable business models. For example, Alibaba, Baidu, and Tencent are currently leveraging on the immense personal and transactional data they have and offer personalized and segmented financial products, such as micro-credits and insurance policies that can be highly effective in the context of the emerging Chinese political economy.

In this context, the current economic modelling of IoT ecosystems is rather poor. The efforts to integrate the three major technologies discussed – broadband, distributed computing, and mobile communication – into industrial and consumer IoT markets are in their infancy. These efforts are also subject to multiple conflicting demands such as simultaneous competition for standards versus competition within standards. The economic modelling of IoT tends to have a dominant focus on technology and macroeconomics and can easily overlook crucial micro-economic and social aspects. For example, the current work on pricing models for IoT applications is developed for particular segments of the IoT architecture and focuses either on rather specific service configurations or on generic representation of functionalities, which does not support true end-to-end business models (e.g. Luong *et al.*, 2016; Mathur *et al.*, 2015). We note that empirical studies on the value creation associated with IoT technology are in still their infancy (e.g. Balaji and Roy, 2016).

The commonly used economic and pricing strategies in developing IoT systems can be categorized into three groups, based on how to set the price: economic concepts-based pricing, game-theoretic and auction-based pricing, and optimization-based pricing (Luong *et al.*, 2016). The economic concepts-based pricing strategies are grounded in the classical economic concepts such as cost, profit, demand, and supply functions. The game-theoretic and auction-based pricing are based on formal study of decision-making where several players, such as buyers of sensing data, sellers, or service providers, must make choices that potentially affect the interests of other players (Luong *et al.*, 2016).

In different markets, challenges can be less about how to generate incentives to contribute data, and more about how to balance the contributions in multi-sided markets or how to control the degrees of ownership and openness in processing, transacting, and monetizing data. Pricing strategies in platform markets, for example, imply responses to two sets of constraints, as each side of the platform can be both a consumer of the service and an input of the service offered to the other side. This dual competition may generate complex strategies using cross-subsidies, a departure of prices from marginal costs, and suboptimal pricing strategies for the intermediary platforms (Weyl, 2010). In particular, industry platform owners face the dilemma to promote long-term innovation versus short-term appropriation (Tiwana *et al.*, 2010).

Businesses are increasingly using big data and data analytics to "make sense" of who their existing or potential customers are and what they might want. This can be viewed as part of the information economy, which emphasizes the emergence of economies of scale on the demand side, network economies, and reduced or minimal (re)production costs (Shapiro and Varian, 1999). These economic priorities raise important concerns related to the privacy, security, and protection across the social spectrum, be these institutions or individuals. For example, anonymized large-scale financial metadata can easily be re-identified from a handful of spatio-temporal pieces of external information (De Montjoye *et al.*, 2017). Furthermore, the process of re-identification varies substantially with gender and income, which poses critical ethical questions about the fairness of business models that are based on the exchange of personal data. But empirical research on the customer trade-off between privacy and monetary incentives shows that individual privacy decisions can be malleable to endowment and order effects (Acquisti *et al.*, 2013). The estimated valuations of privacy are larger when individuals consider trading personal data for money and smaller when people pay money for privacy (Acquisti *et al.*, 2013).

In this context, data analytics service providers might be driven to rethink privacy and trustworthiness as core values for big data (D'Acquisto *et al.*, 2015). They will have to promote professionals who can not only understand and capitalize on personal data but also prevent its commodification through, for example, an increase in its availability. At the same time, these efforts have started to be challenged by the development of containerized personal databases, or data boxes, that allow individual users and communities to collect, mediate access, and exchange personal data (Chaudhry *et al.*, 2015; Ng *et al.*, 2017). In the UK, Ng *et al.* (2017) have proposed such a self-regulating and self-reinforcing ecosystem based on open-source approaches that would allow greater control over personal data usage and would create and perpetuate trust across different actors involved. This approach would also avoid price gouging and could attract a variety of funding, including private and community investments, private equity, venture capital, and public offerings. Data generated by privately owned IoT systems could enhance the scope and resilience of, and add value to, such personal data ecosystems.

Harnessing economic value from IoT platforms is related to the consolidation of multiple business ecosystems in which competition is not driven solely by conventional economic strategies, but increasingly by social and cultural factors. In such ecosystems, the buyers, producers and suppliers of products and services, middlemen, financial and social organizations, and local communities jointly provide a variety of applications, products, and services to each other. Such platforms should be easily expandable and provide incentives for contribution by developers, promoting a bottom-up development of the ecosystem (Mineraud *et al.*, 2016). Without coexistence of distributed and scalable models that rely on more than direct economic interests, the IoT ecosystem could soon become an increasingly fragmented space. Also, many economic models may then be highly volatile, vendor dependent, and less transparent to those who do not own them or partner with such owners.

The scarcity of business models

New or adapted business models could be enabled by the use of IoT systems to co-create value in a service-dominant (Vargo *et al.*, 2008; Vargo and Lusch, 2016) or customer-dominant logic for marketing (Heinonen *et al.*, 2010). However, most of the business models in the IoT space are empirical (e.g. Breidbach and Maglio, 2016) or conceptual (Gubbi *et al.*, 2013) in nature. Such literature focuses on parts of the overall business environment and does not consider the effects that a low or nearly "zero margin economy" would have on the classic labour theory of value. Rather, the actual implementation of IoT implies creation of, and participation in, information marketplaces (IM) that allow exchange, mining, processing, and interpretation of personal data (Höller *et al.*, 2014). These successive processes transform data generated by IoT infrastructure into active economic agents and generate dynamic information value chains (Höller *et al.*, 2014).

IoT businesses also struggle to establish asymmetric business models, for example, to identify complements that could be commoditized in order to create value and drive growth for their core business. What seems to be more critical for industries is that elements of scale and intentional design hold a series of risks, including fixing a narrow range of values and overlooking critical social and governance needs that are able to evolve and also to mediate between diverse and conflicting values systems (Miorandi *et al.*, 2014).

IoT business models may become attractive and viable when businesses manage to create systems that offer automated, autonomous, and intelligent trustworthiness mechanisms that ensure privacy, security, and other aspects important for the resiliency and acceptability of the products and services that rely on them. One such development is represented by the extension of existing machine-to-machine (M2M) services into the IoT space. However, this move implies fundamental transformations to M2M businesses, such as transition from essentially proprietary to partly non-proprietary solutions, from application-specific devices towards application-independent devices, integration of and increased reliance on web services, and possibly important levels of adoption of open standards and interfaces, and active involvement of developer communities (Höller *et al.*, 2014, pp. 30–31). Such dynamics would lead to more complex adoption of dynamic pricing and non-uniform (differential) pricing, which prices resources and services differently based on the type, time, and location of usage.

Economic costs and the "productivity paradox"

The costs of designing, implementing, and maintaining IoT systems could be unpredictable and increase with each solution, due to different factors, such as resiliency, emerging security threats, or support for legacy systems. Most current business models do not take such factors into consideration. Technical IoT solutions will also, in the short to medium term, incur costs for testing of devices, connectivity, radio signals, and so forth, and these costs are hard to quantify. This leads to a latest manifestation of the "productivity paradox" noted for ICT. This term is commonly associated with the discussion following Robert Solow's 1987 quip: "you can see the computer age everywhere but in the productivity statistics" and addresses key issues such as the lag between investment in technology and productivity gains. In the decade of ICT, for example, empirical evidence suggests that productivity gains due to ICT are lower than those known from earlier general-purpose technologies (Gordon, 2016). In contrast, current consulting studies suggest that IoT and AI might boost productivity impact of ICT (e.g. Purdy and Daugherty, 2016). However, we do not really know how the balance between investment in IoT and productivity gains would actually look like in the midterm future.

The productivity paradox can be addressed in a variety of ways. ExxonMobil and Lockheed Martin currently work on an open, but standardized, secure and interoperable process control system that represents, they argue, the economic and scalable alternative to digitizing the entire plant production with an integrated solution offered by one vendor (Montague, 2017). The new open process control system would use open architectures and virtualization so that partner and client companies can pick and match components to digitize their infrastructure and services. Indeed, theorists and business professionals advocate for hybrid architectures that optimize a series of costs for delivering resources and services (such as the unit cost, opportunity cost, delivered cost, and total solution costs) as well as understand, manage, and price risks (e.g. Weinman, 2012).

Such radical transformations cannot be easily managed unless system integrators have sufficient scale to understand the huge number of technologies well enough to integrate them fully on behalf of customers, and an ability to capture the added value created in the emerging industrial structure. The added value assures the capital flows required for R&D investment to enable participation in the systems integration market (Höller *et al.*, 2014). In this context, "value" consists in the consolidation of technical and economic capabilities in the macro-sphere. It is likely that the largest industrial actors and new system integrators will drive this process.

The direct economic risks in this space reside in the volatility of the rather immature IoT markets. Important financial incentives in both macro-sphere and micro-sphere tend to replace the modern economic models based on value proposition and economic costing. The 2016 DDoS attacks that exploited simple but poorly secured IoT end devices, such as baby monitors with immutable default passwords (Burgess, 2016), show that the model of low-cost, low-security IoT solutions may not be sustainable and thus not valuable for the general public. It also points to the need of sharing and enforcing best practice at global scale and invites more research, standards development, and collaboration in the accountability and liability domains.

Major players in the macro-sphere have the capacity to build secure environments in which IoT data can be safely harnessed and monetized directly by trading mechanisms or indirectly by creating revenue-generated services or increasing accuracy. The FinTech sector, for example, aims to use IoT data to improve predictions and perform better risk assessment in sensitive markets, such as derivatives markets. However, there is relatively little work on the economic impact on cyber risk related to IoT. It is particularly difficult to quantify this impact because of the lack of suitable data and the lack of universal standardized frameworks to assess cyber risk (Koch and Rodosek, 2016) and because historical measures will not work in a risk environment that is changing fast (DiMase *et al.*, 2015).

Creating economic value

The interconnection discussed in the previous section facilitates the ubiquitous flow of smart data generated by various value-creation factors, such as equipment, humans, organizations, processes, and products (Stock and Seliger, 2016). Such factors can then be assembled in value-creation modules, which – at the higher aggregation layer – may constitute a smart factory. In an Industry 4.0 context, the horizontal integration represents the dynamic establishment of a network of value-creation modules that transcends the physical borders of a smart factory. The economic value of IoT can thus be neither fixed nor restricted to particular business owners. Rather, economic value is created throughout the process of data exchange in ways that are non-transparent to end users and to most entities involved in this exchange. This process includes creating virtual representations of products, processes, and machines, which can transfer and account for different kinds of knowledge between each other.

Privacy is one of the main concerns related to data processing. To ensure that maximum economic value can be harnessed from the IoT, future IoT solutions should have algorithms and mechanisms by which data owners can specify and control consent to data access or transfer of data to different controllers – as demanded by the GDPR legislation. Ideally, the raw data would remain under the control of the data owners (Mineraud *et al.*, 2016), which would trigger questions regarding data pollution and data ownership in situations such as the death of the data owner or erroneous data transfer. There are multiple security and privacy concerns about the effects of IoT and cloud computing integration, the main concern being the interoperability of the two areas (Díaz *et al.*, 2016). In such scenarios, pre-processing data techniques and data mining algorithms present visible advantages over open-source projects and enterprise products (Díaz *et al.*, 2016). While these techniques can reduce data pollution, they also need an understanding of the cost of data storage. More generally, IoT technology that incorporates privacy-by-design or privacy-enhancing technology from the ground up will increase its social and economic value; for example, it can help to make IoT-enabled digital systems GDPR compliant.

The economic value of IoT platforms stems from their ability to connect a mass of diverse sensing and actuating devices, each with different constraints and capabilities. The corresponding gap in the IoT platforms is represented by the lack of communication standards and communication protocols. An ideal IoT platform would offer a pool of standardized communication protocols, with IoT devices being able to select appropriate protocols (Mineraud *et al.*, 2016). Instead, the critical fragmentation between protocols utilized for communication within and across resource-constrained and resource-rich devices is not foreseen to change in the near future (Al-Fuqaha *et al.*, 2015). Hence, standardized integration of sensing and actuating technologies is a main gap for harnessing economic value from the IoT.

The lack of established, dedicated IoT marketplaces restricts the potential for creating economic value in this space. Current application stores, for example, only support the delivery of purchased software to mobile terminals supported by a specific platform. While some IoT platforms have dedicated application stores, not many allow applications to be publicly shared, and only few vendors promise to enable the usage–charging of the end users of these applications. These gaps need to be addressed with the creation of standardized and dedicated IoT marketplaces (Mineraud *et al.*, 2016). Solutions could be pursued in the integration of IoT with cloud computing (Cavalcante *et al.*, 2016; Díaz *et al.*, 2016). But the past 3 years have seen only limited research on these themes.

Main findings pertaining to the economic viewpoint

The main challenges and gaps in the IoT space from the economic viewpoint are:

Lack of reliable models for multi-modal values of IoT systems
We need models that can represent multi-modal values and their interactions to support decision-making. Many IoT applications can create non-monetary value, typically in health and education systems, which could impact key economic values, such as reducible public health spending.

Lack of reliable methods for identifying cost factors/quantities for IoT systems' lifecycle
The dominance of financial mechanisms for the digital technology over more conservative costing models favours technical capabilities over market needs. Many cost factors of design, implementation, and operation are unknown or inadequately assessed.

Ill-understood trade-offs between technical and social capabilities and economic costs
Providers of IoT solutions face the increased pressure to build solutions that are able to scale and cover very different, and potentially conflicting, needs. There is a demand for better modelling and analysis capabilities to support decision-making in this space.

Better understanding the risks and opportunities of IoT technology fragmentation
Harnessing economic value from IoT might be impacted by the existence of multiple competitive IoT ecosystems that could form an increasingly fragmented space in which economic models are likely to be volatile, vendor dependent, and less transparent. But heterogeneity may also offer advantages through competitive innovation.

Bridging the value gap between idealized/theoretical designs and actual implementations
For example, the ITU-T defines an IoT device as "a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing" (ITU-T, 2012). But these features all come with economic costs that are either unclear or understudied.

Current lack of interoperability
True interoperability of IoT devices is crucial to maximize value (McKinsey, 2015) and includes the possibility to adopt open standards.

Limited current use cases of IoT data
The trend to broaden IoT data use from anomaly detection and system control to optimization currently takes place mostly in the industry sector only. This process also involves the assessment and innovation of what provides the greatest economic value (McKinsey, 2015).

The technical viewpoint

Most of the values currently associated with IoT are generated by the innovative technical capabilities of rather individual IoT devices and solutions. This represents a limitation in terms of harnessing economic value from IoT, and this section suggests how one may transcend such constraints.

Designing architectures for IoT

Technical specifications and reference architectures for IoT (systems of) systems are far from being completed and standardized. The architectural models are heterogeneous with respect to their degree of openness and closure and the level of decentralization (see, for example, IBM, 2015). In complex systems, there is no good understanding as to what extent standardization is actually possible. A key aspect of IoT is that individual devices and services tend to coexist within Systems of Systems that might have porous boundaries.

However, key concepts such as the pivotal points of interoperability (PPI) – developed in an IoT-Enabled Smart City Framework (NIST, 2017a) – assure that a limited set of consensus standardized interfaces can exist in practice. These interfaces enable composition of cyber-physical systems in the absence of any formal agreement, without constraining innovation (NIST, 2017b, p. 9). Since IoT systems operate in less predictive environments than ICT systems, it is hard for conventional data-driven programming to account for all relevant events or system states.

In terms of creating value, the main gap in this space is the lack of mechanisms that support the creation of innovative and enriched web-of-things contents. It has been suggested that such mechanisms should be integrated into IoT middleware to perform data analysis operations on data streams. "Computational thinking" (Wing, 2006) calls for increased attention to building computing infrastructures that are mindful of the real-world complexities and engage with the existing economic and social aspects (Blanchette, 2012).

This gap could be addressed by processing streams efficiently, by handling different formats and models as well as energy limitations of IoT environments (Mineraud *et al.*, 2016), and by the timely generation of real-time information for IoT applications (Díaz *et al.*, 2016). We may see more "edge analytic solutions" such as "cloudlets" that maximize energy efficiency, reduce privacy threats, and minimize latencies by analysing the data closer to the place where data are produced (Mineraud *et al.*, 2016). Although different cloud platforms have different aims and are divided into several categories, they can be orchestrated in order to create transversal values (Díaz *et al.*, 2016).

The problem of software for IoT

In the mid-1980s, it was realized that it can take 15–20 years for software technologies to evolve from concept formulation to accepted popularization (Redwine and Riddle, 1985). By the 2000s, for example, this evolution was completed for system architectures (Shaw, 2001). In recent years, there has been a shift in R&D from accepting such time scales to time spans of just a few years for software technology to mature and propagate itself. This shift also led to viewing cyber security as a service that one could purchase to make a software system secure. In short, we find that ICT systems essentially consist of a layered ecosystem of technologies and hardware that have many security vulnerabilities whose source or number may be impossible to assess (e.g. Shin *et al.*, 2015; Trippel *et al.*, 2017). Under these circumstances, the state of cyber security can be described as being in a "shameful state of unpreparedness" (Arquilla, 2017, p. 10).

Industries continue to respect the software-as-framework paradigm also because they have to integrate the incumbent technologies and customized software solutions with emerging technologies such as IoT. Solutions to this issue include the need to adjust the way in which increasingly autonomous systems are engineered, for example, by borrowing concepts from civil engineering (Kaplan, 2017, p. 38), risk engineering processes (Huth *et al.*, 2016), privacy-by-design policies (Cavoukian, 2011; D'Acquisti *et al.*, 2015), and from methodologies of value-sensitive design (Friedman *et al.*, 2008).

Such conceptual approaches are echoed by initiatives that advocate the need for software development that is not merely craft-based but rooted in a true engineering discipline (Jacobson *et al.*, 2016). This assumes the codification and sharing of knowledge – so organizations have to tailor their methods in order to be more efficient at code development – freeing the practices and presenting them in ways that would allow engineers to confidently and predictably engage in the practices they need (Jacobson *et al.*, 2016). Such developments would increase the involvement of categories other than software developers and data scientists in creating value in the IoT space.

The design of IoT

The state of the art in IoT could be characterized by the challenges to understand the cyber-physical nature of IoT devices, the scalability and interoperability issues, and the interaction with the social world. Attempting to emulate and coherently interact with the physical environment through IoT devices and processes is challenging, not least because logical systems have to understand and manage the unpredictability of physical and social life. Most IoT solutions need to be developed in cooperation with end users. There are an increasing number of examples that use human-centred design principles to build advanced ICT and IoT applications (e.g. Hilbert, 2016; Hilbert *et al.*, 2016). The privacy-by-design framework, for example, focuses on entrusting privacy assurance as a default mode of operation and on building systems in a client-centric way in order to maximize user control and minimize network and service provider involvement (Cavoukian, 2011; Spiekermann, 2012; D'Acquisto *et al.*, 2015). However, the lack of explicit informed consent mechanism in end-user agreements between IoT providers and users represents an ongoing problem (e.g. Perera *et al.*, 2015). Both the private and public sector have an ethical responsibility here, and GDPR is likely to provide regulatory muscle to see adoption of privacy by design in future IoT technology.

Security and privacy

Data analytics is increasingly pushed towards the edges of IoT systems. One key advantage is that many quantities of interest, such as statistical measures, can therefore be computed without requiring centralized access to personal data sets. This can therefore avoid the need for privacy protection mechanisms and compliance measures. At the same time, it is now widely recognized that security and privacy are people-centric rather than technology-centric notions. The recent European Courts of Justice ruling on the Safe Harbor Agreement (2015), the new data privacy laws passed by the European Parliament (2016), and the EU-US Privacy Shield framework (2016) reinforce this principle. Further work should be done in aligning this legislation with legislation that regulates IoT ecosystems.

In this context, distributed-ledger technology may offer opportunities for more reliable and resilient data storage, with interfaces that are user-centric and that give users both a sense of control and genuine control over their data (LRF and ATI, 2017). We expect that mature instances of such user-centric data management approaches will appear in the public sector, notably local governments, and in IoT-relevant verticals such as intelligent transportation systems. These developments would enhance the more technical values currently associated with IoT, with important social and economic features that are more relevant for end users.

Main findings pertaining to the technical viewpoint

The following challenges and gaps have been identified:

Better understanding of the cyber-physical nature of systems

This aspect relates to the qualities and dynamics of IoT end devices such as sensors and readers designed to constantly work in, interact with, and gather information from a physical environment. The IoT industry is currently focusing more on the technical capabilities, disjointed from the economic and social or physical ones, and their interaction.

Multidisciplinary expertise for IoT system design

Cyber-physical systems require solutions that are not IT-only, but rather a combination of technologies spanning multiple disciplines and domains of expertise. For example, a carrier wave analysis solution (from physics) can address spoofing of GPS signals, when use of encryption in a public system such as GPS location-based services is problematic (Psiaki *et al.*, 2013, 2014). IoT is ideally placed to bridge, verify, and advance empirical and theoretical research.

Socialization of machines

Machines communicate (e.g. status updates and needs) and create things in cooperation to each other. Socialization of machines runs across the micro-sphere and the macro-sphere of the IoT ecosystem. Its realization is severely limited by current technical (e.g. security and safety), economic (e.g. creation/protection of economic value), and social (e.g. trust) aspects.

Fostering strong competition and standardized interoperability and open collaboration
Delays in IoT standardization and implementation constitute gaps in relation to industry and consumer expectations, but they also represent innovation opportunities. These elements can also be seen as opportunities to allow for the organic development and adoption of IoT in different social contexts.

Balance of innovation with efficient use of incumbent technologies
Industries have realized that the challenges to produce successful IoT products and services consist in the ability to integrate digital products into their respective industries (RAE, 2015, pp. 13–31). The Industry 4.0 sectors depend on their capacity to bring together the dynamism in the IT industry with the particular dynamics in various engineering domains, which have longer R&D and production cycles and different requirements (e.g. Jansen, 2016).

New risk assessment approaches
IoT ecosystems need to include new approaches in relation to structural changes in production and consumption practices. These changes include, for example, rethinking of engineering processes, risk engineering assessment throughout the entire lifecycle of the product, reorganization of labour within organizations, and major transformations in the education system and in the professional landscape.

Information models and Semantics
Current data models are insufficient. Semantics-based information models should be an integral part of security, risk management, and the design of IoT products and business applications in order to increase the safety and predictability of systems – especially in case of attacks or failures. There is a disturbing lack of data and information management in many IoT architectures, the focus being on the technology and its interconnection rather than system integrity.

Conclusion

The entire spectrum of values associated with IoT technology is yet to be rigorously assessed. This article mapped the current trends in assessing value for IoT along three main domains: social, economic, and technical. We showed why value related to IoT could not be reduced to any one of these three domains, although such reductions are currently often practiced. Rather, the meaning of “value” in IoT is continually articulated by the juxtaposition of these domains. For each domain, we detailed how this articulation can take place and then summed up the main findings, gaps and cross-domain implications. We offered a functional model that aggregates and places these findings into the overall logic of the emerging global political economy.

We also discussed when, and how, social and cultural customs can norm and limit the economic and technical capabilities enabled by IoT and digital technology. This implies that future research on value enabled by IoT should necessarily be interdisciplinary. However, we also noted that the IoT space currently tends towards hyper-fragmentation and exclusiveness, rather than towards homogenization and collaboration. We suggested that one of the root causes of this situation is the rather partial and therefore limited understanding and use of the notion of “value” in IoT ecosystems. This article provided evidence as to why, and how, considering the meaning of “value” across disciplines and throughout the entire lifecycle of IoT devices and services – from design to consumption and retirement or recycling – can address this gap. We offered pathways to explore these implications further.

Limitations of the study

This research is dealing with an innovative, dynamic, and often volatile topic. The very meaning of “value” can vary enormously from product to product, from usage to usage, and from community to community. The present study does not attempt to present an exhaustive account of the meaning of “value” in relation to IoT. Rather, it points to, and explores, the main dimensions along which the term “value” can vary: the social, economic, and technical ones. For each of these, the meaning of “value” can vary across populations, individuals, communities, and institutions. Our study indicates how these variations tend to operate, why it is important to consider the transversal implications in relation to IoT technology, and how this can be done. At the same time, our study does not discuss other perspectives on the meaning of “value” in relation to IoT offered by specific disciplines, such as psychology, human–computer interaction, user experience, or development and environment studies. However, the study is informed by the sustained engagement of the UK EPSRC IoT Research Hub “PETRAS” (https://www.petrashub.org) with a broad set of user partners for a wide range of private sectors, government agencies, and charities at international scale.

Acknowledgements

This work was supported by the UK EPSRC with projects [Grant Numbers EP/N020030/1 and EP/N023242/1].

References

Acquisti, A., John, L.K. and Loewenstein, G. (2013). What is Privacy Worth? *Journal of Legal Studies* **42**(2): 249–274.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials* **17**(4): 2347–2376.

Anderson, S., Miorandi, D., Carreras, I. and Robertson, D. (2014). Twelve Big Questions for Research on Social Collective Intelligence. In D. Miorandi, V. Maltese, M. Rovatsos, A. Nijholt, & J. Stewart (Eds.), *Social Collective Intelligence. Combining the Powers of Humans and Machines to Build a Smarter Society* (p. 93). Cham, Heidelberg, New York, Dordrecht, London: Springer.

Arquilla, J. (2017). The Real Lesson of the Alleged Russian Hack. *Communications of the ACM* **60**(4): 10–11.

Balaji, M.S. and Roy, S.K. (2016). Value Co-creation with Internet of Things Technology in the Retail Industry. *Journal of Marketing Management* **33**(1–2): 7–31. https://doi.org/10.1080/0267257X.2016.1217914.

Benkler, Y. (2003). Freedom in the Commons: Towards a Political Economy of Information. *Duke Law Journal* **52**(6): 1245–1276.

Blanchette, J.F. (2012). Computing as if Infrastructure Mattered. *Communications of the ACM* **55**(10): 32–34.

Bloom, N. and Van Reenen, J. (2007). Measuring and Explaining Management Practices Across Firms and Countries. *Quarterly Journal of Economics* **122**(4): 1351–1408. https://doi.org/10.1162/qjec.2007.122.4.1351.

Breidbach, C.F. and Maglio, P.P. (2016). Technology-Enabled Value Co-creation: An Empirical Analysis of Actors, Resources, and Practices. *Industrial Marketing Management* **56,** 73–85. https://doi.org/10.1016/j.indmarman.2016.03.011.

Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M. and Khalil, M. (2007). Lessons from Applying the Systematic Literature Review Process within the Software Engineering Domain. *Journal of Systems and Software* **80**(4): 571–583. https://doi.org/10.1016/j.jss.2006.07.009.

Brynjolfsson, E., Hitt, L.M. and Kim, H.H. (2011). *Strength in Numbers: How Does Data-Driven Decision Making Affect Firm Performance?* http://dx.doi.org/10.2139/ssrn.1819486. Accessed 11 Oct 2017.

Brynjolfsson, E. and McAfee, A. (2011). *Race Against the Machine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy*. Lexington (MA): Digital Frontier Press.

Burgess, M. (2016). Chinese IoT Firm Recalls 4.3 million Connected Cameras After Giant Botnet Attack. *Wired* 25 October 2016. http://www.wired.co.uk/article/internet-down-dyn-october-2016. Accessed 10 July 2017.

Carrier, J.G. and Miller, D. (Eds.). (1998). *Virtualism: A New Political Economy*. Oxford: Berg.

Cavalcante, E., Pereira, J., Alves, M.P., Maia, P., Moura, R., Batista, T., et al. (2016). On the Interplay of Internet of Things and Cloud Computing: A systematic Mapping Study. *Computer Communications* **8990,** 17–33.

Cavoukian, A. (2011). *Privacy by Design Curriculum 2.0*. Available at: http://privacybydesign.ca/publications. Accessed 10 Aug 2016.

Chakravartty, P. and Zhao, Y. (Eds.). (2008). *Global Communication: Toward a Transcultural Political Economy*. Lanham (MD): Rowman and Littlefield.

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H. and McAuley, D. (2015). *Personal Data: Thinking Inside the Box, in Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives, Aarhus, Denmark, August 17–21, 2015*, pp: 29–32. https://doi.org/10.7146/aahcc.v1i1.21312.

Constantinou, A. (2015). *The Business Model Mechanics of Internet Disruptors*. VisionMobile. https://www.slideshare.net/digitalwinners/dw-2015-andreas-constantinou-the-business-model-mechanics-of-internet-disruptors. Accessed 06 July 2017.

Crandall, R., Lehr, W. and Litan, R. (2007). The Effects of Broadband Deployment on Output and Employment: A Cross-sectional Analysis of U.S. Data, *Issues in Economic Policy* **6**: 1–35. https://www.brookings.edu/wp-content/uploads/2016/06/06labor_crandall.pdf. Accessed 06 July 2017.

Crawford, K, Miltner, K. and Gray, M.L. (2014). Critiquing Big Data: Politics, Ethics, Epistemology, *International Journal of Communication* **8**: 1663–1672. http://ijoc.org/index.php/ijoc/article/viewFile/2167/1164. Accessed 09 Aug 2016.

Czernich, N., Falck, O., Kretschmer, T. and Woessmann, L. (2011). Broadband Infrastructure and Economic Growth. *The Economic Journal* **121**(552): 505–532. https://doi.org/10.1111/j.1468-0297.2011.02420.x.

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., De Montjoye, Y.-A. and Bourka, A. (2015). *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, European Union Agency for Network and Information Security (ENISA) Report, December 2015. https://www.enisa.europa.eu/publications/big-data-protection. Accessed 03 July 2017.

DARPA [Defense Advanced Research Projects Agency]. (2016). *Explainable Artificial Intelligence (XAI)*, Broad Agency Announcement. DARPA-BAA-16-53. Available at: https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf. Retrieved 17 Jan 2018.

David, M. (2005). *Science in Society*. New York: Palgrave Macmillan.

DCMS [Department for Culture Media and Sport]. (2016). *Digital Skills for the UK Economy*. A Report by Ecorys UK. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492889/DCMSDigitalSkillsReportJan2016.pdf. Accessed 12 Aug 2016.

De Bruin, B. and Floridi, L. (2016). The Ethics of Cloud Computing. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-016-9759-0.

De Montjoye, Y.-A.., Radaelli, L., Singh, V.K. and Pentland, A.S. (2015). Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. *Research* **347**(6221): 536–539. https://doi.org/10.1126/science.1256297.

Deshpande, A. (2013). Broadband Deployment and the Bandwagon Effect in the UK. *info* **15**(1): 34–47. https://doi.org/10.1108/14636691311296192.

Díaz, M., Martín, C. and Rubio, B. (2016). State-of-the-Art, Challenges, and Open Issues in the Integration of Internet of Things and Cloud Computing. *Journal of Network and Computer Applications* **67,** 99–117.

DiMase, D., Collier, Z.A., Heffner, K. and Linkov, I. (2015). Systems Engineering Framework for Cyber Physical Security and Resilience. *Environment Systems and Decisions* **35**(2): 291–300. https://doi.org/10.1007/s10669-015-9540-y.

Dourish, P. (2003). The Appropriation of Interactive Technologies: Some Lessons from Placeless Documents. *Computer Supported Cooperative Work (CSCW)* **12,** 465–490. https://doi.org/10.1023/A:1026149119426.

Frey, C.B. and Osborne, M.A. (2017). The Future of Employment: How Susceptible are Jobs to Computerisation. *Technological Forecasting and Social Change* **114**(C): 254–280. https://doi.org/10.1016/j.techfore.2016.08.019.

Friedman, B., Kahn, P.H., Jr. and Borning, A. (2008). Value Sensitive Design and Information Systems. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (p. 69). Hoboken (NJ): Wiley.

Friedman, B. and Nissenbaum, H. (1996). Bias in Computer Systems. *ACM Transactions on Information Systems* **14**(3): 330–347.

Fuller, M. (2008). Introduction, the Stuff of Software. In M. Fuller (Ed.), *Software Studies. A Lexicon* (pp. 1–13). Cambridge (MA); London (England): MIT Press.

Gartner. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Press Release, February 7, 2017*. http://www.gartner.com/newsroom/id/3598917. Accessed 10 July 2017.

GDPR [General Data Protection Regulation]. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 10 July 2017.

Gillett, S.E., Lehr, W.H., Osório, CA. and Sirbu, M.A. (2006). *Measuring the Economic Impact of Broadband Deployment*, Final Report, National Technical Assistance, Training, Research, and Evaluation Project No. 99-07-13829. http://cfp.mit.edu/publications/CFP_Papers/Measuring_bb_econ_impact-final.pdf. Accessed 06 July 2017.

Glass, R.L., Ramesh, V. and Vessey, I. (2004). An Analysis of Research in Computing Disciplines. *Communications of the ACM* **47**(6): 89–94. https://doi.org/10.1145/990680.990686.

Goos, M. and Manning, A. (2007). Lousy and Lovely Jobs: The Rising Polarization of Work in Britain. *The Review of Economics and Statistics* **89**(1): 118–133. http://www.mitpressjournals.org/doi/pdfplus/10.1162/rest.89.1.118. Accessed 10 Jan 2017.

Gordon, R.J. (2016). *The Rise and Fall of American Growth: The U.S. Standard of Living since the Civil War*. Princeton, New Jersey: Princeton University Press.

GOS [The Government Office for Science]. (2014). *The Internet of Things: Making the Most of the Second Digital Revolution*, A report by the UK Government Chief Scientific Adviser. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf. Accessed 10 Nov 2016.

Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology* **91,** 481–510.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems* **29**(7): 1645–1660. https://doi.org/10.1016/j.future.2013.01.010.

Haldane, A. (2015). *Labour's Share*. Talk given at the Trades Union Congress, London, 12 November 2015. http://www.bankofengland.co.uk/publications/Pages/speeches/2015/864.aspx. Accessed 06 Feb 2017.

He, H., Xu, K. and Liu, Y. (2012). Internet Resource Pricing Models, Mechanisms, and Methods. *Networking Science* **1,** 48–66. https://doi.org/10.1007/s13119-011-0004-5.

Heinonen, K., Strandvik, T., Mickelsson, K-J., Edvardsson, B., Sundström, B. and Andersson, P. (2010). A Customer-Dominant Logic of Service. *Journal of Service Management* **21**(4): 531–548. https://doi.org/10.1108/09564231011066088.

Hilbert, M. (2016). Big Data for Development: A Review of Promises and Challenges. *Development Policy Review* **34**(1): 135–174.

Hilbert, M., Cheng, S. and Wang, S. (2016). *Digital Tools for Foresight and Foresight of a Digital Future: Fostering Means for and Ends of the SDGs*. Report prepared on behalf of the United Nations Commission on Science and Technology for Development of the United Nations Economic and Social Council, under the auspices of the United Nations Conference on Trade and Development. 15 November 2016.

Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S. and Boyle, D. (2014). *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Oxford: Academic Press.

Hollingsworth, J.R. and Boyer, R. (Eds.). (1997). *Contemporary Capitalism: The Embeddedness of Institutions*. Cambridge; New York: Cambridge University Press.

Hollingsworth, J.R., Müller, K. and Hollingsworth, E.J. (Eds.). (2002). *Advancing Socio-Economics: An Institutionalist Perspective*. Lanham, MD: Rowman and Littlefield.

Huth, M., Vishik, C. and Masucci, R. (2016). From Risk Management to Risk Engineering: Challenges in Future ICT Systems. In E. Griffor (Ed.), *Handbook of System Safety and Security* (pp. 131–174). Cambridge (MA): Elsevier.

IBM. (2015). *Device Democracy. Saving the Future of the Internet of Things*. Executive Report.

ITU-T [International Telecommunication Union – Telecommunication]. (2012). *Overview of the Internet of Things*. Recommendation Y.2060.

Jacobson, I., Spence, I. and Seidewitz, E. (2016). Industrial-Scale Agile from Craft to Engineering. 1–31. *ACM Queue*. Available at https://www.ivarjacobson.com/sites/default/files/field_iji_file/article/industrial_scale_agile_acm.pdf. Accessed 8 Feb 2018.

Jansen, J. (2016). Der Maschinenbau digitalisiert fremd. *Frankfurter Allgemeigne Zeitung*, 4 November 2016. http://www.faz.net/aktuell/wirtschaft/internet-in-der-industrie/technischer-fortschritt-der-maschinenbau-digitalisiert-fremd-14512595.html. Accessed 10 Nov 2016.

Jevons, W.S. (1871). *Theory of Political Economy*. London: Macmillan.

Kaplan, J. (2017). Artificial Intelligence: Think Again. *Communications of the ACM* **60**(1): 36–38.

Keynes, J.M. (1931). Economic Possibilities for Our Grandchildren, in J.M. Keynes (ed.) *Essays in Persuasion*, London: Macmillan, pp. 358–373. https://gutenberg.ca/ebooks/keynes-essaysinpersuasion/keynes-essaysinpersuasion-00-h.html#Economic_Possibilities. Accessed 28 Apr 2017.

Koch, R. and Rodosek, G. (eds). (2016). *Proceedings of the 15th European Conference on Cyber Warfare and Security*. ECCWS 2016: hosted by Universität der Bundeswehr, Munich, Germany, 7–8 July 2016. Available at: https://books.google.co.uk/books?hl=en&lr=&id=ijaeDAAAQBAJ&oi=fnd&pg=PA145&dq=economic+impact+of+cyber+risk&ots=50mTo8TVSV&sig=sD4V76yG5tG6IZIglmnGz3L1qqw&redir_esc=y#v=onepage&q&f=false. Accessed 5 Feb 2018.

Kraemer, F., Van Overveld, K. and Peterson, M. (2011). Is There an Ethics of Algorithms? *Ethics and Information Technology* **13**(3): 251–260. https://doi.org/10.1007/s10676-010-9233-7.

Krämer, J. and Wiewiorra, L. (2012). Network Neutrality and Congestion Sensitive Content Providers: Implications for Content Variety, Broadband Investment, and Regulation. *Information Systems Research* **23**(4): 1303–1321. https://doi.org/10.1287/isre.1120.0420.

Latour, B. (1987). *Science in Action. How to Follow Scientists and Engineers through Society*. Cambridge (MA): Harvard University Press.

Litan, R.E. and Rivlin, A.M. (2001). Projecting the Economic Impact of the Internet. *American Economic Review* **91**(2): 313–317. https://doi.org/10.1257/aer.91.2.313.

LRF and ATI [Lloyd's Register Foundation and The Alan Turing Institute]. (2017). *Insight Report on Distributed Ledger Technologies. Safety of Engineered Systems*. Report Series: No. 2017.4. London: Lloyd's Register Foundation.

Luong, N.C., Hoang, D.T., Wang, P., Niyato, D., Kim, D.I. and Han, Z. (2016). Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey. *IEEE Communications Surveys and Tutorials* **18**(4): 2546–2590.

Marx, K. (1906 [1867]). *Capital: A Critique of Political Economy, Vol. I. The Process of Capitalist Production*. 4th edn. Chicago: Charles H. Kerr and Co. http://www.econlib.org/library/YPDBooks/Marx/mrxCpA.html. Accessed 10 July 2017.

Mathur, P., Nielsen, R.H., Prasad, N.R. and Prasad, R. (2015). Cost Benefit Analysis of Utilising Mobile Nodes in Wireless Sensor Networks. *Wireless Personal Communications* **83**(3): 2333–2346.

Mayer-Schönberger, V. and Cukier, K. (2013). *Big Data: A Revolution that will Transform how We Live, Work and Think*. London: Murray.

McKinsey [McKinsey Global Institute]. (2011). *Big Data: The Next Frontier for Innovation, Competition, and Productivity*. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation. Accessed 10 July 2017.

McKinsey [McKinsey Global Institute]. (2015). *The Internet of Things: Mapping the Value beyond the Hype*, McKinsey & Company. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Accessed 10 July 2017.

Menger, C. (1871). *Principles of Economics [Grundsätze der Volkswirtschaftslehre]* (p. 1981). New York: New York University Press.

Miller, D. (2008). The Uses of Value. *Geoforum* **39,** 1122–1132.

Miller, D., Costa, E., Haynes, N., McDonald, T., Nicolescu, R., Sinanan, J., et al. (2016). *How the World Changed Social Media*. London: UCL Press. https://doi.org/10.14324/111.9781910634493.

Mineraud, J., Mazhelis, O., Su, X. and Tarkoma, S. (2016). A Gap Analysis of Internet-of-Things Platforms. *Computer Communications* **89**(C): 5–16.

Miorandi, D., Maltese, V., Rovatsos, M., Nijholt, A. and Stewart, J. (Eds.). (2014). *Social Collective Intelligence. Combining the Powers of Humans and Machines to Build a Smarter Society*. Cham, Heidelberg, New York, Dordrecht, London: Springer.

Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data and Society* **3**(2): 1–21.

Montague, J. (2017). Breaking the interoperability barrier: ExxonMobil, Lockheed Martin and friends lead charge to open, secure, interoperable process control system. *Control*, 21 March 2017. http://www.controlglobal.com/articles/2017/breaking-the-interoperability-barrier/. Accessed 10 July 2017.

Mosco, P. (2008). Current Trends in the Political Economy of Communication. *Global Media Journal – Canadian Edition* **1**(1): 45–63.

Nakamura, L. (2002). *Cybertypes: Race, Ethnicity, and Identity on the Internet*. New York; London: Routledge.

Ng, I.C.L., Holtby, J., Ma, X., Aucinas. A. and Tasker, P. (2017). *White Paper on Digital Dependency: The need for a Personal Data Exchange infrastructure*, HAT Data Exchange Ltd. http://www.hatdex.org/digital-dependency/. Accessed 10 July 2017.

NIST [National Institute of Standards and Technology]. (2016). *Framework for Cyber-Physical Systems. Release 1.0*. https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf. Accessed 22 June 2017.

NIST [National Institute of Standards and Technology]. (2017a). *International Technical Working Group on IoT-Enabled Smart City Framework*. https://pages.nist.gov/smartcitiesarchitecture/. Accessed 13 July 2017.

NIST [National Institute of Standards and Technology]. (2017b). *Global City Teams Challenge 2016*, NIST Special Publication 1900-01. https://doi.org/10.6028/NIST.SP.1900-01.

Pang, Z., Chen, Q., Han, W. and Zheng, L. (2015). Value-Centric Design of the Internet-of-Things Solution for Food Supply Chain: Value Creation, Sensor Portfolio and Information Fusion. *Information Systems Frontiers* **17**(2): 289–319. https://doi.org/10.1007/s10796-012-9374-9.

Perera, C., Ranjan, R., Wang, L., Khan, S.U. and Zomaya, A.Z. (2015). Big Data Privacy in the Internet of Things Era. *IT Professional* **17**(3): 32–39. https://doi.org/10.1109/MITP.2015.34.

Polanyi, K. (2001 [1944]). *The Great Transformation: The Political and Economic Origins of Our Times*, Boston, MA: Beacon Press.

Powell, W.W. and DiMaggio, P.J. (Eds.). (1991). *The New Institutionalism in Organizational Analysis*. Chicago: University of Chicago Press.

Psiaki, M.L., O'Hanlon, B.W., Powell, S.P., Bhatti, J.A., Wesson, K.D., Humphreys, T.E. and Schofield, A. (2014). GNSS Spoofing Detection Using Two-Antenna Differential Carrier Phase, in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS + 2014), Tampa (FL), September 2014*, pp. 2776–2800.

Psiaki, M.L., Powell, S.P. and O'Hanlon, B.W. (2013). GNSS Spoofing Detection Using High- Frequency Antenna Motion and Carrier-Phase Data, in *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS + 2013), Nashville (TN), September 2013*, pp. 2949–2991.

Purdy, M. and Daugherty, P. (2016). *Why Artificial Intelligence is the Future of Growth*, Accenture Institute for High Performance.

Radner, R. (1968). Competitive Equilibrium under Uncertainty. *Econometrica* **36,** 31–58.

RAE [Royal Academy of Engineering]. (2015). *Connecting Data: Driving Productivity and Innovation*.

Rainie, L. and Wellman, B. (2012). *Networked. The New Social Operating System*. Cambridge, MA: The MIT Press.

Redwine, S. and Riddle, W. (1985). Software Technology Maturation, in *Proceedings of the 8th International Conference on Software Engineering, May 1985*, pp. 189–200.

Ribeiro, M.T., Singh, S. and Guestrin, C. (2016). *"Why Should I Trust You?" Explaining the Predictions of Any Classifier*. arXiv:1602.04938

Ricardo, D. (1821 [1817]). *On The Principles of Political Economy and Taxation*. 3rd edn. London: John Murray. http://www.econlib.org/library/Ricardo/ricP.html. Accessed 10 July 2017.

Rifkin, J. (2014). *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*. New York: Palgrave Macmillan.

Roscoe, T. (2006). The End of Internet Architecture. *Proceedings of the 5th Workshop on Hot Topics in Networks*. Available at: http://conferences.sigcomm.org/hotnets/2006/roscoe06end.pdf. Accessed 8 Feb 2018.

Scott, B. (2016). *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?* Working Paper 2016-1 for the United Nations Research Institute for Social Development, February 2016. http://www.unrisd.org/brett-scott. Accessed 28 June 2017.

Shapiro, C. and Varian, H.R. (1999). *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.

Shaw, M. (2001). The Coming-Of-Age of Software Architecture Research, in *Proceedings of the 23rd International Conference on Software Engineering*, IEEE Computer Society, 2001, pp. 656–664a.

Shin, J., Son, H., Khalil ur, R. and Heo, G. (2015). Development of a Cyber Security Risk Model using Bayesian Networks. *Reliability Engineering and System Safety* **134,** 208–217. https://doi.org/10.1016/j.ress.2014.10.006.

Silverstone, R. and Hirsch, E. (Eds.). (1992). *Consuming Technologies: Media and Information in Domestic Spaces*. London; New York (NY): Routledge.

Simon, H.A. (1957). *Models of Man: Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*. New York; London: John Wiley.

Smith, A. (1904 [1776]). *An Enquiry into the Nature and Causes of the Wealth of Nations*. 5th edn. London; Edinburgh: Methuen & Co., Ltd. http://www.econlib.org/library/Smith/smWN.html. Accessed 10 July 2017.

Spiekermann, S. (2012). The Challenges of Privacy by Design. *ACM Journal on Computing and Cultural Heritage* **55**(7): 38–40.

Stankovic, J.A. (2014). Research Directions for the Internet of Things. *IEEE Internet of Things Journal* **1**(1): 3–9. https://doi.org/10.1109/JIOT.2014.2312291.

Stock, T. and Seliger, G. (2016). Opportunities of Sustainable Manufacturing in Industry 4.0. *Procedia CIRP*, **40**: 536–541. http://linkinghub.elsevier.com/retrieve/pii/S221282711600144X. Accessed 18 Apr 2017.

Tambe, P. (2014). Big Data Investment, Skills, and Firm Value. *Management Science* **60**(6): 1452–1469. https://doi.org/10.1287/mnsc.2014.1899.

Thierer, A. (2015). The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. *Richmond Journal of Law and Technology* **21**(2): 1–118. http://jolt.richmond.edu/v21i2/article6.pdf. Accessed 28 June 2017.

Tiwana, A., Konsynski, B. and Bush, A.A. (2010). Platform Evolution: Coevolution of Platform Architecture. *Governance, and Environmental Dynamics, Information Systems Research* **21**(4): 675–687.

Trippel, T., Weisse, O., Xu, W., Honeyman, P. and Fu, K. 2017. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks, in *Proceedings of the 2nd IEEE European Symposium on Security and Privacy, Paris, April 2017*, pp: 3–18.

Turilli, M. and Floridi, L. (2009). The Ethics of Information Transparency. *Ethics and Information Technology* **11**(2): 105–112. https://doi.org/10.1007/s10676-009-9187-9.

Van Dijk, J. (2005). *The Deepening Divide: Inequality in the Information Society*. Thousand Oaks; (CA) London: Sage.

Vargo, S.L. and Lusch, R.F. (2016). Institutions and Axioms: An Extension and Update of Service-Dominant Logic. *Journal of the Academy of Marketing Science* **44**(1): 5–23.

Vargo, S.L., Maglio, P.P. and Akaka, M.A. (2008). On Value and Value Co-creation: A Service Systems and Service Logic Perspective. *European Management Journal* **26**(3): 145–152. https://doi.org/10.1016/j.emj.2008.04.003.

Walras, L. (1874). *Elements of Pure Economics* [*Élements d'Économie Politique Pure, ou, Theorie de la richesse sociale*], Homewood (IL): Irwin, 1954.

Wang, Y., Huang, M., Zhao, L. and Zhu, X. (2016). Attention-based LSTM for Aspect-level Sentiment Classification, in *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing*, pages 606–615, Austin, Texas, November 1–5, 2016. Available at: https://aclweb.org/anthology/D16-1058. Accessed 17 Jan 2017.

WEF [World Economic Forum]. (2016). *The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution*.

Weinman, J. (2012). *Cloudonomics: The Business Value of Cloud Computing*. Hoboken (NJ): Wiley.

Weyl, E.G. (2010). A Price Theory of Multi-sided Platforms. *American Economic Review* **100**(4): 1642–1672.

Williams, R., Stewart, J. and Slack, R. (2005). *Social Learning in Technological Innovation: Experimenting with Information and Communication Technologies*. Northampton (MA): Elgar.

Williamson, O.E. (1975). *Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization*. London; New York: Free Press; Collier Macmillan.

Williamson, O.E. (1981). The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology* **87**(3): 548–577.

Wing, J.M. (2006). Computational thinking. *Communications of the ACM* **49**(3): 33–35.

Wu, T. (2003). Network Neutrality, Broadband Discrimination. *Journal on Telecommunications and High Technology Law* **2**(1): 141–176. http://www.jthtl.org/content/articles/V2I1/JTHTLv2i1_Wu.PDF. Accessed 06 June 2017.

Zelizer, V. (1987). *Pricing the Priceless Child: The Changing Social Value of Children*. New York: Basic Books.

Zelizer, V. (1997). *The Social Meaning of Money*. Princeton (NJ): Princeton University Press.

About the Authors

Razvan Nicolescu is a digital anthropologist working at the Department of Computing, Imperial College London. He obtained his BSc and MSc in networks and software for telecommunications (University Polytechnics, Bucharest) and his Ph.D. in social anthropology at University College London. His current research focuses on notions of trust and risk in relation to blockchain technology and cyber insurance using IoT.

Michael Huth is Professor and co-lead of the FinTech network at Imperial College London. He is a Diplom-Mathematiker (TU Darmstadt, Germany), obtained his Ph.D. at Tulane University of Louisiana, and was an Assistant Professor at Kansas State University. His present research focuses on cyber security, especially modelling and reasoning about the interplay of trust, security, risk, and economics.

Petar Radanliev is a Post-Doctoral Research Associate at University of Oxford. He completed his Ph.D. in systems engineering at University of South Wales, MSc in Economics and Finance and BA in IT Communications at Aberystwyth University. His current research is focused on harnessing economic value from the IoT and the economic impact of IoT cyber risk.

David De Roure is a Professor of e-Research at University of Oxford. He obtained his Ph.D. at University of Southampton in 1990 and went on to hold the post of Professor of Computer Science, later directing the UK Digital Social Research programme. His current research focuses on social machines, Internet of Things, and cyber security. He is a Fellow of the British Computer Society and the Institute of Mathematics and its Applications.