Received: 31 May 2019 | Revised: 6 December 2019 | Accepted: 23 December 2019

DOI: 10.1111/soc4.12770

ARTICLE

WILEY

The Internet of Things: Social dimensions

Deborah Lupton

Vitalities Lab, Centre for Social Research in Health and Social Policy Research Centre, UNSW Sydney

Correspondence
Deborah Lupton, Vitalities Lab, Centre for Social Research in Health and Social Policy Research Centre, UNSW Sydney, Goodsell Building, Sydney, NSW 2052, Australia.
Email: d.lupton@unsw.edu.au

Abstract

The Internet of Things (IoT) is a vast, dispersed system in which a diverse array of objects, humans, and other living things is connected via "smart" technologies and the Internet. In this article, I present a thematic review of the literature that focuses on the social dimensions of the IoT. Drawing on research published in sociology, anthropology, cultural geography, critical urban studies, science and technology studies, environmental studies, and human–computer interaction studies and design, I outline key conceptual approaches and then discuss four major themes emerging across these dispersed but cognate literatures: (a) techno-utopian imaginaries, (b) risks and harms, (c) lived experiences, and (d) interventions into futures. As I show, to date, most of the social research literature has focused on the topics of smart cities and smart homes in the context of the Global North. Some researchers have begun to employ innovative methods to generate new and alternative ways of imagining IoT technologies. The article concludes with proposing directions for future research. These include directing more attention to publics' role in intervening in the futures of IoT, to applications of smart technologies beyond the smart city and home, and the IoT in the context of the Global South.

1 | INTRODUCTION

The Internet of Things (IoT) is a term that has been adopted to describe a range of new and emerging digital technologies. There are multiple definitions, but for the purposes of this review, I adopt the following widely used definition from the Organisation for Economic Co-operation and Development (OECD, 2016, p. 4): "The IoT refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the

physical world." The IoT has been made possible by technological developments such as smaller and cheaper sensors, reliable ubiquitous wireless connections, mobile devices, improved software for managing large datasets, and an ecosystem for the generation, processing, and storing of data, in conjunction with the emergence of the digital data economy (Maras & Wandt, 2019; Weber & Wong, 2017).

The number of IoT devices is rapidly expanding. The industry analytics company Gartner estimated that in 2017, there were 8.4 billion Internet-connected things in use, an increase of 31% from 2016, with the consumer market the largest user segment (Gartner, 2017). These objects include mobile devices such as smartphones, tablet computers, and wearable devices like fitness trackers and smartwatches, as well as industrial machinery and transport systems. Medical devices can be part of the IoT: continuous blood glucose monitors and digital blood pressure monitors, for example. Some domestic animals and wildlife have been fitted with digital sensors to track their movements. A range of everyday objects that have been equipped with digital sensing and monitoring capabilities are also considered part of the IoT, including children's toys, televisions, digital home voice assistants such as Amazon's Alexa and Google Home, fridges, kettles, toasters, home security, lighting and heating systems, water bottles, toothbrushes, sex toys, and a multitude of other "smart" things.

Social research can offer a nuanced, contextual, and detailed perspective on IoT technologies, including identification of the ways they are promoted and how they are engaged with by users across a range of social groups and spatial locations. In a widely dispersed literature, including contributions from sociology, anthropology, cultural geography, critical urban studies, science and technology studies, environmental studies, and human–computer interaction studies and design, researchers have begun to identify the dominant social imaginaries giving meaning to IoT technologies, aspects of the social, political, spatial and cultural contexts and implications of deployments of the IoT, and the details of people's lived experiences with these technologies. These bodies of research do not often refer to each other, yet they offer highly complementary insights.

In this article, I present a thematic review of these diverse and scattered bodies of social research. In so doing, I aim to identify the important insights that these different fields of social research offer into the social dimensions of the IoT for sociologists and others interested in the social dimensions of these novel and highly promoted (and often over hyped) technologies.

The studies referred to in this review were found through a Google Scholar search combining the search terms "Internet of Things" and the various "smart" terms listed above (e.g., "smart home") with words and phrases such as "social," "cultural," and "political." Google Scholar was used for this purpose because it is far better at identifying publications in the humanities and social sciences than are other reference databases, which are oriented towards the sciences, such as Scopus and Web of Science (Martín-Martín, Orduna-Malea, Thelwall, & Delgado López-Cózar, 2018). Google Scholar is also more inclusive of outputs such as books and book chapters, which are key publications in these disciplinary areas, and has therefore been described as "a superset" of Scopus and Web of Science, "with substantial extra coverage" (Martín-Martín et al., 2018, p. 1160). The citation trails of references surfaced by these initial searches were followed, resulting in the discovery of many more relevant publications that were subsequently reviewed for this article.

A review of the relevant research identified in this way identified four major themes emerging across these dispersed literatures: (a) techno-utopian imaginaries, (b) risks and harms, (c) lived experiences, and (d) interventions into futures. Following a brief conceptual overview, these themes are discussed in detail. The concluding comments outline gaps in the existing literature and directions for future research.

2 | CONCEPTUAL OVERVIEW

Most of social research literature takes a sociomaterial perspective on the entanglements of humans, other living creatures, discourses, ideas, place and space with IoT technologies, and the digital data they generate, acknowledging the discursive and more-than-human dimensions of these assemblages. By adopting a human-centric approach that

also acknowledges the role of non-humans, this perspective offers a very different approach from the often techno-determinist perspective taken by the larger IoT literature across the sciences and legal disciplines.

For many social researchers, the language used in policy and promotional documents and popular culture warrants attention, as it plays a key role in shaping understandings and practices. The role of humans in creating and interacting with the devices, software, and data generated by IoT technologies tends to be backgrounded by the dominant terminology. Humans are often envisaged as simply another "node" of the IoT: as data-generating objects connected to other data-generating object (Lupton, 2019). Indeed, as the literature on smart cities imaginaries has demonstrated, humans tend to be "designed out" of expert visions of IoT futures (Cherry, Hopfe, MacGillivray, & Pidgeon, 2017) or treated as consumers who purchase corporate services rather than politically active citizens (Cardullo & Kitchin, 2019a, 2019b).

Many IoT technologies have yet to be implemented: they exist as idealised visions of the future. The social imaginaries that give meaning to IoT technologies are important to consider, as these imaginaries are ways of framing these technologies and inviting engagement with them in certain ways. The concept of social imaginaries relates to frameworks of culturally shared values and identities, forms of power–knowledge that draw from and shape people's responses to things like novel, emerging, and future digital technologies. Imaginaries come together as part of socio-material assemblages of people, things, and places when new technologies are made sense of and engaged with. They are configured by publics, government, industry, activists, and other stakeholders across a range of media, from policy reports to social media platforms (Herman, Hadlaw, & Swiss, 2014; Jasanoff, 2015).

Cultural geographers and those working in the sub-field of critical urban studies emphasise the importance of considering the spatial contexts in which IoT technologies are implemented and experienced. Spatial dimensions can influence what technologies are present and how they are interacted with by humans and other technologies. IoT technologies can also contribute to humans' sense of space and place (Hoffman & Novak, 2017). For example, Gram-Hanssen and Darby (2018) draw attention to understanding the concept of "home" when evaluating how people experience the smart home environment. As they note, sociological and other social scientific research on the concept of the home has identified several key elements: A home is viewed as a place of security, refuge, and control; for activity; for supporting relationships, a sense of belonging and continuity; and for portraying and expressing social status, identity and values. For smart home technologies to be successfully accepted and adopted into everyday life, they need to cohere well with these elements, rather than challenging or disrupting them.

Another important insight offered from the sociomaterial perspective is that IoT technologies can be said to have "double lives" (Lindley et al., 2019, p. 10). They operate in the world as individual material objects, and this is how most people experience them (e.g., when they use their digital home assistants or smart televisions). But there is a much more expanded dimension to the existence of IoT technologies of which many users are unaware. A vast, largely hidden conglomeration of human workers, technological infrastructures, and networks are in place to support the IoT: software, Wi-Fi, servers, continual data-generation and algorithmic processes that are central to smart devices' function and value, and the diverse range of human actors and agencies that are part of these digitally connected networks (Lindley et al., 2019). Smart technologies serve multiple purposes simultaneously, and the different actors and agencies that engage with them have different needs and purposes. For example, householders who use smart energy meters may value their convenience for tracking their homes' energy use, energy companies can use the technologies to save money on employing human meter readers, while power stations are able to use these data to better monitor patterns in community energy use (Lindley et al., 2019, p. 10).

3 | TECHNO-UTOPIAN IMAGINARIES

Social researchers have demonstrated that discourses on the IoT in industry, developer, and government discussions frequently present techno-utopian imaginaries, in which IoT technologies are portrayed as offering innovative solutions and ways to optimise the economy, industrial production, and transport systems and improve citizens' everyday

lives, as well as generate useful data that can be employed for commercial, developmental, or policy purposes. As is evident from other promotional representations of novel digital technologies such as AI and Big Data (Elish & Boyd, 2018; Lupton, 2019), a heightened sense of optimism is frequently put forward in these discussions. IoT technologies are often portrayed as almost magical in their capabilities and their power to be "disruptive" and "revolutionary" (Hazas & Strengers, 2019; Strand, Saltelli, Giampietro, Rommetveit, & Funtowicz, 2018; Strengers, Pink, & Nicholls, 2019).

IoT promoters and developers claim that the interconnected attributes of the IoT can potentially lead to many social and economic benefits, such as better knowledge of people's needs and behaviours, more personalised and customised services, better planning and policy development, improvements in manufacturing and agricultural processes, and more sustainable and efficient energy use. In recent years, a multitude of reports by government agencies and peak bodies such as the OECD, as well as promotional material by developers of the technologies, have championed these benefits. An oft-cited OECD report on the IoT, for example, opens with the statement: "The Internet of Things (IoT) could soon be as commonplace as electricity in the everyday lives of people in OECD countries. As such, it will play a fundamental role in economic and social development" (OECD, 2016, p. 4).

The IoT as a term and concept is itself a metaphor that suggests an imaginary of things that connect seamlessly with and through the Internet as part of a dense network of objects. Objects in the IoT universe are characterised in anthropomorphic terms as "intelligent," "smart," "sociable," and "communicative": in some cases, possessing capabilities beyond those of human intelligence and interactions (Mitew, 2014). Terminology employing the "smart" metaphor is frequently used interchangeably with the IoT. Concepts such as "smart cities," "smart environments," "smart factories," "smart healthcare," "smart agriculture," "smart transport," "smart workplaces," "smart schools," "smart hospitals," "smart grids," "smart buildings," and "smart homes" include reference to the IoT. Computer scientists and informatics researchers have often made bold claims relating to the futures of the IoT: for example, that they can operate by "putting intelligence into everyday objects," thereby working to "form a system where the real and digital worlds meet and are continuously in symbiotic interaction" (Borgia, 2014, p. 1).

In recent times, techno-utopian visions for IoT technologies are particularly promoted in relation to smart cities (sometimes referred to as "smart urbanism"). Smart cities are frequently positioned as providing many insights using ubiquitous computing, datafication, algorithmic processing, and real-time presentation of information in dashboards as well as stimulating their citizens' creativity and capacity for entrepreneurship (Kitchin, 2014b; Kitchin, Lauriault, & McArdle, 2015; Leszczynski, 2016). Many industry and government promotional representations of the smart city outline visions of a range of connected smart things and services such as smart homes, smart transport, smart schools, start-up and maker spaces, smart utilities systems, smart energy grids, and smart meters. Time and again, it has been pointed out by social researchers that smart city imaginaries position these urban spaces as modern, exciting, dynamic, efficient, prosperous, and sustainable (Caprotti & Cowley, 2019; Leszczynski, 2016; March, 2018; Sadowski & Bendor, 2018; Taylor Buck & While, 2017; White, 2016). These imaginaries have played a major role in corporate enterprises, architectural work, urban planning, and policy development (March, 2018).

Smart home technologies have also attracted utopian visions of the future of the home. These imaginaries represent IoT devices such as robotic cleaners, digital home assistants, smart security systems, and smart energy meters as offering greater comfort, relaxation, safety, convenience, and labour-saving capacities for people who take them up in their homes and, in some cases, as assisting with reductions in home energy use (Hargreaves, Wilson, & Hauxwell-Baldwin, 2018; Hazas & Strengers, 2019; Richardson, Hjorth, Strengers, & Balmford, 2017; Strengers, Kennedy, Arcari, Nicholls, & Gregg, 2019).

"Smart" often refers to energy efficiency, but it can also suggest a high level of sophistication of communication between the devices in the network, sensitivity, and responsiveness to changes in the environment (often involving AI and machine learning) as well as referring to the insights that can be garnered from the reams of digital data generated, processed, and exchanged by the technologies (Allhoff & Henschke, 2018; Gram-Hanssen & Darby, 2018). In these representations, smart things are often portrayed as possessing agencies distinct from the humans who are parts of their assemblages (Gram-Hanssen & Darby, 2018). IoT technologies are portrayed as contributing to the

generation of "smart" people rather than people being actively positioned as making the technologies smarter (Kitchin, 2014b; Vanolo, 2013). The background work of humans in assisting smart systems to operate is rendered invisible (Gray & Suri, 2019).

4 | RISKS AND HARMS

In stark contrast to the techno-utopian imaginaries of the possibilities of the IoT, social researchers have shown how popular culture has operated as an important source of dystopian imaginaries concerning the IoT. News reports of personal data breaches and citizen surveillance and science fiction such as the *Black Mirror* television series portray IoT technologies as harmful and disturbing (Cirucci & Vacker, 2018; Goode, 2018; Lupton, 2019). As these popular cultural representations suggest, the IoT blurs the boundaries between private and public domains in ways that can be perceived as unsettling or frightening (Lindley et al., 2019; Lindley, Coultona, & Altera, 2019; Pierce, 2019).

In these imaginaries, increasing datafication of people and the things with which they engage using sensor-based technologies in the IoT is considered to generate a raft of potential harms and risks. A central dystopian imaginary receiving expression in popular culture and industry fora relates to the apparent all-seeing power of digital technologies such as IoT devices. Statements appearing in the mass media such as "there is no such thing as privacy" or "the internet knows everything about you" make hyperbolic assumptions about the capacities of IoT technologies to discover and reveal people's secrets (Lupton, 2019).

There is further evidence of a growing awareness of issues relating to publics' data privacy and security in relation to the IoT in policy documents and the computer engineering literature. Contributors to this literature have highlighted the potential for the data generated by IoT technologies to be breached or leaked and for malicious actors to gain access to IoT systems with the intent to cause disruption. They note that the IoT is particularly vulnerable to such breaches or attacks because of the highly connected nature of the technologies involved and the combination of different datasets offering insights into people's behaviours and habits together with a lack of adequate protection of the systems against egress or failure. It is argued that as more smart devices become connected to each other and ever-greater amounts of data distributed among IoT networks, risks are heightened further (see, e.g., Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Van Oorschot & Smith, 2019).

This literature tends to discuss data privacy and security at an abstract, generalised, or technical level. Social researchers have made important observations about people's lived experiences and the broader political and socio-economic aspects of the use of personal data derived from IoT use, offering a perspective that goes beyond technological or regulatory fixes. They have pointed out that personal data from digital technology use have taken on value in the digital data economy, which can lead to exploitation by third parties and discrimination against marginalised social groups. These data, and other personal information generated by IoT devices, can potentially be sold to advertising and data harvesting and brokering companies and combined with other datasets to generate detailed data profiles and inferences about users (Kitchin, 2014a, 2014b; Sadowski, 2019; van Zoonen, 2016). It has been noted by many commentators that IoT-generated data could be used for government surveillance purposes, and cybercriminals could be hacking these data for their own purposes as well (Leszczynski, 2016; Lyon, 2018).

Researchers interested in human rights and social justice issues argue that the IoT is implicated in a number of "data harms" (Redden & Brand, 2019), including punitive or exploitative uses of "dataveillance": the watching of people using data generated about them (Best, 2010; Sadowski, 2019; Sadowski & Pasquale, 2015). These harms include becoming the subject of hidden surveillance, identity theft, and denial of opportunities such as access to credit, social services, credit, and insurance (Maras & Wandt, 2019; van Zoonen, 2016). The potential for the algorithmic decision-making processes undertaken by IoT technologies to be biased, exacerbating social inequalities and social marginalisation, has also been identified (Lindley et al., 2019). Social researchers have noted that dataveillance disproportionately affects already marginalised and disempowered social groups, frequently exacerbating poverty, racism, and sexism (Eubanks, 2018; Noble, 2018; O'Neil, 2016).

Colonisers have long used datafication and dataveillance as means of social control and government of the populations they have colonised (Arora, 2019). Indigenous and First Nations peoples have been particularly targeted by governments using dataveillance systems that restrict their rights and freedoms (Kukutai & Taylor, 2016; Lovett et al., 2019). IoT systems can potentially contribute to these processes. In some parts of Australia, for example, smart city technologies have been implemented in ways that are directed at making the activities of Indigenous populations more visible, perpetuating racism and socio-economic disadvantage (O'Malley & Smith, 2019).

Further, while promotional discourses on smart homes often champion their alleged benefits for better safety for families, social researchers have identified another serious unintended consequence of the security systems that are part of some homes: that of "smart abuse." Some of these technologies can be used by abusers to exert control by conducting digital surveillance on people, including intimidation and harassment of estranged partners or children, stalking them and potentially locating them for targeted violent attacks (Freed et al., 2019; Tanczer, Neira, Parkin, Patel, & Danezis, 2018; Vella, 2018). Smart toys contained within the home environment, which are typically marketed as promoting young children's safety, health, development, and well-being, can also open these vulnerable users to privacy and security risks. Researchers writing about Internet-connected toys designed for children (sometimes referred to as "the internet of toys") have highlighted the possibilities that these devices can facilitate surveillance of child users by the companies who sell the toys, by hackers—or indeed their own parents—in ways that limit their autonomy and challenge their privacy (Holloway, 2019; Holloway & Green, 2016; McReynolds et al., 2017; Milkaite & Lievens, 2019).

5 | LIVED EXPERIENCES

Compared with the extensive body of literature analysing the social imaginaries giving meaning to the IoT, only a relatively small number of studies have investigated people's lived experiences of IoT technologies. As social researchers have pointed out, people's engagements with smart technologies are characterised by improvisation, adaptation, and tinkering, involving forms of often invisible labour (Strengers, Pink, & Nicholls, 2019). These studies demonstrate that the ways that people engage with IoT technologies and the data generated from these technologies are highly contextual, with factors such as gender, age, skills, education level, income, and geographical location structuring their experiences.

The literature on smart homes has provided detailed analyses of people's experiences of living in these environments. This research has demonstrated that the utopian imaginaries promoted by smart home technology developers and advocates often fail to be realised in real-life engagements by users with the technologies. Yolande Strengers and colleagues have led the research on more recent smart home technologies, focusing on the Australian context and using ethnographic approaches (Jensen, Strengers, Kjeldskov, Nicholls, & Skov, 2018; Nicholls & Strengers, 2019; Strengers, Kennedy, et al., 2019; Strengers & Nicholls, 2018). For example, their study involving Australian families who were early adopters of smart home technologies involved home visits, interviews, and photographic documentation of participant's practices (Strengers, Kennedy, et al., 2019). The findings showed that the participants often used smart home surveillance technologies to engage in caring from remote locations by checking that children, family members with disabilities, or pets were safe and protected. They valued the use of smart security technologies to ensure that their homes were secured from intruders but were equally concerned about potential data privacy and security risks posed by third parties gaining access to the data generated by the smart home technologies. The participants also draw attention to the time and effort they were required to spend in "digital housekeeping": the labour involved in ensuring that the smart home technologies operated effectively. This work was often performed by male members of the household.

Another project undertaken by different researchers in the city of Loughborough, UK, also used ethnographic research with households participating in a 9-month trial of smart home technologies (Hargreaves et al., 2018). This study found that the technologies placed significant demands on the householders, which many participants found

frustrating and difficult. The technologies were experienced as both socially and technically disruptive and required forms of adaptation and familiarisation that delayed or limited their use by the participants. They were faced with challenges in learning how to use the devices with little available support. When they did manage to operate the systems successfully, the participants tended to stick to the simple rather than the more advanced modes of operation. Similar to the findings of research by Strengers and colleagues, this study found that the smart home technologies did not necessarily reduce energy use in the homes but rather could intensify energy demands.

Research that goes beyond examining smart city imaginaries to investigating how smart cities operate in practice—the "actually existing smart city" (Shelton, Zook, & Wiig, 2015)—has shown that smart city development is opportunistic, giving rise to unique local forms that tend to be shaped by immediate policy contexts and broader smart city discourses (Caprotti & Cowley, 2019; Karvonen, Cugurullo, & Caprotti, 2019; March, 2018). Smart city systems brought into pre-existing mature urban environments must be implemented in ways that can deal with the complexities of these environments, including tinkering, workarounds, and improvisations. These spontaneous activities are often a far cry from the idealised notions of smart cities. In these contexts, "the smart city is assembled piecemeal, integrated awkwardly into existing configurations of urban governance and the built environment" (Shelton et al., 2015, p. 15).

Researchers analysing the enactments of smart cities have shown that these initiatives and partnerships are redolent with numerous potential tensions (Caprotti & Cowley, 2019; Karvonen et al., 2019; Taylor Buck & While, 2017). These include the partial reliance of the smart cities vision on connections between different spheres of urban management and service provision in the context of increasing moves towards the splintering and disaggregation of these services, such as privatisation. Another tension emerges from the tendency of corporate actors offering smart city technologies to focus on wealthy cities or areas in cities with the capacity to pay for their services, to the exclusion of less socio-economically advantaged areas. Further, the contextual needs of specific areas require attention in service provision, but these are often ignored for a focus on developing universal solutions. A difficulty also lies in the lack of resources and technological expertise in public sector services compared with those enjoyed by the corporate smart city providers with which they attempt to partner (Caprotti & Cowley, 2019; Karvonen et al., 2019; Taylor Buck & While, 2017).

Analysis of smart city projects in Barcelona (March & Ribera-Fumaz, 2016) found that "smart" discourses and practices were both intentionally and unintentionally mobilised in ways that depoliticised urban redevelopment and environmental management programmes. The researchers identified manifold contradictions between what they characterised as the "grand visions" of the Barcelona smart city initiatives and the experiences of citizens of the city, most of whom were excluded from participation in the initiatives. They noted that Barcelona was opened as a testing ground to private capital to develop their smart projects. In many cases, the interests of the citizens of Barcelona were not compatible with those of these private enterprises. The researchers argue that there is a need to continue to direct planning and policy efforts to supporting and improving existing basic service infrastructures that in many cases may have little to do with smart city programmes.

The Tenison Road project, based in London, involved a year-long collaboration of Microsoft Research social researchers with academic computer scientists and geographers (Taylor, Lindley, Regan, & Sweeney, 2014). The project was directed at understanding how the production and use of digital and other forms of information about place are bound up with sociocultural and spatial dimensions: or what the researchers characterise as "data-in-place." The street's residents already had concerns about the increased traffic along their street and were looking for ways to intervene in the local council's and developers' plans. Residents were encouraged to curate existing information about the street in an archive, record aspects of the street such as residents' movements and the local plants and wildlife, and use citizen sensing to generate data about environmental pollution and flows of traffic through the street. This type of detailed investigation into how urban data that is situated and contextual can be generated through community-based activities highlights the ways in which by-product data generated by sensors and software installed by corporations in top-down initiatives often fail to document dimensions of places that are important to residents.

Smart farming devices include the deployment of devices such as sensors used to monitor soil, farm animals, water, and plants, with the intention of gathering detailed data to improve the efficiency, productivity, animal welfare, and environmental sustainability of farms and reduce pollution and overuse of pesticides and fertilisers. A growing body of social research has begun to examine the experiences of farmers with "smart farm" IoT technologies, thus moving beyond the urban context that has preoccupied many studies thus far (Blok & Gremmen, 2018; Eastwood, Klerkx, Ayre, & Dela Rue, 2019; Klerkx, Jakku, & Labarthe, 2019; Rotz et al., 2019). One example is a project based on New Zealand (Eastwood et al., 2019), including interviews with stakeholders involved with smart dairy farming technologies. The researchers noted that advocates for these IoT devices have tended to focus on technology development and on-farm use while ignoring the socio-ethical implications. The stakeholder interviews identified concerns about the potential for farm staff to lose their autonomy and become deskilled if relying on digital data, diminishing their embodied connection with and knowledge of their land and animals. Farmers also reported worries about outsiders assuming that the IoT technologies they were using were "unnatural," detrimental to animal welfare, or disruptive of accepted modes of dairying, potentially leading to the erosion of public trust in the quality of dairy foods. As these findings suggest, long-held and culturally situated beliefs and norms concerning farming knowledge, technologies, nature, and the embodied interactions of farmers with their livestock, crops, and the land are central to the acceptability and value of IoT technologies in agriculture for both farmers and publics. It is these kinds of issues and unexpected consequences that detailed interview-based and ethnographic research can surface.

6 | INTERVENING IN FUTURES

A key issue identified in the IoT social research literature is that of publics' trust in the IoT and how this can be adequately supported and protected in the light of the risks and potential harms that have been identified. Social researchers have noted that forecasting scenarios by experts addressing topics such as IoT technologies are problematic, as they tend to be based on economic modelling and rarely identify or acknowledge the tacit assumptions that underpin these scenarios. Little is known about citizens' desires or aspirations for smart environments such as smart cities or smart homes (Vanolo, 2016). In response, social researchers have called for a different way of developing forecasting scenarios that involve detailed understanding of the sometimes unexpected ways that people respond to novel technologies as part of the mundane routines of their everyday lives (Strengers, Pink, & Nicholls, 2019). For example, in their project involving developing future-oriented scenarios, Strengers and colleagues identified important factors such as people wanting to cater for the needs of their pets when engaging with smart energy use systems.

Researchers in critical urban studies have proposed some ideas for an alternative vision of the smart city. They call for an agenda that is oriented away from corporate interests and foregrounding the knowledge, interests, and priorities of socially and politically marginalised, disadvantaged, or excluded groups (Leontidou, 2015; McFarlane & Söderström, 2017). McFarlane and Söderström (2017) argue that to better imagine a future for smart cities that is more socially equitable, a return to an older definition of "smart" is required. They suggest that a citizen-led approach can allow for a different kind of learning about urban environments that foregrounds the kinds of knowledge and learning citizens need to improve their lives and environment.

Researchers working in speculative design, design fiction, and design futures have developed some methods for configuring new ways of imagining IoT technologies. These approaches seek to generate narratives and imaginaries concerning designed objects or services that are fictional, as a way of critically reflecting on the potential social impact of new and emerging technologies (Blythe et al., 2018; Coulton, Lindley, & Cooper, 2018). Some design researchers have sought to develop alternative metaphors or concepts to stimulate new ways of thinking about the IoT. They suggest that this work can also be a way of identifying and then confronting and possibly alleviating or resolving deep-seated anxieties concerning the IoT (Coulton et al., 2018; Pierce & DiSalvo, 2018).

In a design-led inquiry, Pierce (2019) took up the concept of "the creepy line" to develop three concepts pertaining to the futures of smart home security cameras. The creepy line refers to the boundary between what kinds of new digital technologies are considered useful and acceptable and which are not. Creepy is an adjective used in relation to digital technologies that create feelings of discomfort, anxiety, and suspicion. As Pierce notes, smart home technologies such as Internet-connected security cameras are particularly likely to be experienced as creepy because of their potential to facilitate surveillance of highly intimate spaces by third parties, including potentially malicious actors. The three concepts developed by Pierce were (a) digital leakage, or the propensity for personal digital data to be shared, stolen, or misused in ways unknown to those to whom this information pertains; (b) hole-and-corner applications, which are concealed from users and can be harmful or non-beneficial for them; and (c) foot-in-the-door devices, which work to normalise and integrate a technology that was previously rejected as unacceptable or unnecessary. In his article, Pierce outlines various speculative scenarios related to each of these concepts involving how these technologies may be taken up in the future.

In another example, Stead, Coulton, Lindley, and Coulton (2019) note that IoT technologies tend to be designed for inherent redundancy and disposability, rather than with sustainable design principles in mind that promote recycling, repair, and re-use of the devices. They generated design fictions involving imagined prototypes of IoT technologies that embody a set of key design criteria for sustainability. One example is the "Toaster for Life" prototype. This "smart" device has been designed with five primary sustainable attributes: its users can upgrade it, repair it, customise it, and recycle it, and all components and parts are trackable so that users can monitor how they are recycled if they dispose of them. This is a "Toaster for Life" because it is designed to never require replacement once purchased.

These studies work towards developing future scenarios that help to make sense of where IoT technologies may be heading. Once these imaginaries are created, the possibility for intervening in futures can be thought through. This may include identifying not only potential risks and harms but also ways in which the benefits of the IoT can be more effectively, ethically, and safely distributed. One example from design research is Seymour's (2019) prototype IoT device, which combines smart home assistant technology with enhancing users' awareness of their data privacy. His "Aretha" device is like Google Home or Alexa, with one key difference: Aretha is programmed to generate conversations with its users to alert them about how it and the smart devices to which it is connected are generating and using their data.

7 | CONCLUDING COMMENTS

As I have shown in this thematic review, social research has gone some way in identifying the social imaginaries giving meaning to the IoT and the complexities of the human/non-human relationships enacted as part of IoT assemblages. Social researchers have also emphasised that idealised promotional visions of the potential of IoT technologies frequently assume a seamless deployment and public acceptance, often concealing or glossing over the mundane, messy, frustrating, and sometimes frightening and dangerous realities of living with these technologies. Contributors to the literature discussed in this review have identified the ambivalences, breakdowns, glitches, and significant risks and unintended consequences of the IoT.

Social researchers have drawn attention to the gendered and spatial aspects of IoT experiences and the potential for abuse, racism, and other forms of social discrimination to be exacerbated by top-down deployment of these technologies. They have raised concerns about expert assumptions about how IoT technologies will be taken up, drawn attention to the lack of publics' engagements in contributing to the development of the IoT, and discussed important issues of social justice and public safety. However, this review has also demonstrated that while citizens tend to be "designed out" in IoT imaginaries, they are far from passive when they interact with IoT technologies as part of their daily lives. People may resist or re-imagine the use of IoT technologies rather than simply accept them in the ways imagined by the developers and promoters. Embedded within specific sociocultural, political, and spatial locations,

people tinker or improvise as they encounter "smart" things, devising ways to work around these devices' limitations or inventing ways to make unexpected uses of them.

For sociologists, a continued effort to acknowledge and engage with research taking place in the often scattered but cognate disciplines and fields which have been included in this review is vital to maintain a fresh and lively perspective on emerging technologies such as the IoT. Some researchers have begun to employ innovative methods to generate new and alternative ways of imagining IoT technologies, including co-design and speculative design methods. Continuing this strand of social research offers intriguing possibilities for challenging corporatised and top-down imaginaries of the IoT and giving publics more of a voice in future developments. This is particularly important for identifying the situated and spatially embedded experiences of engaging with "actually existing" IoT technologies in greater detail as well as uncovering the unexpected consequences of IoT deployment, such as exacerbating family violence or offering cybercriminals direct access to young children.

Social research needs to extend beyond the limited geographical range on which it has focused thus far and on the rapidly growing uses and domains of IoT technologies. As I have shown, social research on the IoT thus far has predominantly focused on the contexts of the smart city and smart home. While a major emphasis in reports from governments and institutions such as the OECD has focused on the industrial uses of IoT technologies, very few social researchers have addressed these domains of deployment. Further research should go beyond these applications to investigate social, cultural, and political dimensions of other emerging IoT environments, such as hospitals, schools, workplaces, and agriculture. Finally, most of the existing research has focused on the IoT in wealthy countries in the Global North. Yet the imaginaries of IoT technologies, such as those relating to the smart city, have now spread to regions such as Asia and Africa (McFarlane & Söderström, 2017). Future social research should direct attention to the spatial, political, and cultural specificities of how the IoT is developing globally.

ORCID

Deborah Lupton https://orcid.org/0000-0003-2658-4430

REFERENCES

Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things*, *1-2*, 55–66. https://doi.org/10.1016/j.iot.2018.08.005

Arora, P. (2019). Decolonizing privacy studies. *Television & New Media*, *20*(4), 366–378. https://doi.org/10.1177/1527476418806092

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*(1), 5–24. https://doi.org/10.1177/1367877909348536

Blok, V., & Gremmen, B. (2018). Agricultural technologies as living machines: Toward a biomimetic conceptualization of smart farming technologies. *Ethics, Policy & Environment*, *21*(2), 246–263.

Blythe, M., Encinas, E., Kaye, J., Avery, M. L., McCabe, R., & Andersen, K. (2018). Imaginary design workbooks: Constructive criticism and practical provocation. Paper presented at the *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal*, pp. 1–12.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1–31. https://doi.org/10.1016/j.comcom.2014.09.008

Caprotti, F., & Cowley, R. (2019). Varieties of smart urbanism in the UK: Discursive logics, the state and local urban context. *Transactions of the Institute of British Geographers*, *44*(3), 587–601. https://doi.org/10.1111/tran.12284

Cardullo, P., & Kitchin, R. (2019a). Being a 'citizen' in the smart city: Up and down the scaffold of smart citizen participation in Dublin, Ireland. *GeoJournal*, *84*(1), 1–13. https://doi.org/10.1007/s10708-018-9845-8

Cardullo, P., & Kitchin, R. (2019b). Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused' smart cities in Europe. *Environment and Planning C: Politics and Space*, *37*(5), 813–830. https://doi.org/10.1177/0263774X18806508

Cherry, C., Hopfe, C., MacGillivray, B., & Pidgeon, N. (2017). Homes as machines: Exploring expert and public imaginaries of low carbon housing futures in the United Kingdom. *Energy Research & Social Science*, *23*, 36–45. https://doi.org/10.1016/j.erss.2016.10.011

Cirucci, A., & Vacker, B. (Eds.). (2018). *Black Mirror and critical media theory*. Lanham: Rowman & Littlefield.

Coulton, P., Lindley, J., & Cooper, R. (2018). *The little book of design fiction for the Internet of Things*. Lancaster: Imagination Lancaster.

Eastwood, C., Klerkx, L., Ayre, M., & Dela Rue, B. (2019). Managing socio-ethical challenges in the development of smart farming: From a fragmented to a comprehensive approach for responsible research and innovation. *Journal of Agricultural and Environmental Ethics*, *32*(5), 741–768. https://doi.org/10.1007/s10806-017-9704-5

Elish, M. C., & boyd, d. (2018). Situating methods in the magic of Big Data and AI. *Communication Monographs*, *85*(1), 57–80.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press.

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019). "Is my phone hacked?" Analyzing clinical computer security interventions with survivors of intimate partner violence. *Proceedings of the ACM on Human–Computer Interactions*, *3*, 202:201–202:224. doi:https://doi.org/10.1145/3359304

Gartner. (2017). Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. Gartner.com. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Goode, L. (2018). Life, but not as we know it: AI and the popular imagination. *Culture Unbound: Journal of Current Cultural Research*, *10*(2), 185–207.

Gram-Hanssen, K., & Darby, S. J. (2018). "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science*, *37*, 94–101. https://doi.org/10.1016/j.erss.2017.09.037

Gray, M. L., & Suri, S. (2019). *Ghost work: How to stop Silicon Valley from building a new global underclass*. Boston: Houghton Mifflin Harcourt.

Hargreaves, T., Wilson, C., & Hauxwell-Baldwin, R. (2018). Learning to live in a smart home. *Building Research & Information*, *46*(1), 127–139. https://doi.org/10.1080/09613218.2017.1286882

Hazas, M., & Strengers, Y. (2019). Promoting smart homes. In J. Rinkinen, E. Shove, & J. Torriti (Eds.), *Energy fables: Challenging ideas in the energy sector*. London: Routledge.

Herman, A., Hadlaw, J., & Swiss, T. (2014). Introduction: Theories of the mobile Internet: Mobilities, assemblages, materialities and imaginaries. In A. Herman, J. Hadlaw, & T. Swiss (Eds.), *Theories of the mobile Internet: Materialities and imaginaries* (pp. 13–24). London: Routledge.

Hoffman, D. L., & Novak, T. P. (2017). Consumer and object experience in the Internet of Things: An assemblage theory approach. *Journal of Consumer Research*, *44*(6), 1178–1204. https://doi.org/10.1093/jcr/ucx105

Holloway, D. (2019). Surveillance capitalism and children's data: The Internet of toys and things for children. *Media International Australia*, *170*(1), 27–36. https://doi.org/10.1177/1329878X19828205

Holloway, D., & Green, L. (2016). The Internet of toys. *Communication Research and Practice*, *2*(4), 506–519.

Jasanoff, S. (2015). Future imperfect: Science, technology, and the imaginations of modernity. In S. Jasanoff & S.-H. Kim (Eds.), *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power* (pp. 1–33). Chicago: University of Chicago Press.

Jensen, R. H., Strengers, Y., Kjeldskov, J., Nicholls, L., & Skov, M. B. (2018). Designing the desirable smart home: A study of household experiences and energy consumption impacts. Paper presented at the *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, *Montreal*, pp. 1–14.

Karvonen, A., Cugurullo, F., & Caprotti, F. (2019). Introduction: Situating smart cities. In A. Karvonen, F. Cugurullo, & F. Caprotti (Eds.), *Inside smart cities: Place, politics and urban innovation* (pp. 19–30). London: Routledge.

Kitchin, R. (2014a). *The data revolution: Big data, open data, data infrastructures and their consequences*. London: Sage.

Kitchin, R. (2014b). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1–14.

Kitchin, R., Lauriault, T. P., & McArdle, G. (2015). Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards. *Regional Studies, Regional Science*, *2*(1), 6–28. https://doi.org/10.1080/21681376.2014.983149

Klerkx, L., Jakku, E., & Labarthe, P. (2019). A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. *NJAS—Wageningen Journal of Life Sciences*, 90–91. http://www.sciencedirect.com/science/article/pii/S1573521419301769, https://doi.org/10.1016/j.njas.2019.100315

Kukutai, T., & Taylor, J. (Eds.). (2016). *Indigenous data sovereignty: Toward an agenda*. Canberra: ANU Press.

Leontidou, L. (2015). 'Smart cities' of the debt crisis: Grassroots creativity in Mediterranean Europe. *Επιθεώρηση κοινωνικών Ερευνών*, *144*(144), 69–101.

Leszczynski, A. (2016). Speculative futures: Cities, data, and governance beyond smart urbanism. *Environment and Planning A: Economy and Space*, *48*(9), 1691–1708. https://doi.org/10.1177/0308518X16651445

Lindley, J. G., Coulton, P., Akmal, H., Hay, D., Van Kleek, M., Cannizzaro, S., & Binns, R. (2019). *The little book of philosophy for the Internet of Things*. Lancaster: Imagination Lancaster.

Lindley, J., Coultona, P., & Altera, H. (2019). Networking with ghosts in the machine. Paper presented at the *Running with Scissors, 13th EAD Conference, Dundee*, pp. 1–13.

Lovett, R., Lee, V., Kukutai, T., Cormack, D., Rainie, S. C., & Walker, J. (2019). Good data practices for Indigenous data sovereignty and governance. In A. Daly, S. K. Devitt, & M. Mann (Eds.), *Good data* (pp. 26–36). Amsterdam: Institute of Network Cultures.

Lupton, D. (2019). *Data selves: More-than-human perspectives*. Cambridge: Polity Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. New York: John Wiley & Sons.

Maras, M.-H., & Wandt, A. S. (2019). Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, *4*(2), 160–177. https://doi.org/10.1080/23738871.2019.1590437

March, H. (2018). The smart city and other ICT-led techno-imaginaries: Any room for dialogue with degrowth? *Journal of Cleaner Production*, *197*, 1694–1703. https://doi.org/10.1016/j.jclepro.2016.09.154

March, H., & Ribera-Fumaz, R. (2016). Smart contradictions: The politics of making Barcelona a self-sufficient city. *European Urban and Regional Studies*, *23*(4), 816–830. https://doi.org/10.1177/0969776414554488

Martín-Martín, A., Orduna-Malea, E., Thelwall, M., & Delgado López-Cózar, E. (2018). Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories. *Journal of Informetrics*, *12*(4), 1160–1177. https://doi.org/10.1016/j.joi.2018.09.002

McFarlane, C., & Söderström, O. (2017). On alternative smart cities. *City*, *21*(3–4), 312–328. https://doi.org/10.1080/13604813.2017.1327166

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys that listen: A study of parents, children, and internet-connected toys. Paper presented at the *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver*, pp. 5197–5207.

Milkaite, I., & Lievens, E. (2019). The Internet of toys: Playing games with children's data? In G. Mascheroni & D. Holloway (Eds.), *The Internet of toys: Practices, affordances and the political economy of children's smart play* (pp. 285–305). Cham: Springer International Publishing.

Mitew, T. (2014). Do objects dream of an Internet of Things? *The Fibreculture Journal*, *23*. http://twentythree.fibreculturejournal.org/fcj-168-do-objects-dream-of-an-internet-of-things/

Nicholls, L., & Strengers, Y. (2019). Robotic vacuum cleaners save energy? Raising cleanliness conventions and energy demand in Australian households with smart home technologies. *Energy Research & Social Science*, *50*, 73–81.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: NYU Press.

O'Malley, P., & Smith, G. (2019). Disruption as distraction: Darwin's Smart City program, public resistance and the racialization of digital governance. Paper presented at the *Disrupting Data Injustices Roundtable, UNSW Sydney*.

O'Neil, C. (2016). *Weapons of math destruction: How Big Data increases inequality and threatens democracy*. London: Penguin Books.

Organisation for Economic Co-operation and Development. (2016). The Internet of Things: Seizing the benefits and addressing the challenges. *OECD Digital Economy Papers*, *252*. https://www.oecd-ilibrary.org/science-and-technology/the-internet-of-things_5jlwvzz8td0n-en

Pierce, J. (2019). Smart home security cameras and shifting lines of creepiness: A design-led inquiry. Paper presented at the *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow*, pp. 1–14.

Pierce, J., & DiSalvo, C. (2018). Addressing network anxieties with alternative design metaphors. Paper presented at the *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal*, pp. 1–13.

Redden, J., & Brand, J. (2019). Data harm record. https://datajusticelab.org/data-harm-record/

Richardson, I., Hjorth, L., Strengers, Y., & Balmford, W. (2017). Careful surveillance at play: Human–animal relations and mobile media in the home. In E. G. Cruz, S. Sumartojo, & S. Pink (Eds.), *Refiguring techniques in digital visual research* (pp. 105–116). Houndmills: Palgrave Macmillan.

Rotz, S., Duncan, E., Small, M., Botschner, J., Dara, R., Mosby, I., … Fraser, E. D. G. (2019). The politics of digital agricultural technologies: A preliminary review. *Sociologia Ruralis*, *59*(2), 203–229. https://doi.org/10.1111/soru.12233

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, *6*(1), 205395171882054. doi:10.1177/2053951718820549. https://doi.org/10.1177/2053951718820549

Sadowski, J., & Bendor, R. (2018). Selling smartness: Corporate narratives and the smart city as a sociotechnical imaginary. *Science, Technology, & Human Values*, *44*(3), 540–563. https://doi.org/10.1177/0162243918806061

Sadowski, J., & Pasquale, F. (2015). The spectrum of control: A social theory of the smart city. *First Monday.*, *20*. http://firstmonday.org/ojs/index.php/fm/article/view/5903/4660

Seymour, W. (2019). Privacy therapy with Aretha: What if your firewall could talk? Paper presented at the *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow*, pp. 1–6.

Shelton, T., Zook, M., & Wiig, A. (2015). The 'actually existing smart city. *Cambridge Journal of Regions, Economy and Society*, *8*(1), 13–25. https://doi.org/10.1093/cjres/rsu026% J Cambridge Journal of Regions,Economy and Society

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Stead, M. R., Coulton, P., Lindley, J. G., & Coulton, C. (2019). *The little book of sustainability for the Internet of Things*. Lancaster: Imagination Lancaster.

Strand, R., Saltelli, A., Giampietro, M., Rommetveit, K., & Funtowicz, S. (2018). New narratives for innovation. *Journal of Cleaner Production*, *197*, 1849–1853. https://doi.org/10.1016/j.jclepro.2016.10.194

Strengers, Y., Kennedy, J., Arcari, P., Nicholls, L., & Gregg, M. (2019). Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters. Paper presented at the *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow*, pp. 1–13.

Strengers, Y., & Nicholls, L. J. M. I. A. (2018). Aesthetic pleasures and gendered tech-work in the 21st-century smart home. *Media International Australia*, *166*(1), 70–80.

Strengers, Y., Pink, S., & Nicholls, L. (2019). Smart energy futures and social practice imaginaries: Forecasting scenarios for pet care in Australian homes. *Energy Research & Social Science*, *48*, 108–115. https://doi.org/10.1016/j.erss.2018.09.015

Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT research report. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf

Taylor, A. S., Lindley, S., Regan, T., & Sweeney, D. (2014). Data and life on the street. *Big Data & Society*, *1*(2), 205395171453927. http://bds.sagepub.com/content/1/2/2053951714539278.abstract

Taylor Buck, N., & While, A. (2017). Competitive urbanism and the limits to smart city innovation: The UK Future Cities initiative. *Urban Studies*, *54*(2), 501–519. https://doi.org/10.1177/0042098015597162

Van Oorschot, P. C., & Smith, S. W. (2019). The Internet of Things: Security challenges. *IEEE Security & Privacy*, *17*(5), 7–9.

Vanolo, A. (2013). Smartmentality: The smart city as disciplinary strategy. *Urban Studies*, *51*(5), 883–898. https://doi.org/10.1177/0042098013494427

Vanolo, A. (2016). Is there anybody out there? The place and role of citizens in tomorrow's smart cities. *Futures*, *82*, 26–36. https://doi.org/10.1016/j.futures.2016.05.010

Vella, H. (2018). Smart abuse: Who controls the controls? *Engineering Technology*, *13*(6), 44–47.

Weber, S., & Wong, R. Y. (2017). The new world of data: Four provocations on the Internet of Things. *First Monday*, *22*(2). https://firstmonday.org/ojs/index.php/fm/article/view/6936

White, J. M. (2016). Anticipatory logics of the smart city's global imaginary. *Urban Geography*, *37*(4), 572–589. https://doi.org/10.1080/02723638.2016.1139879

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

AUTHOR BIOGRAPHY

Deborah Lupton is a SHARP Professor in the Faculty of Arts & Social Sciences, UNSW Sydney, working in the Centre for Social Research in Health and the Social Policy Research Centre and leading the Vitalities Lab. She is the author/co-author of 17 books, the latest of which are *Digital Sociology* (Routledge, 2015), *The Quantified Self* (Polity, 2016), *Digital Health* (Routledge, 2017), *Fat*, *Second Edition* (Routledge, 2018), and *Data Selves* (Polity, 2019). Professor Lupton is a Chief Investigator and leader of the UNSW Node of the Australian Research Council Centre of Excellence in Automated Decision-Making and Society (2020–2026). She is currently serving as a Commissioner on The Lancet and Financial Times Commission "Governing Health Futures 2030: Growing Up in a Digital World" (2019–2021). She is a Fellow of the Academy of the Social Sciences in Australia and holds an Honorary Doctor of Social Science degree awarded by the University of Copenhagen.

How to cite this article: Lupton D. The Internet of Things: Social dimensions. *Sociology Compass*. 2020;14: e12770. https://doi.org/10.1111/soc4.12770