Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2018: 1–14

DOI: 10.1177/2053951718756685
journals.sagepub.com/home/bds
SAGE

Data anxieties: Finding trust in everyday digital mess

Sarah Pink[1], Debora Lanzeni[2] and Heather Horst[3]

Abstract

Digital data is an increasing and continual presence across the sites, activities and relationships of everyday life. In this article we explore what data presence means for the ways that the everyday is organised, sensed, and anticipated. While digital data studies have demonstrated how data is deeply entangled with the way in which everyday life is lived out and valued, at the same time our relationships with data are riddled with anxieties or small niggles or tricky trade-offs and their use is often chaotic and muddled, part of the inevitable uncertainty about what will happen next. If the presence of data is part of the environments we inhabit, this raises the question of how and why data is valuable to us and what forms of hope and trust enable this value to further develop.

Keywords

Anticipatory modes, data anxiety, ethnography, everyday life, futures, technology designers

Introduction

In May 2017 a global cyber attack struck businesses and individuals across the world. Despite including high profile targets, the BBC News reported that: 'only around $60,000 (£46,500) has been paid in ransoms, according to analysis of Bitcoin accounts being used by the criminals. With more than 200,000 machines infected, it's a terrible return' (http://www.bbc.com/news/technology-39931635). There are many possible explanations for this. However, part of the jigsaw of reasons why people and organisations would not bother paying a ransom could simply be because they never thought their data was particularly secure anyway. For instance, Chris, a technology developer who participated in our research explained how for the drone development team he worked with, data could always be lost. As he described it: 'You try and sort of mitigate those circumstances by having some redundancy and having some backups written into the projects you are doing', but he emphasised that, 'no matter how many precautions you take', data could be lost. Almost everyone we interviewed knew or knew of someone who had lost significant digital data in some way, such as due to hardware failure, losing or forgetting passwords, or online platforms closing down. Digital data is rarely thought of by its everyday users as safe, easy to access or manage, or, in the case of personal data, necessarily accurate. There is a growing academic interest in anxieties about data security, surveillance and power (e.g. Barassi, 2017; Dencik et al., 2017) and in how people use and experience self-tracking technologies (Lupton, 2016; Pink and Fors, 2017a, 2017b; Pink et al., 2017a; Ruckenstein, 2016). This literature provides insights into how personal data is created, and used by individuals and organisations. However we still know very little about how everyday data producers and users experience the safety of data storage techniques and technologies in everyday life, what uncertainties, anxieties and concerns, or hopes and forms of trust their relations with data entail, or how these are dealt with.

[1]RMIT University, Melbourne, Australia
[2]RMIT University, Barcelona, Spain
[3]University of Sydney, Australia

Corresponding author:
Sarah Pink, College of Design and Social Context, RMIT University, Melbourne, Victoria 3000, Australia.
Email: sarah.pink@rmit.edu.au

In this article we take a design anthropological approach that accounts for the emergent circumstances of everyday life (Pink et al., 2016; Smith and Otto, 2016) to examine how people improvise to keep their data safe in mundane everyday working, personal and community or technology meetup activities. For anthropologists Tim Ingold and Elizabeth Hallam, improvisation is 'a necessary condition because there is no existing template that instructs us in how to deal with the continually changing contingencies of life' (Ingold and Hallam, 2007: 2), and is 'inseparable from our performative engagements with the materials that surround us' (Ingold and Hallam, 2007: 3). As design anthropologists Wendy Gunn and Christian Clausen express it, by improvising people 'find ways of keeping on going' (2013: 174). We are concerned with how people experience living with data, the anticipatory modes this entails, and how in proceeding through their everyday work or personal activity they improvise to reduce, obscure or alleviate anxieties about data storage and safety. This involves getting under the surface of what data might initially appear to be and encountering the messiness of activities and feelings that surround data. Based on our ethnographic research and interviews in Melbourne, Australia and Barcelona, Spain, which focused upon the value of everyday data in the lives of people who worked with digital technologies in different ways, we advance an understanding of data as incomplete, often dispersed, and saved or stored according to contingent actions and logics. In doing so we highlight the everyday anxieties associated with data. These anxieties relate to how people experience the realities of the messiness of digital data, their uncertainties about how data might be used or accessed in the future, and anticipation around its loss.

To develop our argument we begin by outlining what we mean by data anxiety, and the associated anticipatory terms of trust, and by contrast, hope, through which these anxieties are eased. In doing so we propose a theory of what it feels like to live with data, which informs the discussion in this article. We then provide further details of the ethnographic research sites and processes that enabled us to unravel how people improvise to feel comfortable with data through practices such as creating redundancy and transparency. We conclude by arguing for greater attention to these temporalities of data, and reflecting upon the implications of such work for visions of the future of technologies and data.

Data, anxiety and trust

Digital data is an increasing and continual presence across the sites, activities and relationships of everyday life. Yet, as Dourish and Bell (2011: 4–5) have pointed out technology is not simple, but involves the 'mess' of its constituent or related parts, as well as that of the institutions, power relations that govern its use, and the conflicting discourses that define it. Data also exists within this messy world. For social scientists (digital) data is a critical category rather than a self-evident or given fact (Baym, 2013; boyd and Crawford, 2012; Markham, 2013; Nafus, 2014). Indeed, what has been called the datafication of our everyday lives and worlds – defined as 'the ability to render into data many aspects of the world that have not been quantified before' (Cukier and Mayer-Schoenberger, 2013), has been discussed across many domains of everyday experience including health (Ruckenstein and Dow Schüll, 2017), regulatory and preventative governance and policing (Dencik et al., 2017; Smith and O'Malley, 2017), space (Sumartojo et al., 2016) and sport (Millington and Millington, 2015). Whereas these discussions of data reveal important dimensions of the meaning of how different populations and domains are using data, we focus our attention on how people feel about the safety of their data.

We take as our starting point the impossibility of knowing our futures (Pink and Salazar, 2017) and the need to recognise that 'our futures are contingent because our present is as well' (Bessire and Bond, 2014: 450), whereby understanding how futures are anticipated has become increasingly embedded in contemporary research agendas. As Adams et al. (2009) note, 'one defining quality of our current moment is its characteristic state of anticipation, of thinking and living toward the future' (246). Existing research has critically examined the anticipatory modes of digital data use in social media data for predictive measures such as policing (e.g. Dencik et al., 2017), which is characteristic of the risk averse and audit based cultures of neoliberal states, as demonstrated by research into civil contingencies (Anderson, 2010), safety (Pink et al., 2017a) and ethics (Pink, 2017). Design anthropology approaches everyday life circumstances as emergent (Pink et al., 2016; Smith and Otto, 2016), attending to how people improvise to fill in the gaps between what they think they know and the inevitable uncertainties that actions entail. In these everyday life contexts future focused data practices are central; however, in contrast to the risk mitigation strategies of regulatory governance, they are idiosyncratic and improvisatory. We engage the concept of data anxiety and the related concept of trust to demonstrate how everyday improvisatory actions enabled participants in our research to feel comfortable in this anticipatory mode.

While there is an existing body of scholarship about trust in the social sciences and humanities, it has not developed as a central or mainstream concern for most

academic disciplines. Nevertheless, in an increasingly interdisciplinary context questions about digital trust are frequently foregrounded particularly in organisation studies and in the human–computer interaction (HCI) research field, with particular reference to how and if people will trust new technologies, interfaces, forms of automation and artificial intelligence (e.g. Harper, 2014). Trust, as experienced by our research participants, was coherent with our focus on process, emergence and (im)possible rather than predictable futures. This therefore involves approaching the concept of trust as a feeling that specifically refers to the ability to be able to move on and do something in the immediate future. It need not involve absolute certainty, but entails feeling and knowing enough to be able to take the next step. Hope, in contrast to trust, tends to be related to the aspirational dimensions of how we imagine futures. Pedersen and Liisberg discuss the 'imaginary anticipation' of both hope and trust since 'They concern future states that exceed the immediate control of the person trusting or hoping'. They suggest that 'whereas trust typically concerns near and probable futures that mostly meet our expectations, hope may well paint a scenario of a possible and radically different future' (Pedersen and Liisberg, 2015: 1). Our core focus here is the immediacy of trust, and its relatedness to the activities of improvisation that enable us to step forward in uncertain circumstances (Gunn and Clausen, 2013). Trust is the element of this in which we feel sufficiently confident to be able to act, whereby 'Confidence based on familiarity is the foundation of getting involved in a situation' and differentiates trust from risk (Fredricksen, 2016: 59).

Following this argument, humans trust when we feel confident enough that any improvisatory action is sufficiently cushioned by the familiarity of process or place. This might not be a cognitive decision but rather a sensory experience of feeling or disposition towards something. However, the sense of familiarity is a key. Familiarity is associated with routine. Routines are not always repeated in exactly the same way every time, since nothing can ever be done in the same way more than once. Rather routines are similar enough to be recognised by people as being repeats of previous actions, thoughts and embodied sensory feelings. Thus, people feel comfortable in routines and they feel accomplished when they have completed them (Pink et al., 2017b). It has long since been understood in the social sciences that routines are associated with feelings of what Giddens (1991) called 'ontological security'. As the examples discussed below highlight, even when such security and familiarity is felt, it does not mean that the immediate or far futures are secured. Rather trust is a feeling that is part of a mode of living in a world of uncertainties that 'feels right', a sense of control in a space of uncertainty.

Trust is thus part of how we live with data. This framing of data contextualises its use and the way it is experienced within the everyday uncertainties that people ongoingly have to cope with as they navigate their ways through the contingencies of life. Living with and having to take responsibility for data manifests itself in the form of mundane and often small but relevant anxieties, which might be experienced as more explicit worries, niggles and sometimes feelings of confusion. Yet, people improvise as they go about quashing or suppressing the uncertainties that give rise to anxieties, through taking improvisatory steps in everyday familiar routines or adhering to convincing (for them) logics. These, modes of dealing with everyday anxieties we argue generate forms of trust which enable people to proceed in everyday life and moreover to imagine and work towards everyday futures. Understanding this fills an important gap in our knowledge about how people live with data in the present, and can help us subsequently to think about how people will continue to live with data in an as-yet-unknown and uncertain future.

The anticipatory states most discussed in recent literature on data refer to the anxieties that are experienced, expressed and imagined both in the datafied present and as yet unknown datafied futures have mainly been researched and reported on in relation to questions of security, privacy, and fears about the future implications of what other people, organisations or governance systems might do with data in the future. For example Kate Crawford (2016) proposed that 'Already, the lived reality of Big Data is suffused with a kind of *surveillant anxiety* – the fear that all the data we are shedding every day is too revealing of our intimate selves but may also misrepresent us', which she suggested is coupled with the anxiety of the surveillers fuelled by their awareness that their data will always be incomplete and insufficient. More recent studies have revealed that there certainty are public concerns about data and privacy, such as in fields focused upon governance and security (e.g. Chan and Bennett Moses, 2017). Sometimes this has led to forms of activism, for instance against data driven crime prevention (Smith and O'Malley, 2017), health monitoring (for an example see http://www.unfitbits.com/) and of course actions like that of Edward Snowden (see also Crawford, 2016). While these sets of anxieties and the activist and progressive stances they invoke form an important, and indeed inescapable backdrop to the questions we discuss in this article, data anxieties are not only about the public and more 'spectacular' spheres of life, like public activism and the surveillant modes of large organisations. They are moreover not only related to questions

of Big Data, datafication and their impact of our lives. Therefore, while we acknowledge that questions relating to power and privacy are also integral to the everyday data management, our objective here is introduce another element of data anxieties. In the following two sections, we draw attention to another, equally prevalent but less visible and little discussed element of data anxiety: the anxieties associated with the kinds of everyday data that people handle in the course of their mundane daily routines of home and work life, and which indeed are part of how these two domains sometimes become inseparable from each other.

The ethnographic context

The original impetus for the study emerged from a programme of research with an industry partner that focused on futures and forms of value in relation to digital technologies, data and design. Within this we undertook fieldwork for six months, between November 2016 and April 2017, in Barcelona (Spain) and Melbourne (Australia), while drawing on several years of previous fieldwork in Barcelona. The theme of data anxieties discussed in this article emerged from and was explored within this project.

Barcelona and Melbourne present ideal opportunities for an international study. The two cities belong to different national economies, one of which is relatively affluent (Melbourne) and the other which is in the throes of an economic crisis (Barcelona). However, in spite of this difference they are both global cities of similar population sizes (Barcelona $4.6\,m^1$, and Melbourne over $4.5\,m^2$), and comprise international communities of people involved in technology design. The participants in our research were all selected because they already used digital data extensively in their everyday and working lives. Most of the participants had a strong interest in technology making, design and digital fabrication and either worked in the technology field currently or had a background in technology. However they represented a spectrum of skills in this field, with some being highly skilled in technology design while the skills of others were focused across digital archiving, marketing, events management and technological forums. Participants were aged between 20 to 60 years, with an equal gender division amongst younger participants. Older participants were mostly men.

We undertook ethnographic fieldwork across a series of sites considered relevant due to their focus on emerging technologies: FabLab Barcelona, which houses many digital technology research, development and education programmes, principally with community, educational and non-profit organisations. Launchpad, a coworking and business accelerator located in the suburb of Richmond in Melbourne, where technology meetups and events occurred regularly making it a focus point for the technology start-up community; Make Create, the first makerspace established in Melbourne where groups of technology designers meet to share knowhow and collaborate in technology projects; and the Bitcoin/Blockchain Center in Melbourne. Bitcoin is a decentralised cryptocurrency which allows its users to make transactions without going through third party (such as a bank). Blockchain is the technology makes these transactions possible and visible (for Bitcoin and other transactions), through a dispersed leger system that involves multiple computers, rather than a centralised system.[3] Our fieldwork consisted of a series of encounters where we attended and participated in events and meetups of different sizes (from just a handful of people at a small meet-up to over 100 at Launchpad events) using visual and sensory ethnography research techniques in these interactions (Pink, 2013, 2015) as appropriate, in negotiation with the participants and organisations. We conducted ethnographic interviews, participant observation, ethnographic workshops and tours (Maddox et al., 2016). We video recorded at events and during interviews, especially when we asked them to show us how they enacted and experienced certain data related activities. In all instances our approach to ethnography engaged participants in co-producing ways of knowing with us within the research process and in receiving our feedback about what we had learned with them and because participants worked in the technology field they were interested in our research. In this particular article we discuss how participants saved, moved and stored their data, how they made sure it was safe or secure, and how and why they believed it would be safe in those particular circumstances.

The data anxieties and the activities people engage in to quell them represented a particular strand of the research that referred to something that was not visible through conventional ethnography for two reasons. First, the routines and activities we became interested in were practices that we discovered were used to repress the feelings of anxiety around data. These feelings were rarely expressed or articulated by participants prior to this work. Thus, it did not necessarily exist in the moment that we researched it but needed to be recalled. Data anxieties are real, and felt, but they are ephemeral. They refer to feelings experienced during the flow of everyday life, about a lingering future possibility rather than an explicit state of affairs that has come about in the present. For this reason we sought to research a feeling that we could not locate or witness through observation, and which participants themselves often could not find, until we focused discussions

with them on particular memories of experiences where it had surfaced.

Second, our research subject was elusive because the practical manifestations of data anxieties that might be witnessed ethnographically involved very mundane everyday routines that participants rarely shared with others, and usually performed when alone. Therefore ethnographic fieldwork in workplace localities and participation in events enabled us to observe the visible dimensions of data use and, as shown below to sometimes witness the moments when collective data anxieties were revealed. However, to go under the surface more systematically we collaborated more deliberately with participants by focusing with them in video recorded interviews usually held at the fieldwork locations, and in the workshop. Wherever possible during the interviews participants used and referred to their technologies, showing us how they used them or using them as memory prompts regarding their data activities. Thus in the interview encounters and the workshop we could follow up on moments and hunches, when questions around data anxieties and routines were implied that had emerged during our ethnographic fieldwork.

Strategies for managing data and uncertainty

In the final stages of our research we invited a small group of key participants involved in the Blockchain, tech design and maker environments in Melbourne to the workshop mentioned in the previous section. At the workshop we collaborated with the participants to co-create a hierarchy of what technologies were most trusted and why. While we had in mind a possible discussion of devices, platforms, apps, software, hardware and forms of certification, the participants collectively insisted that the most trustworthy technologies were pen and paper. The discussion explicitly acknowledged that the participants did not regard digital technologies and data as reliable and trustworthy, even though they depended on them for their livelihoods. This might not be a surprising finding for people who work in technology design and development, however, its significance is that it reiterates the point that living with data is coterminous with living with uncertainty. In this section we discuss two modes of coping with the data anxieties associated with uncertainty and forms of trust that are implicated in these: redundancy and transparency.

Redundancy

As we have emphasised, all our participants acknowledged that their data could be lost, stolen, deleted or in some other way become inaccessible to them. They all knew someone who had lost a substantial amount of digital data, or had lost data themselves, and remembered and consistently recounted stories about this. The stories differed in terms of how data was lost and the software and hardware involved. For example, one participant had lost bitcoin investments in the wake of a poorly designed system, another feared that the platform where she archived her PhD notes would close down without her being able to transfer her materials. These narratives demonstrated how data could be lost in any imaginable configuration of hardware and software, but that this might not always matter, or was something that people always knew was possible. Thus participants did not trust their technologies as failsafe devices for securing their data. Yet simultaneously found ways of dissipating any anxieties around this. Indeed sometimes people's experiences of loss or possible loss appeared not to correspond with their use of their technologies. For instance, another participant did not bother creating a password on her smartphone, yet in the same interview described how she had spent a series of days waiting worriedly while her boyfriend fixed her broken laptop with the help of YouTube videos, leaving it in pieces on their dining table during the process. Other participants described data that they considered to be desirable to keep but not worth the level of care and curation required to ensure that it was either duplicated or even easily accessible. Many participants discussed with us how they managed their multiple email accounts and the data (files, messages) that they contained. Data kept in email archives was not necessarily considered to be data that would be accessed again but that it was good to keep, it formed what we refer to as *data presence*, creating a sense of security that files that were in it could be potentially searched and retrieved, even if it was unlikely this would ever happen, and would possibly be difficult to locate through search functions.

Depending on the logics of loss and access through which they understood data and performed their own mundane everyday improvisatory activities with data, participants variously felt that they could sufficiently trust different configurations of software and hardware. For example, one Melbourne based participant Julien, had previously worked providing technology expertise in a company, and recently left his role to set up a drone start-up with a group of colleagues. Julien had encountered people who had lost access to their data very frequently when in his former role and was keen to stress that he felt data was never safe, and that you can never guarantee or be completely confident that it will not be lost, even if individual knowhow could be a key factor in relation to if data retrieval. In anticipation of this potential loss, he tried to ensure a certain level of duplication in his data archiving, keeping, for example, one copy in the

cloud, another easily accessible on an networked device he used on a daily basis, and another copy saved at home on a non-networked device. Each of these forms of storage could fail, but from his perspective duplication increased the safety of the data, and thus through his routines of duplication he created a familiar process that enabled him to trust that data would probably not be lost. Another participant, Marc, similarly improvised his techniques based on a particular logic through which to understand how duplication or 'redundancy' on different types of platforms and technologies, would reduce the likelihood of his data becoming lost or inaccessible.

Duplication or redundancy of different forms also emerged in our Barcelona research. For instance, Laura worked as a freelancer, across arts and other events. Because she worked in the field of digital arts, she frequently used an iPhone4 and an iMac and worked with data archives and social media campaigns. She was concerned about losing her data and like other participants, had everyday routines for saving, copying and archiving data in hardware, which did not necessarily make the data 'safer' but meant they felt secure about the data in contexts of actual uncertainty and instability. Laura used complex saving routines based in her faith in the robustness of hardware. For example, she described how one organisation she worked for kept everything in Dropbox, so from each of the three years she worked on their project she had a folder. These folders, she explained, were kept in various places – on the hard drive in the organisation's office; in the Dropbox cloud; and on her own iMac – and they were synced from the iMac to an external drive (Time Machine). She was also asked to make a copy and store this on the organisation's server. She described the routines through which this was achieved:

> Laura: When I finish working I copy it all and that's it.
> Debora: Does it worry you if you finish work for the day and you haven't saved it on their server?
> Laura: No, I don't save it on their server. But yes I do always make sure that I copy it onto my own computer . . . if it's only in Dropbox I don't feel comfortable. . . . I have Dropbox installed on my computer but I feel that even there, it's as if it could fail, so I copy the contents to another place. I put it in a folder and I duplicate it. . . . normally I copy the whole folder and replace the previous one with it

The logic of these routines were driven by the participant's own convictions about what she believed was necessary for the data to be safe, her trust in the robustness of the hardware, and were designed to ensure that she personally did not feel anxious about its safety. As such, she did not follow the framework expected by the organisation, but instead relied on her own improvised routines of duplication. She was not concerned about the possibility of the external hard drive being stolen from her home, or if it could break. In fact, she did not even know if it was actually copying the data, since she had never checked to see what was on it. Yet by following the routines of duplication that she described she felt reassured that the data was safe enough. The use of daily or otherwise regular routines of saving and uploading data was a common way that participants in this and other projects (for instance in studies of self-tracking, Pink et al., 2017b).

There was also an emphasis on established process and routine in our other ethnographic sites, relating to collective and shared data. In the makerspace this was evident in the management of data produced within members' personal and collective projects. For instance, Dillon and Ahmed, the two founders and current managers, were making a video featuring their drone project, in order to participate in an accelerator programme. We arrived at the makerspace at about 7 p.m., on a Tuesday when as usual Dillon and Ahmed started to collect cash for a shared pizza order from those members who were staying for dinner. This was usually a relaxed point in the evening when members discussed what they had done and learned that day over a beer while waiting for the pizza delivery. However this Tuesday the atmosphere was different. A group of members were clustered around the corner of the long table, which was covered with cables, hardware, and tools, with their almost silent attention focused on one of three laptops. Ahmed was very tense, looking up from the desk he shared with Dillon, he was telling them 'I don't know what I did'. Turning to us he explained that he had been uploading the video to Alex's computer (Alex is a sound technician who was editing the video), but when he had simultaneously started to transfer the file to Vimeo, if had just disappeared. Almost before Ahmed finished speaking, Dillon began to outline how the process should be performed. First, he told us, he would have downloaded the video from the camera to Alex's computer and sent it by wire to his own computer, commenting that he would never use bluetooth for this procedure. Only on having completed these two steps would he then upload the video to Vimeo. While Dillon seemed to implicitly accuse Ahmed of losing the video because he had not followed the correct routine, at the same time Ahmed's know-how came into the discussion, since Alex answered from the crowded corner, pointing out that Ahmed was an engineer and suggesting there was probably 'something wrong with the software'. The group then moved over to the table and unsuccessfully tried to

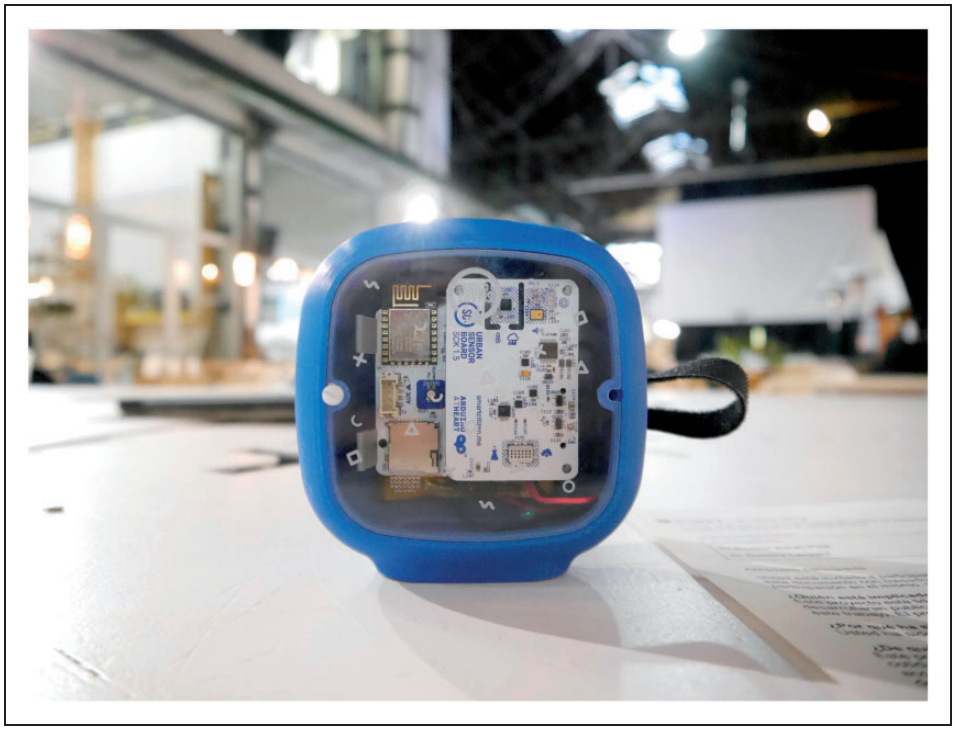

Figure 1. The smart citizen device is used in homes and workplaces.

unravel what had happened. The pizza arrived and after what was a silent and quite tense dinner, Dillon between sips of beer, and more relaxed reflected that 'The video was almost done' and that fortunately they had old versions of it in the editing software, on Alex's computer and on vimeo. Therefore, not only had they an established routine for ensuring the safety of data, but they also made the safety of the video files a collective concern, secured in part through sharing, which we reflect on further in the next section.

In effect, participants reduced their anxiety about possible loss by improvising to establish trusted routines to ensure that data is saved as soon as possible. Here trust is invested in the routine, or a sense of trust is gained through the familiarity of the routine.

Transparency and know-how

For many participants in our study data needed to be saved in proprietary ways, and its security was based in its not being visible to others or only being visible to selected others. However other participants felt that the safety of their data was increased through making it visible and, in turn, transparent. Particularly amongst technology designers, rather than saving data on a closed hard drive, it was felt that data would be safer on an open platform or sharing context. Thus anxieties about data loss were quelled through sharing. This is demonstrated through our research with Smart Citizen designers and users. Smart Citizen (Figures 1 and 2), located online here https://smartcitizen.me, consists of a platform, a kit and its user community which is necessary for it to be operational. It is defined on its web site: 'Smart Citizen is a platform to generate participatory processes of people in the cities. Connecting data, people and knowledge, the objective of the platform is to serve as a node for building productive and open indicators, and distributed tools, and thereafter the collective construction of the city for its own inhabitants'

The platform connects people, data and knowledge related to urban environments. It consists of open source software and hardware developed by and for the community, and which generates indicators about the quality of the air we breathe, the noise we produce and other environmental agents that surrounded us. Smart Citizen is constituted by the data that each of its users generates and shares within the community.[4]

For example Gerard, a tech designer explained that because the code and software used for the Smart Citizen platform is open and not proprietary, it is likely that the code would already have been shared or used elsewhere. Because people use their code to build their own platforms for using Smart Citizen sensors, they can manipulate the data themselves.

As one of the Directors of Smart Citizen in the Barcelona FabLab described,

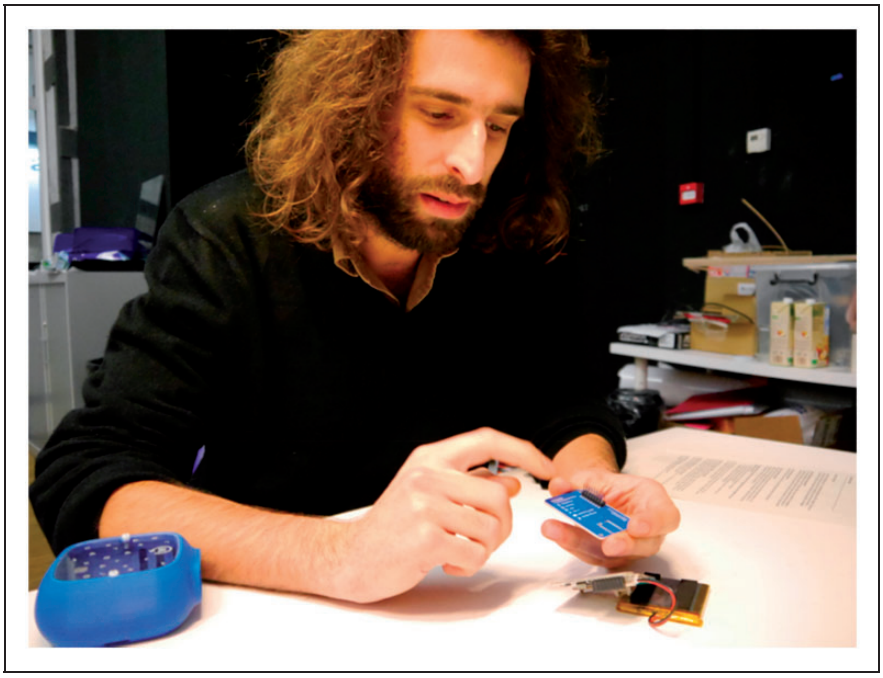

Figure 2. At the FabLab Barcelona.

> 'There are 2 things here, our platform is not distributed, we could do it, . . . it is happening with various technologies,. . . so if we close tomorrow, the data would be locked in there. The difference is that as there is a community around this who has developed the project, there would a process to make the data available'

He further explained that, 'The platform is opensource, so you could set it up again with other servers and could ask them for all the data and it could be reproduced'. Since the code for this platform is open, some users already publish their data on their own platforms that they develop (Maddox et al., 2016). For many of our tech designer participants, sharing data – and maintaining the know how to use it – was often a trusted means of keeping it safe. In this example we see trust invested in the routine process of sharing and creating transparency.

A second example emerged in our research with the Blockchain Centre in Melbourne (Figures 3 and 4). The centre's work is based in a context where the 'Bitcoin and Blockchain ecosystem' has recently rapidly grown in Australia, and 'has relied on industry participants educating customers and members of the public on the technology' and in response to what Bitcoin and Blockchain advocates see as 'a need for knowledge hubs, community centres and impartial not for profit advocacy groups and organisations' (http://blockchain-centre.com.au/).

We were interested in Blockchain and Bitcoin because they represent a form of value which is outside the 'system', as participants put it. We attended meet-ups in Melbourne's Blockchain centre and interviewed people involved in advocating for Blockchain, who had invested in it personally, were interested in it from a business perspective and for whom passion and advocacy for the technology spilled over between their personal and working/business life.

Participants at the Blockchain Centre told us that making your bitcoin wallet and transactions public was an advantage, since as one participant [name] described:

> 'No one can access it without a private key . . . but anybody can look in your account and in your wallet, all the wallets are online, you can go and check any wallet and see what's in it, you don't know who owns it, you can go and track that down if you want, bitcoin's pseudonymous it's not anonymous you can track down the owner of an account if you try hard enough, but that's the beauty of it, if I know the wallet . . . that you're using I can go and look at it and see how much is in there, I can't take any of it out . . .'

We asked him he felt Bitcoin made money safer because the transactions and amounts are transparent rather than hidden behind the walls of a bank. He responded by explaining, 'Because . . . you can go to a wallet, . . . and see when they were last moved and things like that, I think it does make it safer, if we all know

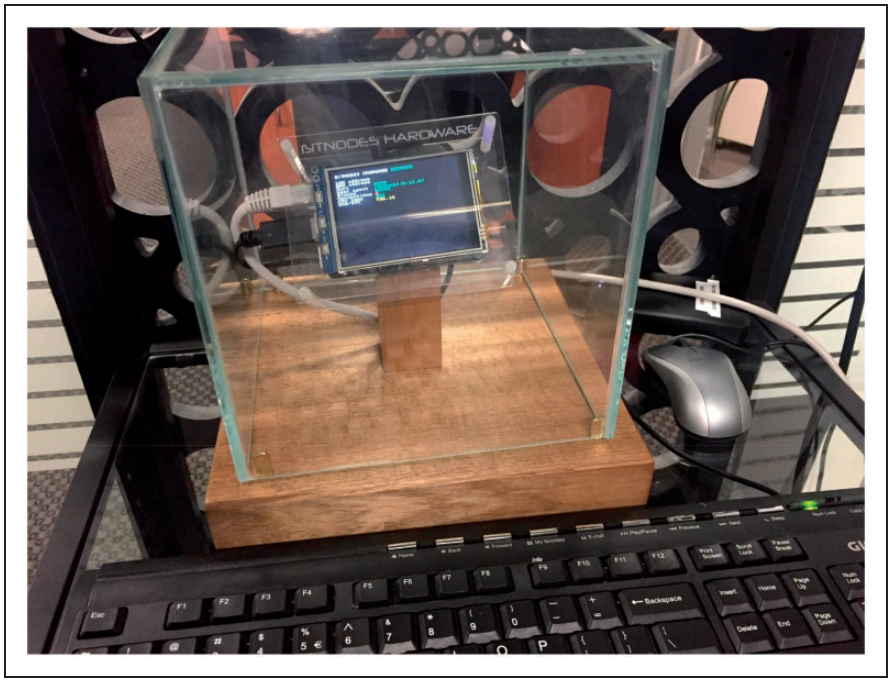

Figure 3. An exhibit from the history of Blockchain at the Blockchain centre in Melbourne.

Figure 4. Martin gives the research team a key blockchain email that he printed off for us.

what's going on it's harder to dupe people about what might have happened'

Yet, as Kelty (2014) and others have observed with respect to open access, making transactions and accounts transparent does not necessarily mean that Bitcoin and accessing digital data is accessible. As Martin, the manager of the Blockchain Centre Melbourne described, using Bitcoin is not simple, since, 'It is a hazard for people to use the system', and can be 'scary' to learn. The disadvantage of not

learning is that 'you have a custodian instead . . . then they have control over your bitcoins . . .'. To access and trade with bitcoins you must remember a complicated personal key and learn the know-how to use the technology. While bitcoin and Blockchain provide control and freedom, they entail a series of risks which require action so that their users can feel assured of their safety. If you lose your personal key you will lose the bitcoins forever. However, this in itself requires a routine series of safeguards. Martin told us that to be secure, bitcoins should be stored on something with a clean operating system, avoiding connected devices where they could be hacked. The documents that are evidence of Bitcoin should be printed on a printer with no memory so it cannot keep the information, and should be kept in a bank safe.

This know-how and the meticulous organisation that was required to be able to safely use Bitcoins is a stark contrast to how participants with less technological know-how coped with digital data. As Sam, a less tech savvy participant described:

> 'I would be really upset if I lost my Instagram because it's a kind of memory . . . another one I use is a bibliographic cataloguing platform and I am really scared about that . . . I have all my notes there, that would be really bad, . . . [if they commercialize it] or if they close down. I have lots of texts with lots of notes and I always think "I've got to copy everything", . . . but as there isn't a way to do it, and I'm too lazy to copy and paste it, and it's all so disorganized, now that I'm telling you about it I feel pressured about it.'

In contrast with the confidence that tech designers derived from keeping their data visible and transparent on platforms, less knowledgeable users had anxieties about saving digital materials on platforms, platforms closing, not having time or know-how to transfer data, or not having a system of organisation.

Trust and uncertainty: Navigating the temporalities of data

The presence of Big Data in our lives has been influential in recent thinking since it has invited us to re-think the temporalities of data. This has involved conceptualising data beyond the idea of an archive of un-altering or 'stopped' pieces of information that cut through the world, towards seeing data archives as dynamic, potentially 'real-time', moving and changing (mis)representations of everyday realities (Kitchin, 2014). As demonstrated in the previous section, the everyday digital data we are concerned with in this article is equally ongoingly produced and made. By this we do not simply mean that all individual files or data or other digital objects are continually modified by their users, but that the bodies of data to which they belong or with which they are archived are incrementally being modified, usually because they are being added to on a regular basis.

As we see through the examples of duplication and redundancy, digital data is part of ongoing everyday processes of work and leisure. This can be seen in other domains such as self-tracking (see Lupton, 2016, Pink and Fors, 2017a, 2017b; Pink et al., 2017b), where personal data is added to continually and automatically (with varying degrees of human intervention); everyday file making and archiving in contexts of digital labour or personal archiving whereby new files with particular content are made or modified and added to archives; data ongoingly produced by user communities and shared on online platforms; and other forms of data that are not necessarily being modified electronically as individual files are nevertheless changing, such as Bitcoin accounts which are always part of a wider ecology of other Bitcoin accounts, and can have changing market value even if the data itself is not changed.

The temporalities of data we focus on here are also bound up with what we call their 'digital materiality' (Pink et al., 2016) whereby the digital and material are part of the same thing, and continually emerging in new forms. The materiality of data has been emphasised by Dourish in his discussion of emulation (2016) and by STS researchers (Tanweer et al., 2016) with reference to both software and hardware (Star, 1999). This is significant since it is refers to how people constitute relationships between software and hardware as they improvise to make sense of data. As we showed in the discussion of tech design and Bitcoin, there are also patterns in how different logics of software-hardware and proprietary and nonproprietary relationships inform the ways people engage with data. These digital materialities are therefore not fixed in either software or hardware (Karanovic, 2012; Kelty, 2008), but rather in the ongoingly emergent relationship between the two as they become part of the same digital-material thing. The examples of duplication and redundancy can be seen as the digital-material manifestations of data anxieties.

A second element of the temporality of everyday data refers specifically to the temporality through which it is experienced by people. As we have noted already, anxiety is an anticipatory concept that has been associated specifically with Big Data by other researchers. However, we argue that everyday data also needs to be understood in relation to an anticipatory temporality, in that saving data indicates that data needs to exist in an as-yet-unknown but imagined future. As the above examples suggest, this future

might be quite immediate, for instance the next day when files or archives might be used, or it could be in the more distant future, such as in plans for using a bitcoin pension investment. Whatever the case, there is a sense that we need to save digital data specifically in relation to something that might happen next, and to understand this we return to the concept of trust.

While routines govern how people cope with digital data, it is also clear through our ethnographic material that data is something that is continuously produced and, and since it does not 'stop' or become fixed in any way, it needs to continually be coped with. It therefore needs to be understood in research as a processual element of the everyday. This ongoingness of data is also part of people's modes of everyday knowing about data, and way of sensing its presence. For some people everyday storage of data was partly a manual process. For instance whereby one participant intervened to save her folders a second time on her hard drive, while other aspects of this duplication process were automated and saved in Dropbox and on an external hard drive. In this sense, data and life are ongoing together and all are impacted by the contingent circumstances of the present. In these situations of automation people are not always fully conscious or aware of what is happening in relation to their data. For instance our participant did not know if her data was really being saved on the external drive because she had never checked, but she lived with this uncertainty because she invested trust in both the hardware itself and the routines she followed for saving the data. Another participant did not know how the value of his bitcoins would change but had invested trust in the process through which he had stored them, and had been pleased when they dramatically increased in value. The drone-making team did not know if they would lose their Drone's GPS data or not, but were not especially worried since they trusted that by repeating the process they could always recover enough of the flight path for the experience to be meaningful. The example of Bitcoin is worth reiterating and considering in relation to losing access as well as losing the asset. There is also an ambiguity and twist, since in this case loss for some means value for others: a Bitcoin is worth nothing unless you have a digital key to access and trade with it and a percentage of existing bitcoin keys have been lost for ever. While this is digital loss for individuals who lose their keys, it is not necessarily seen as negative by the wider bitcoin user-community since it means that the currency is strengthened because it reduces the number of bitcoins in circulation. In this case trust in the processes through which a key is kept safe is central to evade anxieties about losing data. As we have shown, here trust was produced through the familiar technologies of pen and paper documentation.

Therefore, what happens with data as it becomes embedded in and produced through everyday life activities, and somehow familiarised and domesticated into the everyday through routines that manage it (even if not in the most efficient ways as they would be defined by information technology experts), is contingent and often involves improvisatory responses. If this necessitates 'the recognition that our futures are contingent because our present is as well' (Bessire and Bond, 2014: 450), then we can assume that our data futures are just as likely as the present circumstances described by our participants, to be messy, throw up surprises for us, and thus be just as uncertain. Living with data involves a temporality that is known through the ongoing sense of uncertainty about future accessibility, presence and use of data. Routines such as creating redundancy or engaging in transparency and maintaining the skills, or know-how, to navigate complex technological systems in our everyday lives are ways of creating processes in which to trust and to reduce the anxiety associated with uncertainty. By trusting in familiar routine, participants were able to 'feel alright' as they lived with the uncertainty of data.

Data futures are imagined rather than predictable and to understand them we need to acknowledge what Irving refers to as 'the radical contingency of the future, including futures that we do not and will never know about' (Irving, 2017: 39). It is this contingency and uncertainty about what will happen next that informed the experiences and imaginaries of our research participants, which were riddled with stories, expectations and anxieties that data could be lost, stolen or otherwise disappear or be compromised. Moreover, there have been no design solutions that make data completely secure. Instead our ethnography showed how participants in our research engaged with new technological possibilities in improvisatory ways to enable themselves to feel comfortable *enough* to trust in the continued accessibility and safety of their data. Yet as we have also shown, depending on their technological know-how or lack of it people pursue different logics and ways of making themselves feel comfortable about their data, investing their trust in hardware, software, and in the familiar feel of the routines through which they use various devices, platforms and apps.

Conclusion

We have been concerned in this article with not just the anxieties that surround everyday data, but how these are experienced and articulated, what measures, trade-offs, and tricks people undertake to cope with or disperse anxieties, and how they are subsequently able to trust that their data will be sufficiently safe. In doing so we have advanced a processual theory of trust that

maps out how people cope with the inevitable uncertainty and contingency of the emergent circumstances of everyday life. We have proposed that humans cope with uncertainty by building familiar routines of activity. It is these circumstances that create situations in which they can trust, and as such are able to evade feelings of anxiety about what will happen next and have sufficient confident to improvise to fill in the gaps as they move forward. Our findings regarding how people feel about their data and the technologies they use, and how trust is part of this configuration, demonstrate how this works in practice and as such establishes the theory of how people live with data that we proposed at the beginning of this article.

This has implications for how we understand what is of value to people in their dealings with data, because it highlights what people need to do or have in order to feel comfortable living out their everyday lives with data. Importantly, our findings show that the HCI endeavour to understand human trust in technologies or interfaces is not sufficient, and can be usefully expanded through a design anthropological theory that locates trust as a constitutive part of the circumstances that configure to generate the human confidence needed to improvise. This focus on existing everyday life engagements with data, moreover implies how we might start to think differently about datafied futures. This is because, if we can understand how people are already finding ways to live comfortably with digital data and the uncertainties that are associated with it, then this has implications for how we might design appropriate ways to live with data in the future. Knowing how people manage their lives with data in the present, helps us to consider how the possibilities presented by smart home, smart city and other technological visions might actually play out in a world that social science research has shown clearly is characterised by digital 'mess' (Dourish and Bell, 2011) and will not approximate anything like that advanced by smooth visions of technological innovation accompanied by predictable social change.

To consider futures we also need to attend to the specificities of locality. All of our research sites had a combination of local and international participants, and considered themselves active members of international communities of technology designers. Many of our participants spent time in online design communities, shared code and strategies with other members of these communities and were influenced and inspired by Bitcoin, Blockchain and maker movements around the world (Blomberg and Karasti, 2013; Nardi, 2007). In that sense they were as much part of these online technology communities as they were their local communities in Barcelona and Melbourne. However, a comparative perspective is also useful in showing up why global situatedness can matter. In Barcelona our fieldsite was focused in the FabLab where many organisations are based, but in Melbourne such groups are dispersed across the city. The two sites were also differently supported and/or impacted by national and regional (e.g. European) funding structures and opportunities. For example, in Barcelona the initiatives we researched tended to be publicly funded whereas in Melbourne there was a higher degree of private investment; and Barcelona was generally seen as more central to the global technology innovation scene than Melbourne which had a sense of being more peripheral despite its reputation as a global centre of design. As a result, Barcelona participants had a stronger sense of confidence with reference to the safety of their data, in part because they felt confident in their knowhow and in part because they lived with their data in ways that blurred the distinctions between personal and work lives. In contrast Melbourne participants were more concerned with maintaining data privacy and often kept a clearer division between their professional and private lives. But at the day-to-day level, much of what we observed at various meetings and in the workplace looked very similar and many of the attitudes and aspirations towards the promise of their activities revealed what Tom Boellstorff (2012) describes as the politics of similitude rather than national cultural disjuncture.

As we have shown, we live in a world where people do not usually feel sure that their data is secure, could not be lost, stolen or somehow compromised. That is, living with data means living in a world of uncertainty, where this vulnerability is taken for granted, and the best that can be done is to devise a way of living with data that pushes aside anxieties and feels 'alright'. What feels alright for different individuals varies and there is no single template, logic or set of principles that is universally followed. Often people are chaotic and idiosyncratic in the ways they make, accumulate, look after, or fail to look after digital data. Thus, data do not tend to be organised by people in discrete and complete ways that are coherent with the understandings that software designers have of computer systems, and do not necessarily fit with processes of audit and governance. Moreover, as is well established in critical data studies (Baym, 2013; boyd and Crawford, 2012; Markham, 2013; Nafus, 2014), data is not an entity with objective meanings that can be stolen. Rather it is contingent, in its meanings and in the ways that it is organised. In this sense, when we take as our example the kinds of data that ordinary people store on their personal and work computers, such materials cannot really exist as a solid target for a cyber attack, indeed it difficult for such a dispersed target to be attacked at all. Instead, we can better understand cyber attacks not

as attacking data but as targeting the services and systems that exist for storing and accessing data. It is these means for keeping and accessing data that give data its value because they enable us to use it. However, massive scale cyber attacks are not the only, or the primary, threats to our access to and the security of data. In this article we have started to investigate the question of how people live with data and create their own ways of experiencing it as relatively secure. This, we argue is important to know, since without an understanding of how people actually use, improvise with and feel about everyday mundane data, and what they already do to create the circumstances in which they can trust that it is 'safe enough' we will not have the background understandings that are needed for us to design for possible better data futures.

Acknowledgements

We are grateful to all the people who gave their time and interest to participate with us in this project and to our anonymous non-academic Industry partners for the inspiring conversations we shared.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The research discussed in this article was funded by an industry partner.

Notes

1. http://worldpopulationreview.com/world-cities/barcelona-population/, accessed 1 November 2017.
2. http://www.population.net.au/melbourne-population/, accessed 1 November 2017.
3. Introductions to these technologies provided by the Blockchain Centre are available online here: http://blockchaincentre.com.au/blockchain-research/, accessed 5 November 2017.
4. The Smart Citizen ethnography was undertaken in Barcelona (we could not find active Smart Citizen users in Melbourne).

References

Adams V, Murphy M and Clarke AE (2009) Anticipation: Technoscience, life, affect, temporality. *Subjectivity* 28: 246–265.

Anderson B (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34(6): 777–798.

Barassi V (2017) BabyVeillance? Expecting Parents, Online Surveillance and the Cultural Specificity of Pregnancy Apps. *Social Media + Society* 3(2): 1–10.

Baym N (2013) Data not seen: The uses and shortcomings of social media metrics. *First Monday* 18(10). Available online at http://firstmonday.org/article/view/4873/3752. DOI: 10.5210/fm.v18i10.4873 (accessed 25 January 2018).

Bessire L and Bond D (2014) Ontological anthropology and the deferral of critique. *American Ethnologist* 41(3): 440–456.

Blomberg J and Karasti H (2013) Reflections on 25 years of ethnography in CSCW. *Human Computer Supported Cooperative Work* 22: 373.

Boellstorff T (2012) The politics of similitude: Global sexuality activism, ethnography, and the Western subject. *Transcriptions* 2: 22–39.

boyd D and Crawford K (2012) Critical questions for Big Data. *Information, Communication & Society* 15(5): 662–679.

Chan J and Bennett Moses L (2017) Making sense of Big Data for security. *British Journal of Criminology* 57(2): 299–319.

Crawford K (2016) The anxieties of Big Data. *The New Inquiry*. Available at: https://thenewinquiry.com/the-anxieties-of-big-data/ (accessed 20 December 2017).

Cukier and Mayer-Schoenberger (2013) The rise of Big Data how it's changing the way we think about the world. *Foreign Affairs*.

Dencik L, Hintz A and Carey Z (2017) Prediction, preemption and limits to dissent: Social media and big data uses for policing protests in the UK. *New Media & Society*. Epub ahead of print 2017. http://dx.doi.org/10.1177/1461444817697722.

Dourish P (2016) Rematerializing the platform: Emulation and the digital-material. In: Pink S, Ardevol E and Lanzeni D (eds) *Digital Materialities*. London: Bloomsbury, pp. 29–44.

Dourish P and Bell G (2011) *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing*. Cambridge, MA: MIT Press.

Fredricksen M (2016) Divided uncertainty: A phenomenology of trust, risk and confidence. In: Jagd S and Fuglsang L (eds) *Trust, Organisations and Social Interaction*. Cheltenham: Edward Elgar Publishers.

Giddens A (1991) *Modernity and Self Identity*. Cambridge: Polity Press.

Gunn W and Clausen C (2013) Conceptions of innovation and practice: Designing indoor climate. In: *Design Anthropology: Theory and Practice*. London: Bloomsbury Academic, pp. 159–179.

Harper RHR (2014) *Trust, Computing and Society*. Cambridge: Cambridge University Press.

Ingold T and Hallam E (2007) Creativity and cultural improvisation: An introduction. In: Hallam E and Ingold T (eds) *Creativity and Cultural Improvisation*. Oxford: Berg.

Irving A (2017) The art of turning left and right. In: Salazar J, Pink S, Irving A, et al. (eds) *Anthropologies and Futures*. London: Bloomsbury.

Karanovic J (2012) Free software and the politics of sharing. In: Horst H and Miller D (eds) *Digital Anthropology*. Oxford: Berg Publishers.

Kelty CM (2008) *Two Bits: The Cultural Significance of Free Software*. Durham, NC: Duke University Press.

Kelty C (2014) Beyond copyright and technology: What open access can tell us about precarity, authority, innovation, and automation in the university today. *Cultural Anthropology* 29(2): 203–215.

Kitchin R (2014) *The Data Revolution*. London: Sage.

Lupton D (2016) *The Quantified Self: A Sociology of Self-Tracking*. Cambridge: Polity.

Maddox A, Singh S, Horst H, et al. (2016) An ethnography of bitcoin: Towards a future research agenda. *Australian Journal of Telecommunications and the Digital Economy* 4(1-1). Available at: http://ajtde.telsoc.org/index.php/ajtde/article/view/49. DOI: 10.18080/ajtde.v4n1.49.

Markham A (2013) Undermining 'data': A critical examination of a core term in scientific inquiry. *First Monday* 18(10). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/4868.

Millington B and Millington R (2015) 'The datafication of everything': Toward a sociology of sport and Big Data. *Sociology of Sport Journal* 32: 140–160.

Nafus D (2014) Stuck data, dead data, and disloyal data: The stops and starts in making numbers into social practices. *Distinktion: Scandinavian Journal of Social Theory* 15: 208–222.

Nardi B (2007) Placeless organizations: Collaborating for transformation. *Mind, Culture, and Activity* 14(1–2): 5–22.

Pedersen EO and Liisberg S (2015) Introduction: Trust and hope. In: Pedersen EO and Liisberg S (eds) *Anthropology and Philosophy: Dialogues on Trust and Hope*. Oxford: Berghan.

Pink S (2013) *Doing Visual Ethnography*, 3rd ed. London: Sage.

Pink S (2015) *Doing Sensory Ethnography*, 2nd ed. London: Sage.

Pink S (2017) Ethics in a changing world: Embracing uncertainty, understanding futures, and making responsible interventions. In: Pink S, Fors V, O'Dell T, et al. (eds) *Working in the Between: Theoretical Scholarship and Applied Practice*. Oxford: Berghahn.

Pink S, Ardevol E and Lanzeni D (2016) Digital materiality: Configuring a field of anthropology/design? In: Pink S, Ardevol E and Lanzeni D (eds) *Digital Materialities: Anthropology and Design*. Oxford: Bloomsbury.

Pink S, Dainty A and Morgan J (2017a) Making theory, making interventions: Doing applied scholarship at the in between. In: Fors V, O'Dell T and Pink S (eds) *Theoretical Scholarship and Applied Practice*. Oxford: Berghahn.

Pink S, Sumartojo S, Lupton D, et al. (2017b) Mundane data: The routines, contingencies and accomplishments of digital living. *Big Data and Society* 4(1). Available at: http://journals.sagepub.com/doi/abs/10.1177/2053951717700924.

Pink S and Fors V (2017a) Being in a mediated world: Self-tracking and the mind-body-environment. *Cultural Geographies* 24(3): 375–388.

Pink S and Fors V (2017b) Self-tracking and mobile media: New digital materialities. *Mobile Media and Communication*. 5(3): 219–238. https://doi.org/10.1177/2050157917695578.

Pink S and Salazar JF (2017) Anthropology and futures: Setting the agenda. In: Salazar J, Pink S, Irving A, et al. (eds) Anthropologies and Futures. London: Bloomsbury.

Ruckenstein M (2016) Keeping data alive: Talking DTC genetic testing. *Information, Communication and Society*. 20(7): 1024–1039. http://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1203975.

Ruckenstein M and Dow Schüll N (2017) The datafication of health. *Annual Review of Anthropology* 46: 1.

Smith GJD and O'Malley P (2017) Driving politics: Data-driven governance and resistance. *British Journal of Criminology* 57(2): 275–298.

Smith RC and Otto T (2016) Cultures of the future: Emergence and intervention in design anthropology. In: Smith RC, Vangkilde KT, Kjærsgaard MG, et al. (eds) *Design Anthropological Futures*. London: Bloomsbury Academic, pp. 19–36.

Star SL (1999) The ethnography of infrastructure. *American Behavioral Scientist* 43(3): 377–391.

Sumartojo S, Pink S, Lupton D, et al. (2016) The affective intensities of datafied space. *Emotion, Space and Society* 21: 33–40.

Tanweer A, Fiore-Gartland B and Aragon C (2016) Impediment to insight to innovation: Understanding data assemblages through the breakdown–repair process. *Information, Communication & Society* 19(6): 736–752.