Check for updates

Original Research Article

BIG DATA & SOCIETY

Big Data & Society
July–December: 1–13
© The Author(s) 2023
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20539517231213827
journals.sagepub.com/home/bds
Sage

Everyday digital traces

Andrea Armstrong[1], Jo Briggs[2], Wendy Moncur[3], Daniel Paul Carey[4], Emma Nicol[3] and Burkhard Schafer[5]

Abstract

Our research responds to calls for more engagement with everyday personal data. We used a co-designed, fictional persona called *Alex Smith* to concretise and represent people's online information to help participants (through role-playing) reflect on data and digital traces. Drawing together four fields of scholarly research concerning personal data: digital traces and the digital self, datafication and dataveillance, mundane, everyday data and the data journey – our aim was to advance understandings of personal data by exploring ordinary people's seemingly innocuous digital traces generated through everyday online interactions. Our paper presents three key findings from our analysis: (1) how ordinary people cope with and manage everyday data; (2) the haunting effects and affects of peer-to-peer surveillance and (3) postdigital identities. We argue that greater attention needs to be paid to everyday digital traces – how they are understood, managed and revealed because this has implications for ordinary people, corporate entities and governments. We contribute to a gap in critical data studies literature that calls for further investigations into ordinary people's engagement with data. We also offer a method that can be adapted for and used with different participant groups, which also supports their awareness of cumulative functions of personal data and potential use by un/known actors.

Keywords

Digital traces, peer-to-peer surveillance, data self, datafication, online harms, creative security, data journeys

Introduction

Given the ubiquity of digital traces there have been calls for more research into everyday engagements with personal data (Couldry and Powell, 2014; Kennedy, 2018; Pink et al., 2017; Ruckenstein and Pantzar, 2015). Our research responds to this call. In doing so, we draw together four fields of enquiry in scholarly research: (1) digital traces and the digital self; (2) datafication and dataveillance; (3) mundane data and (4) the data journey.

Our aim is to advance understandings of people's perceptions of their everyday or mundane personal data (Pink et al., 2017), focusing on users' seemingly innocuous digital traces generated through everyday online interactions. These interactions include intentional information sharing, information shared by others, and associated automated application functions, such as social media metadata that exposes a user's location when they post an update. One's digital traces are continually added to and, as such, comprise data that are 'lively' in their dynamic potential for generating new meanings, including through new associations with existing data (Lupton, 2016), even after death. Data's liveliness can confront people with "information about themselves that is not only continually generated but is also used by other actors and agencies in ways of which they may not be fully aware" (Lupton, 2016: 2), for example, live-location sharing information on Instagram can be viewed by anyone exploring the app's maps, not just the account holder's followers (Jones, 2018). Without ongoing care, individual pieces of digital information can be combined or identified by or linked to other information out in the world to reveal unanticipated insights to others, including hostile actors who leverage joined-up information to gain advantage over individuals or their associated others, for example, their employer.

We draw on key findings from a study based on a creative method we designed, which aimed to help to

[1]Silent Spring Consultants, Middlesbrough, UK
[2]Northumbria University, School of Design, Newcastle upon Tyne, UK
[3]Computer and Information Sciences, University of Strathclyde, Glasgow, UK
[4]Independent Researcher, Newcastle upon Tyne, UK
[5]University of Edinburgh, School of Law, Edinburgh, UK

Corresponding author:
Jo Briggs, Northumbria University, School of Design, Newcastle upon Tyne, UK, NE1 8ST.
Email: jobriggs@hotmail.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

concretise and represent people's online information when their understanding of their digital traces was incomplete at best, and at worst fuzzy. The key question for the research team was – how can we help people imagine and reflect on their holistic digital traces rather than individual pieces of information? To do this, we created digital traces from a 'day in the life' of the fictional Alex Smith, intended as a gender-neutral persona constructed by participants from information posted online by or about Alex. We trialled this method with nine individuals recruited from a previous interview study (Nicol et al., 2022), inviting them to enact one of two roles: Alex's new employer or an insurance agent opportunistically selling nonspecific policies. Our contribution comprises knowledge of ordinary people's imaginings of their everyday digital traces and presents three key findings from our analysis of the literature and our study: (1) how, and to what extent, people cope with and manage everyday data; (2) the haunting effects and affects of peer-to-peer surveillance and (3) post-digital identities. Our main argument is that greater attention needs to be paid to everyday digital traces – how they are understood, managed and revealed – as this has implications for individual citizens, data studies research, corporate entities and governments. Furthermore, our research demonstrates and shares our method and insights on how such approaches can render more imaginable and manageable the complexity of personal data and digital traces (Lupton and Watson, 2021). We sufficiently describe the method to enable reproduction or customisation for use with other groups.

Conceptualising everyday digital traces: A review of the literature

To understand everyday digital traces, our analysis is guided by four areas of inquiry: (1) digital traces and the digital self; (2) datafication and dataveillance; (3) mundane data and (4) the data journey.

Digital traces and digital self[1]

There is little disagreement in the literature about what constitutes a digital trace, and there is widespread agreement that it would be difficult not to leave traces (Ertzscheid, 2009; Flyverbom and Murray, 2018; Reigeluth, 2014). Digital traces are banal fragments of a person's past activities or interactions left behind deliberately or unintentionally and these traces combine to form a digital self (Reigeluth, 2014). They can arise from written, audio or video documents, logins, online purchases, or browsing sessions (Ertzscheid, 2009). Social media "likes", "shares" and comments on others' posts add further nuance, working as 'stand-ins for people' (Agre, 1994: 104). Traces also arise as 'side effects of our media-related activities, for example, via cookies, apps and trackers' (Breiter and Hepp, 2018: 387). In the French philosophical tradition, the digital self is framed as an assemblage of traces, which are automatically and ubiquitously produced (Deleuze, 1990; Foucault, 2001). Digital traces are fragile since they do not exist on their own and are always the result of processes of compilation, selection, interpretation and inferences that are drawn based on incomplete information (Laflaquière, 2009). Tracing systems can determine the user's habits on digital technologies, including traces that are problematic, effective, nonpertinent or redundant (Laflaquière, 2009). In other words, all use is left as a trace.

Digital traces enable impression management of a digital self in the permanent "front stage" of the digital sphere, where users present and represent themselves, contributing to self-expression, self-perception and self-representation (Goffman, 1959). They also contribute to the discrepancies between what users *give* (share and show) in explicit displays of friends, interests and online representation, and what they *give off* that can be interpreted by others and amplified in networked publics[2] (boyd, 2008). Users are prompted to share private and ordinary aspects of their life online that have traditionally been hidden from the public gaze (Milan, 2018). These explicit displays are key to developing relationships, acquiring social status and building trust in online environments. Users may well share information even when they care deeply about online privacy (boyd, 2010). Management of this presentation of the digital self can involve 'selecting, filtering, and redistribution of relevant content' (Milan, 2018: 519).

Regardless of what is *given* and *given off* online about an individual, digital traces offer a skewed and incomplete picture of the individual's personality, values and routines (Wolf et al., 2018). Such traces fail to "fully capture the … vibrancy, fluidity and spontaneity of human experience and behaviour" (Lupton, 2020: 1). Their incompleteness can invite inferences (Lupton and Watson, 2021: 4) that are generated from 'fragments of past interactions or activities [… that] when correlated together, allow a pre-emption and prediction of future behaviors' (Reigeluth, 2014: 250).

Even if the picture is skewed, individuals' efforts to curate their digital self may be insufficient to prevent revealing more than intended. Digital traces are leaky, liquid and hard to control (Bauman and Lyon, 2013). Tracking technologies make online activities legible, with implications for privacy, anonymity, informational autonomy and self-determination (Smith, 2018). Users may not realise how their connected traces can be explored by others as a more coherent whole, with insights into their apparently private self (e.g. behaviour, values, habits, etc.) potentially used against them (Nicol et al., 2022).

Datafication and dataveillance

We see above the relationship between the digital self and digital traces but to understand digital traces as part of

everyday social processes that are open to others' gaze we also draw on datafication and dataveillance literature. The ubiquity of digital technologies and processes of 'datafication' shape many parts of our everyday lives (Büchi et al., 2022; Hansen and Flyverbom, 2015; Mayer-Schönberger and Cukier, 2013; van Dijck, 2014).

As Henman (2022: 535) argues, 'digital technologies automatically collect, collate, combine and circulate digital traces of our actions and thoughts, which are used to construct digital personas of us'. This means our physical body is echoed by an increasingly comprehensive 'shadow data body' (see Blackman, 2019). This type of digital surveillance inspired the term *dataveillance* (Clarke, 1988; Buchi et al., 2022; Lupton, 2021; Lupton and Michael, 2017; Smith, 2016). Our data body, however, does more than follow us: it also precedes us. Before we arrive somewhere, we have already been measured and classified (Stalder, 2002). Even after physical death, our data body may continue to grow, reflecting the asynchronous nature of physical and digital lives (Pitsillides et al., 2013) and ongoing risk of harm to the deceased or their relations (Schafer et al., 2023). This means that there are spatial and temporal aspects to the data (Shorey and Howard, 2016) being produced, stored, classified, circulated and re-presented.

The human body also has a central role in *dataveillance* practices, acting as both a producer and recipient of data (Smith, 2016). Digital traces are voluntarily or involuntarily emitted as the body interfaces with networked sensor technologies – for example, security scanners in the airport terminal or physical movements detected by a wearable Fitbit wristband. Smith (2016) understands these digital traces as a *disembodied exhaust* which in turn gives rise to a *data proxy* – an abstracted figure created from the amalgamation of data traces. The *data proxy* paints 'an intimate portrait of a person's habits and situation, a networked impression of self that performatively intercedes social relations and identities' (Smith, 2016: 110). Such proxies increasingly mediate and animate social behaviours and relations in online and offline contexts.

While data are all of the above and more, they are also conspicuous in their absence – a lack of data is another indication of power: the power not to look or to remain hidden (Brunton and Nissenbaum, 2015; Flyverbom, 2016). Data are always active and never neutral in their presence and absence, part of an information geography (Graham and McFarlane, 2014) that is always in flux. With the immense quantities and varieties of data in circulation that attest to the social lives and practices of ourselves, some seek legal recourse to remove compromising details – or 'machinic ghosts' (Smith 2016: 214) – from corporate search engines.

Mundane data

To deepen our understanding of everyday digital traces we must also consider the concept of mundanity and online life (Williams and Waskul, 2007). Often the terms mundanity and everyday are used interchangeably; for example, social media mirroring what is mundane or every day (Ozduzen and Korkut, 2020); spatial Big Data and everyday life (Leszczynski and Crampton, 2016) and the digital mundane as the 'ordinary and taken-for-granted digital objects, practices, productions, and sites that significantly both mediate and are mediated by everyday lives and spatialities' (Leszczynski, 2020: 1194).

Most relevant for our research however, is the work by Pink et al. (2017, 2018) and Lupton (2016). Pink et al. (2017) developed the concept of mundane data as an analytical entry point for understanding Big Data. In doing so, they drew on the work of cultural and media studies scholars who emphasised how digital and mobile technologies have rapidly become part of mundane, everyday life and what was once strange or alien is now familiar (Baym, 2015; Hartmann, 2013; Pink et al., 2017). Familiarity though tends to co-exist with uncertainties and anxieties about the unruliness of everyday data, which has led to considerations of what it feels like to live with the messiness of data (Burgess et al., 2022; Pink et al., 2018). Deborah Lupton (2016) developed the concepts of visceral data and lively data, which respectively acknowledge how data are felt and experienced and how they are relational to other things. These conceptualisations help us understand digital traces in two ways: from the perspective of the user whose digital use and hence traces are now situated in everyday life; and how digital traces can be felt and experienced in positive and harmful ways and that digital use and traces are relational to the "real" world.

Data journeys

To help us develop our methodological approach and understand everyday digital traces and the Alex Smith method, the substantial contributions to participatory data research are helpful, particularly the work on 'data journeys' (Bates et al., 2016; Prieto-Alvarez et al., 2018). The theoretical developments discussed by Bates et al. (2016: 3) to develop their data journeys approach helps to understand and 'illuminate the socio-material life of data'. Bates et al. (2016) distinguish between two interrelated aspects of the data journey – the life of data and the materiality of data. The life of data draws on the work of Massey (1994) and Borgman (2015) to imagine a research design in which the researcher moves through space following data on their journey through interrelated sites of data practice (Bates et al., 2016). Our Alex Smith Study (see more in Methodology section) enabled the participant to follow the data journey (in one day) of a fictional persona (Alex Smith) and examine the sites of their data practice.

The materiality of data is also helpful in understanding our approach because we are interested in the material consequences of data, and the way data has significance in the

world as a digital trace. The Alex Smith method was our way of illuminating the 'material factors that cause data to have consequences' (Bates et al., 2016: 3), focusing on small pieces of apparently harmless separate information that can be viewed online and connected by other actors, beyond the intended recipient.

Towards understanding everyday digital traces

In summary, this article draws together literature on the digital self, dataveillance, mundane data and data journeys to develop our conceptualisation of everyday digital traces. Conceptually, we argue that rather than being focused on corporate harvesting of personal data as raw material that powers an industry of largely unseen and unknowable surveillance (e.g. Zuboff, 2015), our research is concerned with ordinary people's practices of intentional, day-to-day sharing of apparently innocuous personal information and off-the-cuff digital communication. These practices contribute to data surveillance systems, in this case involving peer investigation and monitoring. The surveilling power here comprises dataveillance (van Dijck, 2014) in a disintermediated system – that of the Synopticon – where surveilled and surveillor are subject to each other's gaze (Mathieson, 1997). Without ongoing care, digital traces can be combined to reveal insights to others, including hostile actors who make use of joined-up information to gain advantage, over individuals or their associated others, for example, their employer. The emergence of the digital self – a sort of 'data double' (Haggerty and Ericson, 2000: 611) that mirrors, resembles, and reflects, but especially interacts with the subject that originates it (Ruckenstein, 2014) is now part of how we live every day with data and our digital traces.

Methodologically, our persona-based method is situated in and contributes to existing participatory data research that focuses on everyday data practices, cultures and experiences (Albury et al., 2021; Burgess, 2017; Lupton and Michael, 2017; Michael, 2006). We demonstrate an approach of relevance to current discussions on post-qualitative creative methodologies in human-centred privacy and security (see Coles-Kemp, 2018) and contribute to the vibrant body of work emerging on the pertinence and applicability of co-creative, participatory and sensory methods to understanding experiential dimensions of personal digital information and data (e.g. Kennedy, 2018; Lupton and Watson, 2021). Few studies combine innovative arts and design-based methods with participatory or ethnographic methods even though, as Lupton and Watson (2021) argue, they generate intriguing insights into people's relationships with their personal data. Existing examples include the study by Lupton and Michael (2017) who used cultural probes (objects or tasks, designed to be playful and encourage people to think in new ways) to elicit people's understandings of data generated by or about themselves. In conclusion, they state that their project had 'only just scraped the surface' and that future research needs to delve into other aspects of these lively digital data assemblages (Lupton and Michael, 2017: 267). Kennedy (2018: 19) identifies the everyday as a critical absence in the field of data studies and suggests two approaches to researching living with data. The first, is a phenomenology of datafied agency which 'mobilises a phenomenological excavation of data experiences to explore the possibility of agency in datafied conditions' (Kennedy, 2018: 27). The second is a data-related capabilities approach to understand emotional dimensions that 'highlights the importance of identifying what people need to be capable of doing in order to live well in times of datafication' (Kennedy, 2018: 27).

Our research contributes to this body of work. Like Lupton and Watson's (2021) Living with Personal Data project, Bates et al.'s (2016) Life of Data project and Kennedy's (2018) research focusing on the datafication of working life, we are concerned with both developing the research field and its methodological approaches.

In the next section, we outline the Alex Smith Study and how this helped us gain insights into everyday digital traces.

Methodology – The Alex Smith study

Our objective in designing the method and carrying out the study was to gain insights into people's awareness of cumulative risk exposure *within* their 'everyday' online information-sharing practices, and *across* their personal and working lives. In doing so, we built on from research using Data Narrative Inquiry (Vertesi et al., 2016; Nicol et al., 2022). Outcomes from an earlier interview study involving 26 participants aged between 20 and 59 years who were active online and in full-time employment revealed that participants conceptualised their online practices in discrete idiographic form rather than as connected. Subsequently they adopted incomplete risk models when assessing the potential for harm, considering only individual pieces of shared information rather than accounting for their sum (Schafer et al., 2022). Many found it challenging to envision future scenarios where a hostile actor could use their combined information against them. Several described their online selves as 'boring', seemingly rationalising that their online information was of no interest or value to others. Because these previous efforts using interview techniques failed to elicit deeply nuanced responses, we developed the Alex Smith method.

The study

Rather than asking participants to focus on their own digital traces (due to reasons cited above in addition to ethical challenges of acquiring consent[3]), we proposed a fictional character, *Alex Smith* (with a deliberately gender-ambiguous

name), as a prompt for reflection and discussion. Rather than flesh out the characterisation of Alex Smith we fabricated just their digital trace information, as if shared online, by or about them over one day. This comprised five themed groups of online information presented as sets of digital cards:

- Alex's posts on social media;
- Information relating to Alex posted by others on social media;
- Alex's "background information" made available often publicly, for example, on the Companies House register of UK businesses;
- Locations tracking, for example, Strava;
- Alex's bio-metric information (as this has increasing potential to reach the public domain, e.g. voice recordings).

We invited participants from the earlier study to participate: 9 of 26 responded and agreed to take part. They ranged in age between 20 and 54 years; 3 identified as male, 5 female, 1 non-binary. All were active online and in full-time employment in the UK at the time. Due to the physical distancing requirements of Lockdown, individual sessions took place over Zoom video conferencing platform and Mural, a collaborative whiteboard app, to facilitate use of the card sets. Participants were offered a £20 supermarket voucher for participation in the study. Pre-engagement involved emailing information to acquire necessary consent. The Alex Smith Study took place between 20 October and 4 December 2020.

The Alex Smith method involved the research facilitator inviting the participants to first select and interpret information about Alex, and then to narrate and co-create Alex Smith's digital persona in discussion with the researcher. The researcher explained the scenario and outlined two roles from which to select:

(I) Employer (participants reviewing the traces of Alex as a prospective employer);
(II) An insurer from an insurance company, assessing Alex for non-specific policy cover.

Each session was designed to last 45 to 60 minutes, sufficient time for participants to explore at least 3 sets of the cards (see Figure 1), concluding when it was approaching 60 minutes and at a convenient juncture between card sets. Table 1 provides an overview of the participants, their role choice (employer or insurance) and the order of cards selected. This shows that seven of the nine participants chose the employer role and only two the insurance company. Seven participants chose the social media posts first, one the bio-metric data and one the posts by others about Alex. One participant only had time to choose and discuss two card sets, whereas another participant was able to choose four.

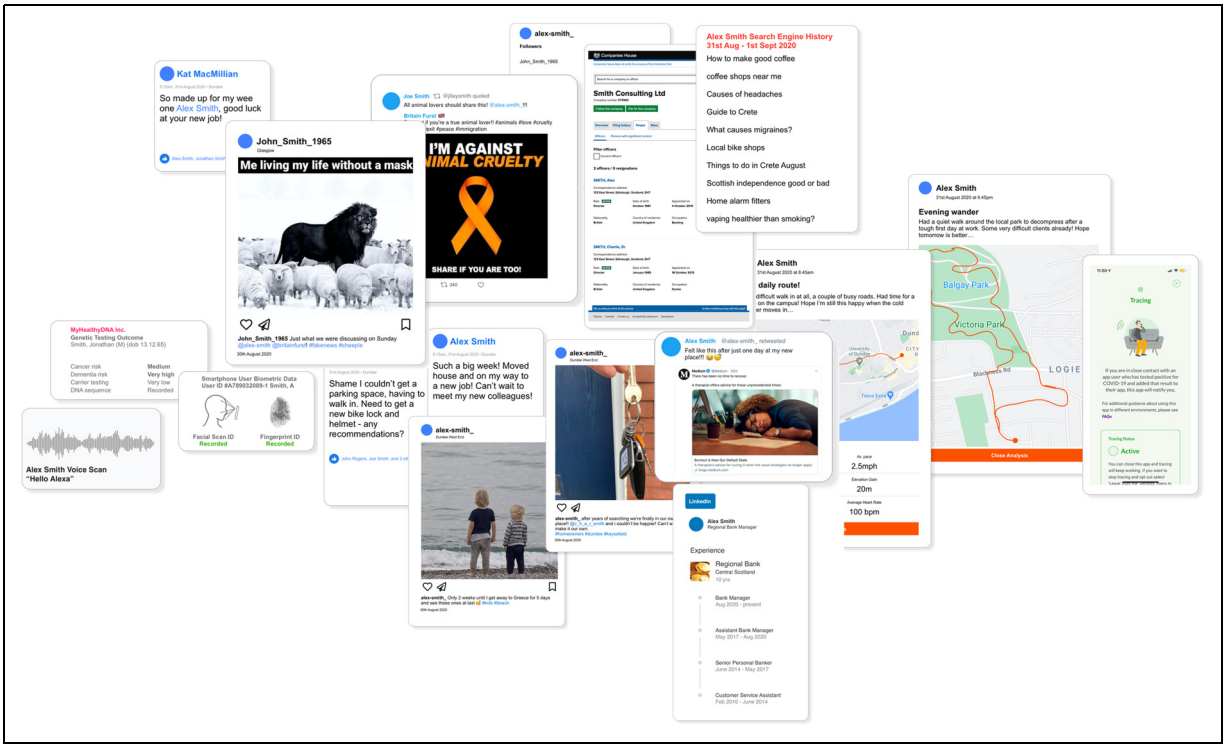

Figure 1. Montage of all five card sets.

Table 1. Participants' details, role chosen, and order of card sets selected.

Participant	Age in years/ gender	Role	Social media posts by Alex	Posts by others about Alex	Background sources	Location tracking	Bio-metric data
1	23 NB	Employer	1		2		3
2	40 M	Insurance	1		2	3	
3	32 F	Insurance	2		4	3	1
4	54 F	Employer	1	3	2		
5	20 F	Employer	1		2		3
6	25 F	Employer	1		2		
7	22 M	Employer	1	3	2		
8	29 M	Employer	1		3	2	
9	31 F	Employer	2	1			

We found that those who chose the 'employer' role offered more personal information and stories about their own digital traces on social media, whereas those who chose the insurance role took on a 'Big Data' perspective that is, determining as an insurer what types of insurance they could sell Alex. The role of insurer was less successful at facilitating self-reflection compared to the employer role. The latter role seemed more pertinent to participants' individual experiences. We discuss this in more detail below.

We recognised that the ambiguity and incompleteness of the information presented as a representation of Alex Smith's online presence would invite conjecture from participants. While we aimed to promote participants' investigation, we also provided facilitation (by one researcher) to help participants to make sense of the information (see Prakash et al., 2021). We used a creative interpretivist approach that supported reflection, discussion and narration to generate insights into understandings around cultural and contextually situated associations of information within digital traces (Goldkuhl, 2012). The aim was to generate findings toward developing an online safety tool that promotes awareness of diachronical (over time) and synchronical (across traces) risks (see Schafer et al., 2022), and safer online sharing practices.

Discussions were audio recorded, professionally transcribed and anonymised. The transcripts were uploaded to Dedoose for coding (Table 2) and analysis by the first two authors. Quotes from participants in the paper are attributed with a pseudonym to maintain anonymity (e.g. Participant one is P1, Participant two is P2 and so on for the nine participants).

Table 2. Codes used to analyse the Alex Smith study transcripts.

Risks and harms
- Awareness of digital traces/Big Data/dataveillance
- Mitigating risk

Method
- Game process
  - Trace chosen
    - Social media posts by Alex
    - Background sources
    - Bio-metric data
    - Location tracking
    - Post by others about Alex
- Ethical issues and dilemmas
- Building rapport with and between whom/what?
- Judging, making assumptions about Alex Smith

Role playing
- Insurance company
- Employer
- Blurring roles
- Researcher/detective role

Touch points – sharing personal stories

Living with everyday data

Three key findings emerged from our analysis: (1) how people manage everyday data; (2) the haunting effects and affects of peer-to-peer surveillance, and (3) post-digital identities. Overall, these findings contribute to literature on how people live with data in their everyday lives. We uncover the 'backstage' (Goffman, 1959) tactics that people use to manage their 'front stage' digital self and the haunting effects and affects of peer-to-peer surveillance. We also draw on the critical debates about post-digital identities to highlight how the method acted as a prompt or nudge for participants to reveal information about the blurring of their online and offline lives and how they manage and curate their online traces.

Managing everyday data

There is an 'ongoingness' of digital traces that requires careful management to cope with what Pink et al. (2018: 11) call the 'processual element of the everyday'. Some participants expressed apathy or resignation about low levels of risk and understood that their data-self required management, and told us that they did not bother to do anything about it: that is, they had a pragmatic acceptance of the risks. In contrast, other participants were terrified,

supporting findings by Lupton and Michael (2017) on the affective dimension of datafication. Our findings go at least some way toward explaining the oft-cited 'privacy paradox': the notion that people are concerned about loss of privacy via their online interactions yet fail to act to preserve it (Barnes, 2006; Hargittai and Marwick, 2016).

Of the participants that revealed their coping and management tactics, we found they had more awareness and knowledge about the ways in which their online activities leave digital traces and that this could be risky and cause them harm in the future. Tactics to mitigate the associated risks included:

- **Curation** 'It's curating. He'd curate, but he knows they still exist. Actually he has nightmares about the fact they still exist' (P4);
- **Using pseudonyms** 'And although I do have social media through … group accounts that I share, and I think … when I've done Google searches of me in the past when it has my name, if I'm writing something personal or doing something for media it tends to be under a pseudonym' (P1);
- **Multiple Tactics** such as entering fake information, changing privacy settings and sparing use of location tracking:

> I do sign up to stuff with fake information often. I use a different date of birth. …I set my Facebook to very private, so you can't really find me unless you're friends with a friend of mine… My Instagram is public, and I've been thinking in the last week or so to put it private … . I don't want everything to be out there… I really try to use location things as sparingly as possible. I need it sometimes to update my FitBit or to sync something to my phone which I'm using, but I really don't like it. I don't like turning on my location. I don't think that's something that people need to know or that my phone needs to know where I am exactly (P3).

The quote from P4 is from when she spoke about how her son curates his digital traces – thus supporting Milan (2018), who said digital traces promote self-reflexivity through curation – and the 'nightmares' he had about photos of his younger self on Facebook. It is beyond the scope of this article to discuss the digital traces of children (for more see Stoilova et al., 2021), but it is important to note that the quote from P4 reveals the temporal dimension of digital traces and the digital self – how we grow up and age physically **and** online. Living with data is part of our everyday life and throughout our lives, which is especially relevant for children growing up in a datafied world.

P1 manages their digital trace by restriction and selection tactics, for example, only contributing to 'group' accounts on social media. We can assume from this that a group account perhaps provides a sense of security because people in the group are perceived as like-minded; it may also have more rules and regulations about membership, for example, screening questions to answer before being accepted and being a private rather than public group. P1 also reveals that they Google themself, and in an attempt to manage their digital trace, they use a pseudonym when writing from a personal perspective or for the media. This finding extends the work by Milan (2018: 518) who advanced the notion that digital traces allow for the recognition and involvement of like-minded others as they 'promote and show(case) collectively by drawing attention to (and making tangible) the participation, networking practices, and the logic of aggregation'.

The haunting effects and affects of peer-to-peer surveillance

The dataveillance literature discussed earlier mainly focuses on the risks and harms of digital traces from surveillance by governments and businesses, yet our research revealed some examples of how peer-to-peer surveillance (amongst friends, family and work colleagues) can have haunting effects and affects. Whereas Blackman (2019) understood 'haunting' as 'shadowing' in terms of the digital self, we develop an understanding of haunting *effects* as the dataveillance gaze and the concrete, material harmful effects related to privacy, discrimination, social justice and personal freedom. The haunting effects (the gaze and the exercising of power) are invisible but are made visible by sorting and ordering. Furthermore, to understand haunting *affects*, we draw on the notion of 'haunted data' (Blackman, 2019) and affect and emotion work by geographers and others to describe a heterogeneous range of phenomena such as depression, euphoria, shame or hate, hope or panic, boredom, anxiety or fear (Anderson, 2013).

We argue that the haunting affects of data are the ways in which digital traces and your data-self emerge and are rendered visible, and this includes emotions such as regret. These findings also contribute to ethical debates about Big Data and the right to be erased or forgotten (Beraldo and Milan, 2019; Kwak et al., 2022) and also to the temporal and material functions of the data journey (Bates et al., 2016). The data capabilities approach advanced by Kennedy (2018) is also useful because it highlights the role that emotions play in ordinary people's everyday engagement with data. In their research for example, pleasure, anger, sadness, guilt, shame, worry, love, empathy, excitement and offence emerged.

We also found that the intentional, day-to-day sharing of apparently innocuous information is not without risks and can cause real harms. P9 recalled a personal experience when she was off sick from work and had posted on Facebook that she had gone shopping. A work colleague had printed this post and shown it to her managers. P9

then had to explain her actions on returning to work. She eventually left the job with no other employment to go to:

> I've been called into an office because I'd tweeted or posted something on Facebook. It was innocuous… yet they were trying to claim that I wasn't ill on a day when I was. I'd posted that I'd been to a shop, and I said 'Well I still need to eat, I still need to leave the house even if I'm ill.' … I was in a new area so I don't have friends that can go [to the shop] and I'd feel uncomfortable asking, to go and buy me things. It was really creepy as well, because it was a colleague who acted kind of friendly and then found these posts and printed them and sent them to, and it was…I no longer spoke to the colleague, unless I had to in a professional manner. If they were in the break room, I'd just get my stuff and leave. There'd be no interaction, which is quite childish, but I felt that it was a huge break of trust in terms of they had access because they'd friended me, and then to have it used in that way made me very conscious of it. So I don't post anything if I'm off ill now. Even if I have just sat on the sofa. (P9)

Peer-to-peer dataveillance in this case felt 'creepy', and the harm led to a 'childish' reaction of 'no interaction' between P9 and the work colleague. There was a huge breach of trust because they had crossed the personal/work boundaries by friending on social media, which was then used maliciously against one of them.

Similarly, but from a different perspective (the person causing the harm rather than the victim), P7 told the story of how he caused a person to lose their job at his parents' company. Here we see the exchange between the respondent (R) and the interviewer (I):

R: The first post that we saw on his Twitter account was something along the lines of '*Fuck work, it's raining this morning.'* It was like fuck work, it's raining outside. But I literally showed my parents. Like we're obviously not going to hire this guy.
I: So he wasn't offered the job. Or had they already hired him and then took it away?
R: No, no. So, their mind was made up. He was amazing. I was in the interview just because I was helping my parents out where I could and that's the guy, he's brilliant. No mistakes in any of the work he's done. Maybe one mistake. And then showed my parents [the Twitter post] and it's like well we're not going (to hire him)… that's such a shame because he was the guy. We thought he was brilliant.
I: Oh my goodness.
R: So yeah, no they basically just said no, we're not going to hire the guy that says '*fuck work*'. (P7)

From another perspective, P8, who holds safeguarding responsibilities within his work with young people, shared his approach to educating them by warning them of the gaze of others, such as peers and employers, when about to share things online:

I: Is this something that you've encountered in your own practice [the Britain First[4] post] or with the young people that you're working for?
R: Yeah, we'll see young people sharing stuff from the likes of Britain First and stuff, and it's like you've got to understand, even if you do agree with that rhetoric, first of all, it doesn't necessarily mean it's true, but also employers do look at what you share and where you share it from. It's getting them to think. So often, it's just a discussion going '*OK, if you want to share something, that's fine, but you understand who is going to see it and who might see it in the future, so if you're going to really go off the rails and put stupid stuff online and I can't stop you doing it, make sure you restrict who can and can't access it, and understand that even if it is on the internet, like even if it's restricted, people will find it. Nothing's hidden on the internet. It could look fine but be aware that somebody will find it if they want to as anybody can.'* (P8)

Our research also revealed how peer-to-peer surveillance changes over the life course, and with time social media posts may not fit with what you now think or know, or with what society expects and tolerates. This extract from P9 shows an emotional response, in this case regret, when reflecting on 'aggressive tweets' she posted after the election of Donald Trump as US President. She imagines the potential risk and harm they would cause if she was a public figure, saying that she would be 'strung up' for some of them.

> I probably regret some of the stuff in terms of the more aggressive tweets, particularly, if I tweeted Donald Trump was a cunt – although I stand by the comment, it's not really appropriate. If I was to become more of a public figure, I don't know how that would happen, but if you were to go through my tweets, I'm sure there'd be something in there that they'd try and string me up with. I don't think it's offensive in terms of, I don't tweet racist things, but I'm sure, especially over the passage of time, that things haven't aged well. (P9)

These few examples of the haunting effects and affects of peer-to-peer dataveillance reveal that while we all inhabit the world of data, we do not experience this world in the same way. Our data journeys are sometimes punctured by the haunting effects of peer-to-peer dataveillance and this haunting may cause real harms as we saw with P9 (experiencing the harm) and P7 (causing the harm). Privacy was breached in both examples. We also see how

P8 who holds a safeguarding role takes responsibility for raising awareness about the data journeys of young people and the potentially harmful consequences of the gaze of others. The warnings given by P8 highlight the temporal aspects of the data journey – the digital trace may have harmful consequences in the future. In the quote from P9, we see another dimension of the data journey – the emotional response of regret when reflecting on past social media posts and that with the 'passage of time…[they] haven't aged well'. P9 then imagines a future harmful scenario showing that the data journey is not only considered in the past and present but also in the future.

Post-digital identities

In this section, we further develop our understanding of everyday engagements and digital traces by drawing on work debating critical post-digital identities in the arts, music, design, computing and social science (Coles-Kemp, 2018; Coles-Kemp et al., 2020; Cramer, 2015; Jandrić and Knox, 2022; Savin-Baden, 2021; Taffel, 2016). These critical debates contend that post-digital is a perspective in which the digital can be seen as part (and, crucially, not *apart*) of the fabric of everyday life, and an oft cited definition is that post-digital is hard to define; messy; unpredictable; digital and analogue; technological and non-technological; biological and informational (Cramer, 2015; Jandrić and Knox, 2022). In research exploring what post-digital lives and identities might look like, Jandrić et al. (2019) discovered that for young people with digital access, boundaries between online and offline did not exist. They moved across and in and out of adjacent spaces easily. This blurring of boundaries between on and offline was most evident in gaming.

Thus, we draw on this notion of post-digital identities to understand our findings from the deployment of our Alex Smith method. We contend that the idea of post-digital can be used quite loosely to apply to a whole range of examples where the online and the offline collide and where information leaks/transfers across and between them. We also argue that seeing something online can trigger recognition through existing knowledge; for example, some participants subjectively reflected on the Alex Smith posts drawing from experience and their own contexts of local politics and community work (P4 and P8). Alex's links to political posts raised concerns with P4, who then reflected on how her office dealt with two recent politically polarising referenda: Brexit and decentralisation of UK Government. While people in her office tended to have a sense of colleagues' political orientation, a 'no politics in the office' rule kept office culture 'professional'.

There was also evidence of participants who had a clear understanding of their professional safeguarding responsibilities, and who also had some had experience of responsible practice pre-internet. Here, the work of Davis and Jurgenson (2014) is most relevant, as they distinguish between two different types of context collapse – context collusions and context collisions – with the important distinction being that of intentionality. Whereas *context collusion* is the 'process whereby social actors intentionally collapse, blur, and flatten contexts, especially using various social media', *context collision* is the 'situation when different social environments unintentionally and unexpectedly come crashing into each other' (Davis and Jurgenson, 2014: 480). These participants intentionally and actively resisted the collapse of their digital selves. For example, community and youth workers (P4 and P8) were clear that in their online identities and behaviour, they must be careful and professional and that this was non-negotiable and there were clearly defined boundaries. Their digital identity was thus a professional, depoliticised re-presentation of self.

Another participant had worked in UK Government. A combination of the role-playing and the facilitator asking questions to understand more about the Alex Smith persona revealed another example of how the post-digital identity is managed. P5 'would always check what I'm posting' while working with parliament, and in response to the question from the facilitator about how she would judge what to share, she said she would cross-check linked sources to 'fact check'. When reposting, including anything political, she would only do this with a source from a direct associate, saying she was aware that social media posts were always subject to others' interpretation and validation even within the same political group. She had learnt from experience that her time was better spent considering what she was about to post rather than sharing something 'without really thinking about it', which then led to 'backlash' that required considerable time and effort on her part to remedy.

Conclusion

The purpose of this article was to advance understandings of everyday or mundane data (Pink et al., 2017) by exploring ordinary people's seemingly innocuous digital traces generated through everyday online interactions and to share our approach using the Alex Smith method. Our aim was to not only provide insights into how people perceive and manage their data, and a method to approach these perceptions and practices, but also to raise public awareness and defence when it comes to the multiple value and responsible use of digital traces. We acknowledge the limitations of the study – the sample was small in that there were only nine participants, therefore we are unable to generalise our findings. Rather they offer examples of everyday digital traces from which to develop further research and indeed, have informed a browser-based tool that we subsequently developed (see Azzopardi et al., 2022).

The unique contributions of our paper are: First, we draw on the work of Blackman (2019) to develop a new understanding, which we call the 'haunting effects and affects of peer-to-peer surveillance'. Peer-to-peer surveillance is an under-researched area of dataveillance and its focus is surveillance amongst ordinary people and between *known* friends, family and work colleagues rather than *unknown* government and businesses which dominates in the literature. Our understanding of the haunting *effects* combines the powerful dataveillance gaze and the harmful effects related to privacy. Although the haunting effects are invisible, they are made visible by sorting and ordering. By haunting *affects*, we extend the notion of 'haunted data' (Blackman, 2019) and affect and emotion work by geographers and others to describe moods, visceral responses, shared atmospheres, fleeting feelings and societal moods, amongst others (Anderson, 2013, Kennedy, 2018). Thus, we advance a way of understanding peer-to-peer surveillance and the ways in which digital traces and your data – self can be rendered visible by friends, family and work colleagues and the emotional impacts and temporal aspects of those revelations.

Second, we advance work on data journeys by arguing that a consideration of the haunting effects and affects of peer-to-peer surveillance further develops understandings of the way that digital traces can puncture and cause friction during the data journey of ordinary people and illicit various emotional responses. For example, we saw how the work colleague of P9 effectively stalked her data journey and used it maliciously by reporting her social media post made whilst sick to their boss. This caused a friction in an ordinary person's data journey. It rendered an emotional response in P9, resulting in a loss of trust within the workplace, a breach of privacy and a real harm leading to P9 leaving her job without having another to go to. Our research also revealed insights into the temporal dimensions of the data journey when viewed through the lens of peer-to-peer surveillance. Peer-to-peer surveillance changes over the life course, and with time, social media posts may not fit with what you now think or know, or with what society expects and tolerates. Just as digital traces accumulate over time, the digital self is represented as a snapshot in time – for example, as a photo in a place at a particular age, or as a log of visiting a place at a particular time. The digital trace is partial and thus open to others' interpretation; and while we all inhabit the world of data, we do not experience it in the same way. Our data journeys are unique but simultaneously emmeshed with others'.

Third, it was evident that some participants conceptualised their digital activities as enmeshed with the fabric of their everyday life, supporting the literature (e.g. Jandrić et al., 2019) that there is no online and offline. Respondents demonstrated what Davis and Jurgenson (2014) call context collusion and our findings show very well that/how digital traces question/make it difficult for people to keep their different social contexts or social roles apart and separate from each other. This finding also advances understandings of ordinary people's data journey. We argue that by examining everyday digital traces in the data journey of ordinary people reveals both context collusion (intentionally collapsing, blurring and flattening contexts) and collision (the unintentional and unexpected social environments crashing into each other). Everyday digital traces are part of the temporal and material aspects of the data journey. We saw this also in relation to the (post-)pandemic re-combinations of working and living across private, personal and professional contexts. Certainly, participants referred to their information leaking from and transferring across and between different sources. This comprises a rich area for further research, especially relating to the multimodal potentiality of visual and other non-language-based media; and the linking between something seen online triggering recognition within embodied, yet to be articulated or shared in the world, personal knowledge. On the other hand, those with substantial safeguarding experience acquired through professional responsibilities including pre-internet, both intentionally and actively resisted any context collusion taking a non-negotiable stance grounded in their heightened awareness of how online information is always open to the gaze, judgement and malevolent use of known or unknown others.

Fourth, we reflect on our methodological contribution and consider two questions. The first question is: what can the example of everyday digital traces contribute to the discussion of data journey approaches to 'sites' and perspectives of data production and (potentially) (re)use of data?

We argue that it is the mutability and durability of digital traces, that is, the way they can be aggregated, linked and re-configured and the persistence of them over time. As digital traces move through time their material context can stay the same, that is, the social media source, while the social context can change, altering the perception, understanding and acceptability of that trace in the eyes of others and in the eyes of the original poster, for example, if they posted as a child. While this may lead to the original poster attempting to homogenise and clean their digital trace some traces are unknown, unintentional, or forgotten about, leading to consequences or even harms in the future.

We also argue for the self as a site of data production. In their project the Secret Life of Weather Datum focused on UK-based sites of weather data production, Bates et al. (2016) mapped the journey of data between relevant organisations, projects, datasets and individuals. The data produced was not personal but nevertheless revealed how friction in the movement of data can reflect and be shaped by power dynamics, for example, the example of the museum weather station, the publicness of the data

produced and Open Data policies that would have an impact on the small-scale commercialisation of the data. When considering everyday digital traces there are multiple sites of data practice, that is, the different social media platforms used over the life course, etc. As Edwards (2010) argues, the data journey is not a smooth, continuous flow but rather one of disjointed breaks, pauses and friction.

Our research also reveals the way the researcher becomes part of the data journey of their research subject – being a traveller – to stop off, take in the surroundings and absorb the culture. Our Alex Smith method enabled participants to become the traveller. Our creative method enabled participants to articulate approaches to mitigating online risk, an awareness of the care required to control and maintain separation between digital traces, and of possible collisions when different social contexts become proximate, for example, between the public, private, personal and professional self (see Davis and Jurgenson, 2014). Mostly, participants discussed these separations and collision of traces from their own perspectives and experiences, showing how the method, combined with the discussions the researcher enabled, encouraged some to narrate and self-disclose quite personal information. It was interesting to note that the three (P1, P5 and P9) who did so were employed in professional sectors such as the civil service, government and teaching, where privacy, security, responsibility and the morality of public servants are particularly scrutinised and expected.

A second questions is: how does a data journey approach shed new light on the discussion of digital traces and privacy issues?

Here we argue that the publicness of some digital traces or the intentional sharing of them means that strangers along with known others can become a traveller and stop off and observe the ordinary person. This may be someone who is nosy, a stalker, a potential or actual employer, or larger agencies such as governments, or even AI. As Bates et al. (2016: 10–11) argue, overall:

> …the data journeys methodology illuminated the ways in which data are produced, processed and used across diverse sites of practice that are interconnected by the movement of data across space and time, the ways in which socio-cultural values and material factors come together to frame and give justification for these practices, and how together these contribute to the production of emergent socio-material conditions.

Overall, our research synthesises from disparate fields and findings from the deployment of our creative method to contribute insights into how people imagine and reflect on their holistic digital traces, with implications for citizens, data studies research, corporate entities and governments. Additionally our persona-based method, which is presented with sufficient detail to enable reproduction or customisation, demonstrates the value of such creative approaches in rendering more imaginable and manageable the complexity of personal data and digital traces.

Declaration of conflicting interests

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

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Engineering and Physical Sciences Research Council (grant number EP/R033854/1, EP/R033870/1, EP/R033889/2, EP/R033897/1).

ORCID iDs

Andrea Armstrong https://orcid.org/0000-0003-4685-7715
Wendy Moncur https://orcid.org/0000-0002-1485-4723
Daniel Paul Carey https://orcid.org/0000-0002-7311-0038
Burkhard Schafer https://orcid.org/0000-0002-6025-4593

Notes

1. We use 'digital self' to mean the person you are online as opposed to the 'real world' self.
2. We draw on boyd's (2008) understanding of networked publics as **unmediated publics**, which are areas that have boundaries and are structurally defined.
3. We were concerned that informed consent is impossible to acquire when participants do not know what they are consenting to, and that in recognising connections across their personal information of which they were previously unaware, they could experience a 'revelation' and distress.
4. Britain First is a far-right political party.

References

Agre PE (1994) Surveillance and capture: Two models of privacy. *Information Society* 10: 101–127.

Albury K, Burgess J, Kay B, et al. (2021) Everyday data cultures. 22nd Annual Conference of the Association of Internet Researchers, virtual event.

Anderson B (2013) Affect and emotion. In: Johnson N, Schein R and Winders J (eds) *The Wiley-Blackwell Companion to Cultural Geography*. Chichester: John Wiley & Sons, pp. 452–464.

Azzopardi L, Briggs J, Duheric M, et al. (2022) Are Taylor's posts risky? Evaluating cumulative revelations in online personal data: A persona-based tool for evaluating awareness of online risks and harms. Proceeding of Conference on Research and Development in Information Retrieval, 3295–3299.

Barnes SB (2006) A privacy paradox: Social networking in the United States. *First Monday* 11(9) DOI: 10.5210/fm.v11i9.1394

Bates J, Lin YW and Goodale P (2016) Data journeys: Capturing the socio-material constitution of data objects and flows. *Big Data & Society* 3(2): 1–12.

Bauman Z and Lyon D (2013) *Liquid surveillance: A conversation*. Chichester, UK: John Wiley & Sons.

Baym N (2015) *Personal Connections in the Digital Age*, 2nd ed Cambridge: Polity.
Beraldo D and Milan S (2019) From data politics to the contentious politics of data. *Big Data & Society* 6(2): 1–11.
Blackman L (2019) *Haunted Data: Affect, Transmedia, Weird Science*. London: Bloomsbury.
Borgman C (2015) *Big Data, Little Data, No Data*. Cambridge: MIT Press.
boyd d (2008) Why youth (heart) social network sites: The role of networked publics in teenage social life. In Buckingham D. (ed.) *Youth, Identity, and Digital Media*. Cambridge: MIT Press, pp. 2007–2016.
boyd d (2010) Public by default private when necessary. Available from https://www.zephoria.org/thoughts/archives/2010/01/25/public_by_defau.html (blog post accessed July 2023).
Breiter A and Hepp A (2018) The complexity of datafication: Putting digital traces in context. In Hepp A, Breiter A and Hasebrink U (eds) *Communicative Figurations Transforming Communications–Studies in Cross-Media Research*. London: Palgrave Macmillan, Cham, pp. 387–405.
Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge: MIT Press.
Büchi M, Festic N and Latzer M (2022) The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society* 9(1): 1–14.
Burgess J (2017) *Hook-up apps' vernacular data cultures*. Social Life of Data symposium, April, RMIT University, Melbourne.
Burgess J, Albury K, McCosker A, et al. (2022) *Everyday Data Cultures.* Cambridge UK: Polity Press.
Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512.
Coles-Kemp L (2018) *Practising creative securities*. Surrey, UK: Royal Holloway University of London. https://bookleteer.com/collection.html?id=28.
Coles-Kemp L, Jensen RB and Heath C. (2020) Too much information: Questioning security in a post-digital society. Proceedings of the Conference on Human Factors in Computing Systems. ACM, New York, USA, 1–14.
Couldry N and Powell A (2014) Big data from the bottom up. *Big Data & Society* 1(2): 1–5.
Cramer F (2015) What is 'post-digital'? In Berry DM and Dieter M (eds) *Postdigital Aesthetics: Art, Computation and Design*. New York: Palgrave Macmillan, pp. 12–26.
Davis JL and Jurgenson N (2014) Context collapse: Theorizing context collusions and collisions. *Information, Communication & Society* 17(4): 476–485.
Deleuze G (1990) *Logique du sens*. New York, NY, USA: Columbia University Press.
Edwards P (2010) *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*. Cambridge, MA: MIT Press.
Ertzscheid O (2009) L'homme est un document comme les autres: Du world wide web au world life web. *Hermès* 53: 33–40.
Flyverbom M (2016) Digital agel transparency: Mediation and the management of visibilities. *International Journal of Communication* 10: 13.
Flyverbom M and Murray J (2018) Datastructuring—organizing and curating digital traces into action. *Big Data & Society* 5(2): 1–12.
Foucault M (2001) *L'herméneutique du sujet*. Paris: Seuil/Gallimard. Paris.
Goffman E (1959) *The Presentation of Self in Everyday Life*. New York, NY: Anchor Books.
Goldkuhl G (2012) Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems* 21(2): 135–146.
Graham S and McFarlane C (2014) *Infrastructural Lives: Urban Infrastructure in Context*. London: Routledge.
Haggerty KD and Ericson RV (2000) The surveillance assemblage. *British Journal of Sociology* 51(4): 605–622.
Hansen HK and Flyverbom M (2015) The politics of transparency and the calibration of knowledge in the digital age. *Organization* 22(6): 872–889.
Hargittai E and Marwick A (2016) What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication* 10: 21.
Hartmann M (2013) From domestication to mediated mobilism. *Mobile Media and Communication* 1(1): 42–49.
Henman PWF (2022) Digital social policy: Past, present, future. *Journal of Social Policy* 51(3): 535–550.
Jandrić P and Knox J (2022) The postdigital turn: Philosophy, education, research. *Policy Futures in Education* 20(7): 780–795.
Jandrić P, Ryberg T, Knox J, et al. (2019) Postdigital dialogue. *Postdigital Science and Education* 1(1): 163–189.
Jones A (2018) Have you signed up for a tracking app by mistake? *Guardian*. https://www.theguardian.com/technology/shortcuts/2018/jan/29/have-you-signed-up-for-a-tracking-app-by-mistake (accessed August 2022).
Kennedy H (2018) Living with data: Aligning data studies and data activism through a focus on everyday experiences of datafication. *Krisis Journal for Contemporary Philosophy* 1: 18–30.
Kwak C, Lee J and Lee H (2022) Could you ever forget me? Why people want to be forgotten online. *Journal of Business Ethics* 179(1): 25–42.
Laflaquière J (2009) *Conception de système à base de traces numériques dans les environnements informatiques documentaires*, Thèse de l. Université de Technologie de Troyes.
Leszczynski A (2020) Digital methods III: The digital mundane. *Progress in Human Geography* 44(6): 1194–1201.
Leszczynski A and Crampton J (2016) Introduction: Spatial big data and everyday life. *Big Data & Society* 3(2): 1–6.
Lupton A and Watson A (2021) Towards more-than-human digital data studies: Developing research-creation methods. *Qualitative Research* 21(4): 463–480.
Lupton D (2016) *The Quantified Self*. Cambridge: Polity Press.
Lupton D (2020) Thinking with care about personal data profiling: A more-than-human approach. *International Journal of Communication* 14: 19.
Lupton D (2021) Not the real me': Social imaginaries of personal data profiling. *Cultural Sociology* 15(1): 3–21.
Lupton D and Michael M (2017) Depends on who's got the data': Public understandings of personal digital dataveillance. *Surveillance & Society* 15(2): 254–268.
Massey D (1994) *Space, Place and Gender*. Minneapolis: University of Minnesota Press.
Mathieson T (1997) The viewer society. *Theoretical Criminology* 1(2): 215–234.
Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.

Michael M (2006) *Technoscience and Everyday Life*. Open University Press.

Milan S (2018) Political agency, digital traces, and bottom-up data practices. *International Journal of Communications* 12: 507–527.

Nicol E, Briggs J, Moncur W, et al. (2022) Revealing cumulative risks in online personal information: A data narrative study. Proceeding of ACM Human Computer Interaction. *6, CSCW2*, Article 323.

Ozduzen O and Korkut U (2020) Enmeshing the mundane and the political: Twitter, LGBTI+ outing and macropolitical polarisation in Turkey. *Contemporary Politics* 26(5): 493–511.

Pink S, Lanzeni D and Horst H (2018) Data anxieties: Finding trust in everyday digital mess. *Big Data & Society* 5(1): 1–14.

Pink S, Sumartojo S, Lupton D, et al. (2017) Mundane data: The routines, contingencies and accomplishments of digital living. *Big Data & Society* 4(1): 1–12.

Pitsillides S, Waller M and Fairfax D (2013) Digital death: What role does digital information play in the way we are (re)membered? In Warburton S and Hatzipanagos S (eds) *Digital Identity and Social Media*. Hershey, Pennsylvania, USA: IGI Global, pp. 75–90.

Prakash M, Kang W, Li W, et al. (2021) Embodying a narrative: Spatializing abstract narrative themes for forensic exploration. EA of the 2021 CHI Conference on Human Factors in Computing Systems: 1–6.

Prieto-Alvarez CG, Martinez-Maldonado R and Buckingham Shum S (2018) Mapping learner-data journeys: Evolution of a visual co-design tool. In Proceedings of the 30th Australian conference on computer-human interaction, 205–214.

Reigeluth TB (2014) Why data is not enough: Digital traces as control of self and self-control. *Surveillance & Society* 12(2): 243–254.

Ruckenstein M (2014) Visualized and interacted life: Personal analytics and engagements with data doubles. *Societies* 4(1): 68–84.

Ruckenstein M and Pantzar M (2015) Datafied life: Techno-anthropology as a site for exploration and experimentation. *Techné: Research in Philosophy and Technology* 19(2): 191–210.

Savin-Baden M (2021) *Postdigital Humans: Transitions, Transformations and Transcendence*. Cham: Springer.

Schafer B, Briggs J, Moncur W, et al. (2023) What the Dickens: Post-mortem privacy and intergenerational trust. *Computer Law & Security Review* 49: 105800.

Schafer B, Nash C, Carey D, et al. (2022) *Making Sense of Trifles: Data Narratives and Cumulative Data Disclosure*. Jusletter IT.

Shorey S and Howard PN (2016) Automation, algorithms, and politics| automation, big data and politics: A research review. *International Journal of Communication* 10: 5032–5055.

Smith GJ (2016) Surveillance, data and embodiment: On the work of being watched. *Body & Society* 22(2): 108–139.

Smith GJ (2018) Data doxa: The affective consequences of data practices. *Big Data & Society* 5(1): 1–15.

Stalder F (2002) Privacy is not the antidote to surveillance. *Surveillance & Society* 1(1): 120–124.

Stoilova M, Nandagiri R and Livingstone S (2021) Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society* 24(4): 557–575.

Taffel S (2016) Perspectives on the postdigital: Beyond rhetorics of progress and novelty. *Convergence: The International Journal of Research Into New Media Technologies* 22(3): 324–338.

Van Dijck J (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.

Vertesi J, Kaye JJarosewski, et al. (2016) Data narratives: Uncovering tensions in personal data management. In Proceedings of Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16), pp. 478–490.

Williams JP and Waskul DD (2007) Mundane life in a media age. *Symbolic Interaction* 30(4): 627–636.

Wolf C, Ringland KE, Gao I, et al. (2018) Participating through data: Charting relational tensions in multiplatform data flows. In Proceedings of ACM Human Computer Interaction 2, CSCW, article 184.

Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civilisation. *Journal of Information Technology* 30: 75–89.