Thinking With Care About Personal Data Profiling: A More-Than-Human Approach

DEBORAH LUPTON
University of New South Wales (UNSW) Sydney, Australia

People's understandings and practices related to their digitized personal information are urgent topics of social inquiry in an increasingly datafied world. This article draws on findings from an Australian qualitative study in which the stimulus of the "data persona" and an online platform were used to engage participants' social imaginaries concerning how data profiling can benefit or harm them and to what extent they care about their personal data. The findings were theorized by thinking with more-than-human scholarship and theories of care. The study found that although these participants were well aware of data profiling and algorithmic processes such as those used for targeted advertising, most did not feel personally vulnerable to harms or risks. The participants suggested that datafication and dataveillance could never access their "real selves." Data profiling was predominantly viewed as helpful in providing better customization. In some situations, however, data profiling and related data processing could be selective, fragmentary, and dehumanizing. The article ends with discussion of the broader implications of the study's findings for theorizing and understanding human–data relations.

Keywords: digital data, personal data, data profiling, selfhood, more-than-human theory

The expansion of digital technologies and services that generate detailed information about people has incited much interest of late from social researchers. The term "datafication" is frequently employed in this literature to describe how people's bodies and practices are rendered into digitized information when they go online, use apps and "smart" devices, or move in environments embedded with digital sensors (van Dijck, 2014), and "dataveillance" is used to describe the systematic collection and use of these data for the purposes of watching people (Clarke & Greenleaf, 2018). Some social theorists have argued that datafication and dataveillance are increasingly contributing to people's concepts of selfhood, forming "numbered lives" (Wernimont, 2019), "digital selves" (Cheney-Lippold, 2018), or "data selves" (Lupton, 2019), even to the point of "colonizing" (Couldry & Mejias, 2019) identities and "controlling our lives" (Sadowski, 2020). In response, some researchers and policymakers have begun to call for greater attention to be paid to potential "data harms" (Redden & Brand, 2019) and for publics to develop better "data literacies" (Frank, Walker, Attard, & Tygel, 2016) as a way of publicizing and countering these harms in the interests of "data justice" (L. Taylor, 2017).

Deborah Lupton: d.lupton@unsw.edu.au
Date submitted: 2019–09–26

At the heart of these issues are, first, ideas of human identity, selfhood, and social relations, and second, concepts of care. Much of the current literature on these issues tends to separate humans from their personal digital data and the agents who use these data, positioning the former as lacking agency in the face of the exploitation of the latter. In this article, I seek to adopt a different perspective on these issues. I draw on some findings from an empirical study to discuss how datafication and dataveillance can be considered from the lens of more-than-human theories and, more specifically, scholarship taking up these perspectives to address "matters of care" and stimulate new ways of "thinking with care" (Puig de la Bellacasa, 2017). As Puig de la Bellacasa (2017) observes, thinking with care involves directing attention to the intersections of humans and nonhumans in caring relations. She calls for decentering human agency in caring practices and recognizing the distribution of capacities in human–nonhuman care assemblages. This approach involves paying close attention to how care operates as a knowledge-making practice and its affective dimensions, as well as its fraught politics (Martin, Myers, & Viseu, 2015).

In what follows, I draw on findings from my Data Personas study, which was designed to explore how a group of Australian adults conceptualized personal data profiling and its benefits as well as its harms. In adopting more-than-human theoretical perspectives, I position people as coming together with digital technologies to produce human–data assemblages that are constantly changing (see Lupton, 2019). The study elicited the participants' social imaginaries concerning such issues as how personal data collection, archiving, processing, and use are conducted; who benefits or is harmed from these processes; how well personal data are preserved and protected for people's own use into the future; and how adequately they are protected from misuse by third parties. I first provide an overview of the ways in which datafication and dataveillance have been increasingly imagined in both the popular media and in media and social science scholarship as exploiting people, restricting their life opportunities, and harming their well-being. I then elaborate on the theoretical perspectives I worked with in designing the Data Personas study and analyzing the participants' responses. Details of how the study was carried out are then explained and the analysis presented, with attention to the ways in which the participants responded to questions about how they can benefit from or be harmed by their data personas and how they can protect their personas. The article ends with discussion of the broader implications of the study's findings for theorizing and understanding human–data relations.

Background

An increasingly critical perspective on datafication and dataveillance has been advanced in recent years in academic scholarship and popular media coverage. Some of this commentary has been in response to scandals concerning the misuse of personal data. Since Edward Snowden's revelations in 2013 outlining how Western governments have conducted dataveillance on their unsuspecting citizens (Lyon, 2014), a series of highly publicized massive data breaches, leaks, and hacks have affected tens of millions of service users worldwide. These include leaks or breaches of the personal data entered by users into services such as the adultery website Ashley Madison, Yahoo! Groups, and Microsoft Outlook, as well as the notorious Facebook/Cambridge Analytica scandal in 2018.

News reports have frequently portrayed these processes as manipulative and exploitative of the vital forces of humans, peering unceasingly into their minds and hearts in the effort to know them better and thereby sell people products they do not want; influence their political views; or prevent them from accessing opportunities such as travel, access to credit, or insurance coverage. The words "addiction," "pathology," "toxicity," "control," and "weaponization" are frequently employed in these imaginaries, implying that people lack agency over their personal data and how they are used by others (Lupton, 2019).

The academic literature on datafication and dataveillance has similarly predominantly focused on how people are watched by third parties who seek to exploit them and profit from their personal data (Andrejevic, 2014; Sadowski, 2020). In recent years, researchers' attention has turned to the use of digitized personal information to score, rank, and make predictions about people by employing data mining and algorithmic profiling techniques (Cheney-Lippold, 2018). In this literature, people's personal data are portrayed as vulnerable in their sheer openness to exploitation and value to others, particularly for members of social groups that are already socioeconomically disadvantaged. Books with titles such as *Algorithms of Oppression* (Noble, 2018) and *Weapons of Math Destruction* (O'Neil, 2016) express these vulnerabilities and suggest that human flourishing is limited by processes of datafication and dataveillance.

A narrative about people's apparent resignation to datafication and dataveillance is also gaining ground in fields such as surveillance studies, new media studies, and critical data studies. The terms "online apathy" (Hargittai & Marwick, 2016) and "digital resignation" have been employed by some researchers to describe people's responses to such issues as how well their personal data are protected and how third parties make use of them (Draper & Turow, 2019). Another term is "surveillance realism" (Dencik & Cable, 2017), used to describe publics' awareness that dataveillance and datafication are pervasive and normalized despite recognition of their injustices, thus limiting possibilities of resisting or thinking otherwise.

In response to these concerns, researchers working in critical data studies, as well as regulators and civil society and other advocacy groups, have called for greater attention to be paid to ensuring that digitized personal information is collected and processed in more socially responsible ways. They have demanded that researchers, governments, and Internet companies be held more stringently to account for how they use these data (Clarke & Greenleaf, 2018; Petty, Saba, Lewis, Gangadharan, & Eubanks, 2018). The European Union's General Data Protection Regulation, effected in 2018, is an example of a major legal response to protecting the information of "the data subject," including a right for this subject not to be subjected to a decision made by automated decision making (Brkan, 2019).

Taken together, these popular cultural and academic discussions present predominantly dystopian visions for the futures of personal data. The predominant focus concerning care in relation to personal data highlights the role of organizations, regulatory agencies, and institutions in protecting citizens. Although it is clearly important to identify misuses of personal data and institutional responsibilities for citizen protection, these representations of datafication and dataveillance can veer toward positioning publics as lacking agency. They can also often elide any differences in the ways that diverse social groups and people living in different geographical regions experience these phenomena: for example, the United States compared with Australia, or privileged nations in the Global North compared with those in the Global South (Arora, 2019; Couldry & Mejias, 2019; Milan & Treré, 2019).

It is important to recognize that datafication and dataveillance can be experienced and understood by different social groups in very different ways, according to such attributes as age, geographical location, political context, access to digital technologies and infrastructures, education level, and other sociodemographic characteristics. Previous studies have demonstrated that although many of the platforms and apps with which people engage are globalized, generating similar flows of personal data across the countries in which they are used, national services and systems using personal data differ considerably. For example, countries such as the United States have progressed much further than others in using data profiling, with automated decision-making systems applied to such processes as welfare payments, job applications, insurance, predictive policing, and criminal sentencing. These processes have been identified as working to discriminate against disadvantaged and marginalized social groups in ways that are often hidden and cannot be easily challenged (Petty et al., 2018).

Even within nation-states, the experiences of people with these processes can differ wildly. Research in the U.S. context has shown that compared with more socioeconomically privileged people, disadvantaged people feel more threatened by harms such as loss or theft of their financial information, lack of knowledge about what information is being collected about them, becoming the victim of Internet fraud or scam, or targeted for online harassment (Madden, Gilman, Levy, & Marwick, 2017; Petty et al., 2018). In contrast, recent social research with more privileged people in other countries in the Global North (Bucher, 2018), including Finland (Ruckenstein & Granroth, 2020) and Denmark (Lomborg & Kapsch, 2019), has found that although participants had a high level of awareness and knowledge about how algorithmic processing of personal data and related practices operate, they reported few negative experiences with it beyond occasional frustration or annoyance that targeted advertising can be intrusive or inaccurate.

As these studies demonstrate, concepts of data privacy are historically, culturally, politically, and geographically contingent (Arora, 2019; Kukutai & Taylor, 2016; Milan & Treré, 2019), and so too is the extent to which people "care" for and about their personal data and how this information is used by third parties. This research highlights the importance of identifying and considering the situated complexities and ambivalences that are part of people's lived experiences of dataveillance and datafication. Thus far, however, few inquiries have fully engaged with the more-than-human aspects of these dimensions and the implications of this perspective for understanding matters of care in relation to digitized information about people and their lives.

More-Than-Human Theory and Care

More-than-human theory can cast a different light on people's encounters with and enactments of their personal data (Lupton, 2019). This approach, as it is expounded in feminist new materialism (Barad, 2007; Bennett, 2009; Braidotti, 2019; Haraway, 2016) and in Indigenous (Bawaka Country et al., 2015; Todd, 2016) and non-Western cosmologies (Kwek, 2018; Lee, Sakuno, Prebensen, & Kimura, 2018), positions humans as coming together with nonhumans (other animals and living things, objects, place, and space) in dynamic ways as they move through their everyday lives. It draws attention to the distributed and relational dimensions of the agential capacities that are generated in and through humans' encounters with nonhumans. Barad (2007) uses the term "intra-action" to encapsulate the idea that these capacities are never pre-existing but are rather always emergent as humans gather with nonhuman agents. For Braidotti (2006), the approach she characterizes as a "nomadic ethics" recognizes the mutability and complexity of identities as they are mediated globally and technologically, challenging the idea of moral universalism.

More-than-human theory has significant implications for how care in the context of human–data assemblages might be conceptualized. Once it is accepted that at the onto-ethico-epistemological level (Barad, 2007) humans are never inseparable from nonhumans, the notion of care becomes expanded to a more-than-human dimension. More-than-human theorists have sought to recast theorizations of care around notions of responsiveness (Haraway, 2015; Puig de la Bellacasa, 2017). Responsiveness involves attentiveness to the relations and entanglements that humans have with nonhumans as well as with each other. Indigenous and non-Western philosophies have traditionally emphasized the ethical relationships that humans have with nonhumans, particularly in relation to the physical environment and other living things. They highlight the importance of attentiveness to the interrelated and embodied responsibilities of care when humans and nonhumans come together, and to the life forces that are generated (Bawaka Country et al., 2015; Kwek, 2018; Todd, 2016). Indigenous perspectives are also strongly contextualized, referring to embodied traditions of thought and practice that are specific to geographical locations. They therefore draw attention to the emplaced and historical nature of ethical relationships of care in more-than-human worlds.

Some researchers are beginning to experiment with applying this approach to human-made objects such as digital technologies and the data generated from humans' use of these technologies, in ways that can work to reorient social inquiry toward concepts of care. From a more-than-human perspective, human–data assemblages can be considered as lively, constantly moving, and changing as new data points are created when humans move through their days and make contact with technologies that produce digitized information about and with them (Bucher, 2018; Lupton, 2019; Wernimont, 2019). These assemblages can be materialized in many different formats using digital technologies or hands-on methods, including two-dimensional data visualizations such as graphs, numbers, and images; and three-dimensional objects such as craft and art works or artifacts made by 3D printers (Kennedy & Hill, 2018; Lupton, 2017). Data materializations can generate a range of affects, connections, and capacities that can work to make people feel that their data matter and help them to care about and for their data (Kennedy & Hill, 2018; Lupton, 2019; Wernimont, 2019).

Building on this emerging scholarship on the sociomateriality of digitized information, I argue that adopting a "thinking with care" approach and viewing data as human–nonhuman assemblages can generate awareness of and attentiveness to the affective as well as social, cultural, and political dimensions of these assemblages. This approach can address questions that go beyond a preoccupation with institutional agency and the repressive nature of datafication and dataveillance, avoiding a techno-deterministic, top-down perspective that sets people and data/technologies as separate from and in opposition to each other. These questions include the following: How do we care for our personal data, and how much do we care about them? What affordances and affects are generated with and through our data? What ethical relations should we have with our data, and how might these change across time and space? What should our responsibilities be with and for them? The Data Personas study was designed as a way of beginning to address these questions by bringing more-than-human theoretical perspectives together with empirical research based in Australia.

The Data Personas Study

In Australia, numerous personal data scandals have received public attention over the past decade, including local events as well as the globalized breaches that have received international attention. These events have been mostly related to poor implementation of data entry or profiling systems by the Australian government. The "robo-debt" scandal was one such scandal, receiving a high level of news media scrutiny in late 2016 and early 2017, when it was suggested that social security recipients were being unfairly treated by inaccurate algorithmic processing of their income and tax data (Henman, 2019).

In attempting to site research on personal data in a more-than-human context, and building on the concept of thinking with care, the Data Personas study gave participants the opportunity to consider the ways in which digital data are generated about them, who benefits from these data, and the risks and harms of these data for themselves. It also provoked them to consider how they themselves could use their personal data, how their data could be protected and preserved for their own purposes, and what measures could be introduced in the future to help them benefit from their data. The project therefore sought to introduce a perspective on personal data that recognizes not only its potential to restrict people's freedoms and opportunities, but also its possibilities for publics.

I used the stimulus of the "data persona" as a way of inviting participants to think about and express these issues. This approach sought to elicit the participants' social imaginaries: that is, the dominant frameworks of discourses and ideas that are shaped by and enacted through practices (C. Taylor, 2004) and operate as cultural resources in creating and sharing meaning (Jasanoff & Kim, 2013). I developed a series of questions for the study that used the data persona concept to stimulate the participants to imagine how their personal data were being generated and which third parties may be accessing and using their data. A definition of the "data persona" was provided to the participants as follows: "A version of you made by finding personal information about you from when you move around in spaces embedded with sensors or use digital devices like smartphones, wearable technologies, tablet computers, laptops and desktop computers." The words "persona" and "version of you" were deliberately chosen to bestow a sense of humanness and selfhood on the concept of a human–data assemblage (compared with terms such as big data or data profile) as part of encouraging responsiveness and a more-than-human perspective, but also attempting to avoid the suggestion that such a data profile incorporates every detail about an individual. We all have multiple data personas that are continually forming and re-forming, but in the interest of simplicity, I used the singular rather than the plural.

To conduct the study, I used an online platform that is tailored toward qualitative research that had been developed by a research company. I worked with the research company to customize the dedicated project platform. The project had been approved by the University of Canberra Human Research Ethics Committee (I was located at that university at the time the study was conducted). Questions were uploaded onto the platform and participants were asked to first review the project participant information and agree to participate by checking an online button before responding to them.

The participants were derived from the company's panels, which consist of people who have volunteered to be approached for participation in commercial or university research. Panel members 18 years of age and over were sent invitations to participate, and the first 40 people to express their interest were signed up to the study. The participants resided in all states in Australia and included 22 women and 18 men. The participant group was on the younger side: 28 were 18 to 39 years of age, and 12 were over 40 years (only two were 60 years or over). In terms of educational backgrounds, 18 participants reported high school or technical college training; the remainder (22) reported having at least some university-level education. The participant group was quite diverse in terms of ethnicity/racial background: 27 reported Anglo-Celtic ancestry, and the remaining 13 participants reported other ethnic/racial heritages. This diversity reflects that of the Australian population in general, in which almost half of Australians were born overseas or have at least one parent who was born overseas, and one in five speaks a language other than English at home (Australian Bureau of Statistics, 2018a).

After the project was made live on the platform, the participants were given four days to log in and respond to all the questions by typing in their answers directly next to each question. They were asked to answer using complete sentences and in as much detail as possible. The participants were not able to view other participants' details or their responses. However, I was able to review the responses in real time, allowing me to check that the participants understood what was asked of them and to respond to any questions or need for clarification that they might have had. Following completion, the participants were given a gift card worth AUD$60 as compensation for their time.

The thinking required of the participants included asking them to consider both how their data persona might be configured and used by themselves and others in the contemporary moment, and to project their imaginations into the future (10 and 20 years hence). The study began with a sensitizing question that asked the participants to list as many ways as they could think of in which information about them is collected, both digital and nondigital. They were then introduced to the concept of the data persona, provided with the definition, and asked a series of questions related to it. One of the key questions I wanted to address was the extent to which the participants know about and understand data profiling and related processes. I was also interested in investigating to what extent people value their data, as well as how much they care, in terms of protecting and preserving their data.

For the purposes of this article, I focus on the participants' responses to the following questions:

- Who can see or use your data persona? How can your data persona help or benefit you? How can it harm or disadvantage you?
- In 10 years' time, how can this data persona help or benefit you? How can it harm or disadvantage you?
- In 20 years' time, how can this data persona help or benefit you? How can it harm or disadvantage you?
- If there are personal data you want to keep into the future, how you can best preserve them (keep your own data from being lost, damaged, or stolen)? How can you protect your data from access by unknown or unauthorized others?

These questions were designed to elicit the participants' social imaginaries concerning their personal data in the context of the multi-dimensional nature of care: as affective engagements, the practices of routine labor to maintain and support the exigencies of everyday life, and as an ethico-political involvement (Braidotti, 2006; Puig de la Bellacasa, 2017). Thinking with more-than-human theory, I read through the participants' responses to the prompts and questions I gave them, looking at their descriptions of affective forces, relational connections, and agential capacities in the imaginaries they outlined. As such, these responses can be characterized as "imaginaries of care" (Puig de la Bellacasa, 2017, p. 220) as they relate to people's personal data.

Findings

Imaginaries of Data Profiling

The participants' accounts commonly highlighted what they imagine to be the continual personal datafication and dataveillance that operate in their everyday lives. They were able to list many ways in which personal data are generated from their online interactions. People were particularly knowledgeable about the ways in which their data are collected by social media companies (especially Facebook); Google; online retailers; online services such as travel booking; and government agencies such as the tax office, immigration, and national health service. As participant Paul commented,

> Information is relayed back to companies from God knows what cookies that have been placed on my devices. Information is also gathered from my voluntary inputs into websites and by purchasing from aggregators of information. Location is gathered from my device reporting its position and relayed by tracking cookies. The sky (or should that be cloud) is the limit! Whatever I input, search and research, go to and purchase is available for collection. Whatever I do on my device can be captured in one way or another. So the only information not available will be the things I do offline.

It is notable, however, that most participants challenged the idea that data profilers know everything about them. Most people thought that most dimensions of their "real selves" remain protected from the egresses of datafication and dataveillance, as Paul said, "The things I do offline." In the participants' imaginaries, their data personas are only limited representations of their selves. The participants argued that data profilers would only know the most superficial aspects of their selves and their activities: Important aspects of their "real" selves, such as their biography, secret thoughts and spirituality could not be accessed, as they are kept hidden from data profilers. As Monica contended, "Data profilers don't have full access to the inner workings of the mind," and Michelle suggested that "data profilers don't know who I am as a person and what my life experiences have done to shape me." The affordances of human–data assemblages, in these imaginaries, are limited to the kinds of information that are externalized from the human body/self during interactions online or using mobile devices.

Current Benefits and Harms of Data Personas

The participants could identify many ways in which their data personas could currently help them. They referred above all to the convenience offered by their personal data being collected and algorithmically processed by third parties. It was noted by the participants that their data personas could be used to make decisions on their behalf and therefore save them time. For example, their data personas could help them find jobs, be used for self-monitoring, and provide people with tailored special offers or discounts and targeted advertising. Alessandra said,

> Government offices such as ATO [Australian Taxation Office], public transport, Medicare, etc. Universities, private doctors, pharmacies, retail stores, etc. use my data persona. They can send latest updates, changes, reminders, courses, special promotions, etc. I think it could be a help and benefit for myself as it will save time instead of having to research these products or services. There are no disadvantages or harms at all, as long as it is not intrusive, and we are able to unsubscribe.

People pointed out that digitized information about them from various sources could be brought together in different services, allowing for greater personalization and customization. For example, Jo described the ways in which third-party use of her personal data helps her by targeting relevant advertising and offers to her and providing business or employment opportunities:

> I think data profiling can benefit me in being shown things I might like based on my data persona—for example, Facebook ads linked to things I have searched in my browser through cookies. It can also benefit me by businesses such as utility companies offering me better deals. LinkedIn is a way people can find me in a business capacity and know a lot about my qualifications and work experience. I can be searched for by my career and have had recruiters target me—so if I was after a new job, this would be a benefit.

Some people also highlighted the possibilities of data personas to facilitate better self-knowledge as well as offer opportunities for others to learn more about them:

> My data persona is a fun but unnecessary tool for self-evaluation. It does make finding jobs helpful, as people can discover me and make evaluations on my abilities to an extent that I can control. I enjoy being able to quantify my days and make some objective evaluations, but it's equally possible to do this without a data persona. (Mark)

On the negative side, some participants described examples when their data personas could potentially harm them. These examples typically outlined hypothetical situations in which people's personal information is subject to misuse, involving hackers exploiting information for their own purposes, scams, or identity fraud. As Emily put it,

> My data persona can harm me, as this information could fall into the wrong hands—such as hackers who could use my personal info for gain such as making fake Facebook profiles or spreading [computer] viruses. If a total stranger who is up to no good can access my personal information, they could impersonate me to steal money, get fake IDs, and do things illegally, that could in turn land me in a lot of trouble.

However, these scenarios were for the most part described as potential risks that could happen to other people. Few participants gave examples of personal experience of these types of personal data misuse. Their general lack of concern is encapsulated in Jo's response:

> I guess there is some harm in that I am not anonymous, but honestly, I don't really worry about it. The only thing I am concerned about is unsavory characters knowing where my children go to school or where we live. But we talk about cyber safety all the time with our children, so we are mitigating the risk as much as we can.

In contrast, the participants were readily able to describe their experiences of feeling annoyed by pestering from advertisers using targeted advertising or the feeling that agencies are using their data personas to make decisions on their behalf:

> My data persona can be a disadvantage, as this also means advertisers can target me for things I don't need but may want, or they expose me to things I didn't know I want but now I do, so I spend more money on things I don't actually need. (Bronwyn)

At a more abstract level of concern, some participants said they are worried that if taken to the extreme, data profiling could limit human agency and creativity, reveal too much of the hidden self, or dehumanize people by treating them only as customers. Jack and Kate explained it this way:

> Possible harms are limited creativity and freedom of thought. Constraining us as individuals. Removes human element from decision making—less reliance on spiritual and emotional. (Jack)

> A harm could be that you are treated like you are just a consumer, not a person. No room to feel free to be who you truly are, as there may be a chance that if you do or say something wrong, it exists in this database forever and could possibly be used against you. (Kate)

These kinds of responses articulate imaginaries that go beyond personal data privacy concerns. They surface concerns that go to the heart of how humanness and selfhood are imagined and defined. As Jack's response suggests, his concept of selfhood and humanness privilege attributes of creativity, freedom of thought, the spiritual, and the emotional. He imagines that data profiling could constrain these elements of people's humanity. For Kate, data profiling could limit selfhood and freedoms by defining people simply in terms of what kind of consumer they are calculated to be. Furthermore, people's capacity for self-expression could potentially be limited by their awareness that digitized information is long-lasting and could be accessed by others to make judgments about them.

In these imaginaries, data profiling is positioned as partial, selective, constrictive, and dehumanizing. The potential loss of connection with others was raised by Mark. He noted that if people such as employers were able to access personal data profiles, this might result in discrimination based not on face-to-face assessments of people's competencies, but on potentially flawed automated decision making:

> It harms you because it displays your life to strangers. These people and businesses do not know you. They do not deserve to know you and your fears. In terms of employment, your weaknesses should not be displayed or questioned from a computer analysing data points, but rather a person who interacts with you and gets to know you. It could lead to people feeling inferior and unstable and contribute to declines in social interaction and connection.

In this imaginary, Mark is drawing a distinction between what can be known about people from their online engagements compared with face-to-face encounters. According to him, digitized information and decision making cannot replace the deeper insights offered by knowing someone through developing an in-person relationship over time.

Benefits and Harms of Data Personas in the Future

In responding to a question about future benefits or harms of data personas, the participants imagined scenarios in which better customization and personalization could improve online services. They suggested that businesses and retailers would be able to more accurately target advertising and sell more goods, while government agencies could generate better information on citizens for development, planning, and to deliver better services:

> I think it would be used for making decisions about infrastructure—schools, hospitals, transport, etc. This would be beneficial because it would mean that money was spent in areas of high growth, etc. (Michaela)

> In 10 years, data profilers could save our time by looking for a product or searching the best possible prices or matches, so it will be easier for us to find, buy, or choose a product, meaning a win-win for both parties with mutual benefits. (Alessandra)

The possibilities of future digital assistants drawing on people's data were outlined by several people. For example, Maria outlined an imagined future in which data profiling could be customized to help her with caring for herself and her family:

> I could log into a certain online system, greeted by a virtual version of myself. It would know what groceries I buy regularly, when I'm due for my next health check-up, dental appointment, haircut, etc. When I need to refuel my car, do an oil check, book a service, etc. My persona would be more family-focused featuring details about my children and spouse to manage responsibilities, like the above, seamlessly.

Mark imagined a future in which people looking for work and their prospective employers could both use profiling software to work in their best interests:

> I think employers in the future will be able to know exactly which candidate from a bucket of 50 they want for the position, not based on their previous skills and employment, but from their interests and personality, which will be derived from a whole heap of different data points stored online. Data can help you in this instance because it can save you time, money, and effort.

These imaginaries outline datafication and dataveillance futures that present a largely utopian ideal of more and better personal data being used for improving services or targeted marketing. This is the imaginary of "surveillance as a service," as outlined by West (2019), in which people value the sense of intimacy and convenience generated from feeling "known" by a company.

Ways to Protect Personal Data

Most participants were able to outline an extensive array of practices that could be used to protect their data from unauthorized egress by others or from loss or deterioration. They referred mostly to the use of encryption and virus software, cloud computing services, making multiple back-ups, using external hard drives, and changing passwords. Several people were able to go into quite some detail about these practices. For example, Kerry explained the various approaches she could imagine using:

> I think the main way of protecting personal data is to have different passwords for everything and change these passwords regularly. Have virus protection software on your computer. Look for the secure icon on any website where you are going to enter your credit card details. Set privacy controls on Facebook.

Some participants, such as David, displayed high levels of technical knowledge. He outlined a complicated plan for protecting his personal data using numerous practices and devices, acknowledging the importance of remaining vigilant as digital devices and software changed or were compromised:

> To protect against intruders, you need to invest in encrypted cloud-based data storage systems or protected hardware such as retina or fingerprint protected hardware. This is a tricky question because there is no way to guarantee the retention of data. Kept in the cloud relies on companies such as Google or Amazon remaining viable and also depends on no acts of God wiping out a data center. I would tend towards storing information on physical media such as hard drives and SSD drives, but you would have to constantly update hardware and software as technology changes.

David mentioned using physical media rather than cloud-based software as a way of protecting his data. Some people took this idea even further, noting that they prefer keeping paper copies of their important information and feel that they could protect this more easily than digitized information stored in cloud computing. As Rose put it, "I think perhaps because of my age, I prefer hard copies of data rather than soft or cloud storage."

Other people mentioned the possibility of "never going online" (Sarah) to limit the volume of personal data available about them. Steve's idea was to "revert back to when everything was done manually. Therefore, I would record all my personal details in a diary/notebook." Some participants described practices involving avoiding specific apps or online interactions that they thought would generate too many sensitive data about them. Donna, for example, noted,

> I try to ensure that, wherever possible, only my family and friends have access to anything that I'd like to keep private. I don't put my GPS on unless I am lost and need to use Google Maps, I'm not a part of Facebook and don't put posts on any sites. I have deliberately chosen not to be a part of Facebook so a profiler would not know my friend list and should not have access to any photos of me.

Jay also outlined his strategies of avoiding going online too much to minimize the generation and use of his data by third parties: "I think the best way is to keep personal data to a minimum on social media, browsers, and search engines." Desmond, for his part, argued that into the future his data persona

> will contain data that is way out of date. I'm embarking on a mission to strictly control the amount of information out there about me and this means that in 20 years there should only be a skeleton picture of myself and my data.

Evident in these social imaginaries of protecting one's personal data, therefore, are careful practices that involve responsiveness to the lively nature of digital devices and personal data, but also their vulnerability. As noted earlier, the participants thought that datafication technologies are unable to know many of the most important aspects about them: those attributes that people consider most private and revealing of their selfhood. One way that this sense of protecting the real self from the dataveillance gaze is achieved is by engaging in practices of protecting their data. Another way is avoiding activities such as app or social media use that reveals their details to data profilers in the first place.

Discussion and Conclusion

I have argued in this article that adopting a more-than-human perspective on care in relation to personal digital data can challenge the reductionism and universalism that is often found in popular media reporting and scholarly analyses of datafication and dataveillance. Building on the idea of human–data assemblages as more-than-human, the theorizing of matters of care can begin to acknowledge the reciprocity and interdependency of these relations and agential capacities. Digitized caring practices, as outlined in the beginning of this article, are advocated as ways of improving and enhancing human lives. Adopting this perspective means we can begin to move toward the kind of decentering of human agency and highlighting responsiveness called for by more-than-human approaches to care. It can potentially reorient personal data's meaning from a technical and intangible phenomenon that can be difficult to conceptualize to an embodied phenomenon. It can begin to address the questions of how personal data come to matter (Lupton, 2018), and how we can care with and for our personal data.

The findings of the Data Personas study contribute to previous literature on publics' understanding and practices related to their personal data by thinking with these more-than-human perspectives. The research objective was not to identify whether participants held "informed" or "accurate" understandings. Any perspective will always be situated and acculturated as well as shaped by biographical experiences. Rather, I was interested in the social imaginaries expressed by the participants in their responses, and the ways in which they imagined they were living as data subjects. Using the stimulus of the "data persona" worked to engage participants in acts of imaginative responsiveness, considering the benefits and harms of becoming data subjects, and how and why (or indeed, whether) they should protect their data personas.

The findings suggest that just as human–data assemblages are emergent, lively, and nomadic, so too are the concepts and relations of care concerning them. The participants were able to respond attentively to the data persona stimulus and the questions they were asked. Positioning data profiling and related algorithmic processing in this way was able to generate some unexpected findings. The participants recognized and acknowledged the intra-actions and capacities generated by the affordances of datafication and dataveillance. They imagined a plethora of ways in which third parties could process and use their digitized information, both in the present and into the future. They also described practices of caring for their personal data to protect them from deterioration or unauthorized access to details they wanted to keep private. However, for the most part, the participants expressed little concern about any negative impacts on their lives or identities of these practices. This is because they positioned themselves to a large extent as exerting and maintaining the capacity to control their personal data.

Similarly, most people imagined futures in which there would be expanded datafication of people's lives and activities. These practices were viewed as leading to better personalization and customization of services. Some participants expressed concern about the partial nature of data profiling, and the potential for human agency, relational connections, and understandings of each other to be undermined by algorithmic-processing practices. For the most part, however, and similar to the findings of studies conducted in Finland (Ruckenstein & Granroth, 2020) and Denmark (Lomborg & Kapsch, 2019), there was little sense from these Australian participants' responses that they feel threatened by and vulnerable to third-party use of their personal data or by data profiling systems. They are aware of obvious uses of their personal data by companies such as Facebook and Google to target them for advertising but view these practices as mostly useful and convenient. Participants said they view data profiling by agents who create and use their data personas as providing helpful services such as better targeted advertising, special offers, improved government services, or access to employment opportunities, thereby facilitating rather than preventing access to opportunities. Although these participants recognized that their personal data profiles could potentially be used for illegal purposes such as identity theft, they did not envisage scenarios involving restriction of their life opportunities. In their imaginaries, the very liveliness and dynamic nature of these data assemblages mean that they are not seen as anything more than superficial and limited and that third-party use is equally constrained.

It is notable that these imaginaries do not correspond to the universalizing dystopian visions of datafication and dataveillance put forward in the popular media and in some of the academic literature. However, this apparent "lack of care" does not suggest conformance to the apathy or resignation to dataveillance that some researchers have identified among people in the United States (Draper & Turow, 2019; Hargittai & Marwick, 2016). Nor is this response the kind of defensive strategy of avoiding confronting the imagined controlling agencies of dataveillance that Ellis (2020) found in his English participants. Rather, this imaginary of care stemmed from these Australian participants' convictions that the key elements of their identities—and particularly what makes them unique and human—have resisted digitization. For the large part, these participants view their data personas as only very partial or superficial representations of their "real" selves. Although the participants acknowledged the existence of a distributed body/self, as represented in their data profiles, they were reluctant to relinquish the idea of the inherent, closed off, non-mediated body/self that they believe resides in the non-datafied spaces of their lives, and particularly inside their individuated bodies. In this imaginary, rather than data personas representing the "projected interior" of selfhood (Goodings & Tucker, 2014, p. 39), they are conceptualized as merely surfaces. The "mining" of selfhood and embodiment that takes place from digital traces can only go to a limited depth, according to these imaginaries.

The participants in my study demonstrated little knowledge or concern about data inequities. Few of them pointed to any ways in which already disadvantaged people may be further marginalized by data profiling, despite the high levels of news media attention given to the robo-debt event, for example, and to Snowden's revelations several years prior to the study. These are different responses from those elicited in other studies, such as Dencik and Cable's (2017) focus group and interview study with British participants soon after the Snowden events. Dencik and Cable reminded their participants about Snowden's revelations before engaging in discussions and interviews, so it is perhaps not surprising that their participants appeared more concerned about and resigned to dataveillance than were my participants. Using the data persona approach, I would argue, allowed my participants to draw on their own knowledge and experiences of data profiling rather than sensitizing them to specific data breaches or misuses such as those revealed by Snowden or any other scandal that received high levels of mass media attention. I deliberately did not ask or remind them about these events precisely because I wanted to see to what extent the participants might spontaneously bring them up in their responses to the more general questions that I asked them.

The location of these participants in Australia and their relative socioeconomic advantage underpin their attitudes and experiences related to their data personas. The people in my study did not recount the same kinds or degree of experiences of stigmatization, exploitation, racism, or other forms of social discrimination and restriction of their lives by datafication and dataveillance as some of the more disadvantaged groups that have been included in other studies such as the U.S.-based "Data Bodies" project (Petty et al., 2018). Few of my participants had experienced (at least to their knowledge) the kinds of threats and harms suffered by disadvantaged people in countries such as the United States, where data profiling has a far greater impact on the everyday lives of citizens. The respondents said that they are aware of potential harms such as identity fraud, but they did not report direct experience or knowledge of these events or any other illicit use of their data. These findings reflect the Australian Bureau of Statistics' latest figures from representative surveys of Australian households in 2016–2017, which found a very low incidence of respondents reporting experiences of their personal data being misused. Only one in 20 respondents reported experiencing "abuse of personal information" (Australian Bureau of Statistics, 2018b).

Acknowledging the relative socioeconomic privilege of my participants, the next step in building on these findings is to conduct further research that targets social groups in Australia that are less advantaged and more marginalized. It is likely that members of such groups will have very different life experiences of datafication and dataveillance. For example, Indigenous Australians, along with other Indigenous and First Nations peoples worldwide, have been calling for the decolonizing of Indigenous data and for data sovereignty, allowing them greater control over the types of data that are collected about them (in any form, digital or non-digital) and the ways in which they are used (Kukutai & Taylor, 2016). Further detailed research is called for that addresses how people from different socioeconomic backgrounds and geographical locations care about and for their data personas and the implications of how datafication and dataveillance can both open and restrict agential capacities.

References

Andrejevic, M. (2014). The big data divide. *International Journal of Communication, 8*, 1673–1689. Retrieved from http://ijoc.org/index.php/ijoc/article/view/2161

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

Australian Bureau of Statistics. (2018a). *Census reveals a fast changing, culturally diverse nation.* Retrieved from http://www.abs.gov.au/ausstats/abs%40.nsf/lookup/Media%20Release3

Australian Bureau of Statistics. (2018b). *Household use of information technology, Australia, 2016–17.* Retrieved from https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12016-17?OpenDocument

Barad, K. (2007). *Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning*. Durham, NC: Duke University Press.

Bawaka Country, Wright, S., Suchet-Pearson, S., Lloyd, K., Burarrwanga, L., Ganambarr, R., . . . Djawundil, Maymuru, D. (2015). Working with and learning from Country: Decentring human author-ity. *Cultural Geographies, 22*(2), 269–283. doi:10.1177/1474474014539248

Bennett, J. (2009). *Vibrant matter: A political ecology of things*. Durham, NC: Duke University Press.

Braidotti, R. (2006). *Transpositions: On nomadic ethics*. Cambridge, UK: Polity Press.

Braidotti, R. (2019). A theoretical framework for the critical posthumanities. *Theory, Culture & Society, 36*(6), 31–61. doi:10.1177/0263276418771486

Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology, 27*(2), 91–121. doi:10.1093/ijlit/eay017

Bucher, T. (2018). *If . . . then: Algorithmic power and politics*. Oxford, UK: Oxford University Press.

Cheney-Lippold, J. (2018). *We are data: Algorithms and the making of our digital selves*. New York: New York University Press.

Clarke, R., & Greenleaf, G. (2018). Dataveillance regulation: A research framework. *Journal of Law and Information Science, 25*(1). Retrieved from https://www.scribd.com/document/371829503/Dataveillance-Regulation-A-Research-Framework-Roger-Clarke-and-Graham-Greenleaf#fullscreen=1

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 20*(4), 336–349. doi:10.1177/1527476418796632

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763–781. Retrieved from https://ijoc.org/index.php/ijoc/article/view/5524/1939

Dijck, J. van. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208. doi:10.24908/ss.v12i2.4776

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839.

Ellis, D. (2020). Techno-securitisation of everyday life and cultures of surveillance-apatheia. *Science as Culture*, *29*(1), 11–29*.* doi:10.1080/09505431.2018.1561660

Frank, M., Walker, J., Attard, J., & Tygel, A. (2016). Data literacy—What is it and how can we make it happen? *Journal of Community Informatics, 12*(3). Retrieved from http://www.ci-journal.net/index.php/ciej/article/view/1347

Goodings, L., & Tucker, I. (2014). Social media and the co-production of bodies online: Bergson, Serres and Facebook's timeline. *Media, Culture & Society, 36*(1), 37–51. doi:10.1177/0163443713507813

Haraway, D. (2015). Anthropocene, Capitalocene, Plantationocene, Chthulucene: Making kin. *Environmental Humanities, 6*(1), 159–165. doi:10.1215/22011919-3615934

Haraway, D. (2016). *Staying with the trouble: Making kin in the Chthulucene*. Durham, NC: Duke University Press.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737–3757. Retrieved from http://ijoc.org/index.php/ijoc/article/view/4655/1738

Henman, P. (2019). Of algorithms, apps and advice: Digital social policy and service delivery. *Journal of Asian Public Policy, 12*(1), 71–89. doi:10.1080/17516234.2018.1495885

Jasanoff, S., & Kim, S.-H. (2013). Sociotechnical imaginaries and national energy policies. *Science as Culture, 22*(2), 189–196. doi:10.1080/09505431.2013.786990

Kennedy, H., & Hill, R. L. (2018). The feeling of numbers: Emotions in everyday engagements with data and their visualisation. *Sociology, 52*(4), 830–848. doi:10.1177/0038038516674675

Kukutai, T., & Taylor, J. (Eds.). (2016). *Indigenous data sovereignty: Towards an agenda*. Canberra, Australia: Australian National University Press.

Kwek, D. H. B. (2018). The importance of being useless: A cross-cultural contribution to the new materialisms from Zhuangzi. *Theory, Culture & Society, 35*(7–8), 21–48. doi:10.1177/0263276418806381

Lee, Y.-S., Sakuno, S., Prebensen, N., & Kimura, K. (2018). Tracing Shintoism in Japanese nature-based domestic tourism experiences. *Cogent Social Sciences, 4*(1). Retrieved from https://www.tandfonline.com/doi/full/10.1080/23311886.2018.1446671

Lomborg, S., & Kapsch, P. H. (2019). Decoding algorithms. *Media, Culture & Society*. Advance online publication. doi:10.1177/0163443719855301

Lupton, D. (2017). Feeling your data: Touch and making sense of personal digital data. *New Media & Society, 19*(10), 1599–1614. doi:10.1177/1461444817717515

Lupton, D. (2018). How do data come to matter? Living and becoming with personal data. *Big Data & Society, 5*(2). Retrieved from https://journals.sagepub.com/doi/full/10.1177/2053951718786314

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

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2). Retrieved from http://bds.sagepub.com/content/1/2/2053951714541861

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*(1), 53–125.

Martin, A., Myers, N., & Viseu, A. (2015). The politics of care in technoscience. *Social Studies of Science, 45*(5), 625–641. doi:10.1177/0306312715602073

Milan, S., & Treré, E. (2019). Big data from the south(s): Beyond data universalism. *Television & New Media, 20*(4), 319–335. doi:10.1177/1527476419837739

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

O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. London, UK: Penguin Books.

Petty, T., Saba, M., Lewis, T., Gangadharan, S. P., & Eubanks, V. (2018). *Reclaiming our data.* Retrieved from https://www.odbproject.org/wp-content/uploads/2016/12/ODB.InterimReport.FINAL_.7.16.2018.pdf

Puig de la Bellacasa, M. (2017). *Matters of care: Speculative ethics in more than human worlds*. Minneapolis: University of Minnesota Press.

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

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24. doi:10.1080/17530350.2019.1574866

Sadowski, J. (2020). *Too smart: How digital capitalism is extracting data, controlling our lives, and taking over the world*. Cambridge, MA: MIT Press.

Taylor, C. (2004). *Modern social imaginaries*. Durham, NC: Duke University Press.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society, 4*(2). Retrieved from https://journals.sagepub.com/doi/full/10.1177/2053951717736335

Todd, Z. (2016). An Indigenous feminist’s take on the ontological turn: “Ontology” is just another word for colonialism. *Journal of Historical Sociology, 29*(1), 4–22. doi:10.1111/johs.12124

Wernimont, J. (2019). *Numbered lives: Life and death in quantum media*. Cambridge, MA: MIT Press.

West, E. (2019). Amazon: Surveillance as a service. *Surveillance & Society, 17*(1/2), 27–33. doi:10.24908/ss.v17i1/2.13008