Back Cover

This book provides an empirical and philosophical investigation of selftracking practices. In recent years, there has been an explosion of apps and devices that enable the data capturing and monitoring of everyday activities, behaviours and habits. Encouraged by movements such as the Quantified Self, a growing number of people are embracing this culture of quantification and tracking in the spirit of improving their health and wellbeing.

The aim of this book is to enhance understanding of this fast-growing trend, bringing together scholars who are working at the forefront of the critical study of self-tracking practices. Each chapter provides a different conceptual lens through which one can examine these practices, while grounding the discussion in relevant empirical examples.

From phenomenology to discourse analysis, from questions of identity, privacy and agency to issues of surveillance and tracking at the workplace, this edited collection takes on a wide, and yet focused, approach to the timely topic of self-tracking. It constitutes a useful companion for scholars, students and everyday users interested in the Quantified Self phenomenon.

Btihaj Ajana is Associate Professor and Marie Curie Fellow at Aarhus Institute of Advanced Studies, Denmark. She is also a Senior Lecturer at the department of Digital Humanities, King's College London. Her academic work is interdisciplinary in nature, spanning areas of digital culture, media praxis, and biopolitics. She is the author of Governing through Biometrics: The Biopolitics of Identity (Palgrave Macmillan, 2013).

palgrave
macmillan

Spine

Edited by
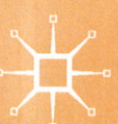Btihaj Ajana

Self-Tracking

palgrave▸pivot

Front Cover

palgrave▸pivot

SELF-TRACKING

Empirical and Philosophical Investigations

Edited by Btihaj Ajana

Taylor, Phil, and Peter Bain. 1999. "An Assembly Line in the Head": Work and Employee Relations in the Call Centre. *Industrial Relations Journal* 30 (2): 101–117.

Thompson, P., and S. Ackroyd. 1995. All Quiet on the Workplace Front? Critique of Recent Trends in British Industrial Sociology. *Sociology* 29: 615–633.

CHAPTER 8

Data Privacy: Users' Thoughts on Quantified Self Personal Data

Keith Spiller, Kirstie Ball, Arosha Bandara, Maureen Meadows, Ciaran McCormick, Bashar Nuseibeh and Blaine A. Price

Abstract The logging of personal data has been shown to offer many benefits for those wanting to, for example, get fitter, get stronger or get to know themselves better. In this chapter, we concentrate on the privacy values attributed to Quantified-Self (QS) data. Using evidence taken from research interviews, this chapter reviews privacy in relation to personal data and offers an empirical perspective on how QS users view and value the data they collect, and often display publically, as well as their

K. Spiller (✉)
Birmingham City University, Birmingham, UK
e-mail: Keith.Spiller@bcu.ac.uk

K. Ball
St. Andrews University, St Andrews, UK

A. Bandara · C. McCormick · B. Nuseibeh · B.A. Price
Open University, Milton Keynes, UK

M. Meadows
Coventry University, Coventry, UK

attitudes towards the handling of their data by QS device manufacturers. We question appreciations of privacy in QS data and elaborate on how users value their QS privacy.

Keywords Self-tracking · Quantified Self · Personal data · Privacy

Introduction

In this chapter, we draw from research interviews with two groups of Quantified Self (QS) users and examine their understanding of the privacy of their data. The premise of our enquiry centres on how users volunteer data to QS devices, shared platforms and to the manufacturers of the devices. The goal of QS is often to allow users to improve on aspects of their lives and ultimately to get to know themselves better. The data also allow device manufacturers and third parties to 'get to know' users—for instance, how often a user goes for a run, how well they sleep, how many calories they eat or when they menstruate. QS data contain intimate details of users' lives and their activities, and Solove (2006) makes a convincing argument for considerations for data privacy of this kind; particularly how it is collected, processed, disseminated and scrutinised. Indeed privacy, as we understand it, is a personal expectation based on the fact that everyone is free to avoid unwanted attention (Wilkins 1987). The use of QS data presents a challenge because QS companies sell data to third parties, as well as use the data to their own advantage (Olson 2014a, b; Advisory 2014; Schumer 2015). These companies do offer assurances. To cite one example, Fitbit offers a Privacy Pledge—which is representative of the terms and conditions provided by other device manufacturers—giving the assurance, 'We will never sell your data, and will only share personally identifiable data when you direct us to'. The pledge later states, 'Fitbit may share or sell aggregated, de-identified data that does not identify you' and later still attests, 'If it is necessary in connection with the sale, merger, bankruptcy, sale of assets or reorganization of our company, your PII [personally identifiable information] can be sold...' (Fitbit 2016). The final comment does go on to explain that if the company is sold, they will insist on the purchasing company, maintaining the privacy pledge as outlined here; however, the wording of the Pledge presents some ambiguity as to how users can understand and appreciate

the ownership of their QS data. In digital contexts, aspects such as PII can include name, address, date of birth, credit card number or QS data (Boyd 2014), and these are the building blocks of digital communications, transactions and QS. It is this information that smooths the transfer of data, allows users to participate in QS and also allows manufacturers to extract value from the data. Privacy in these circumstances is often an assumed and unquestioned privilege, one enjoys apathetically. Indifferent views such as 'I have nothing to hide, so therefore nothing to fear', Solove (2006; 2007) has argued, translates as 'I don't care what happens, so long as it does not happen to me'. And this sentiment, we contend, may be evident in the views of QS users. In what follows, we question how QS users view and value the data they collect and often display publicly, as well as their attitudes towards the handling of their data by QS manufacturers.

Bettering Oneself

The QS literature has tended to focus on improvements enabled by data, as well as the technological developments of QS devices (Swan 2012; Till 2014). Key focuses amongst this work have been on efficiency, betterment and motivational practices (Suel 2013; Swan 2013); emphasis often centres on taking control of health, fitness, calorie intake, etc. Indeed, the collection and management of personal data have promoted work on QS data as a form of self-responsibilisation—a term taken from New Labour's modernistic agenda to empower local governments to make their own informed decisions (Barnett 2003). Pressing in this QS work are aspects of neoliberal responsibilisations, for example, a liberal economy model favouring privatisation, de-regulation and fiscal austerity that aids the growth of the economic market (Whitson 2013; Moore and Robinson 2015). One does not have to look far to see how responsibilisation is being incentivised in QS terms, for instance, tracking food intake to aid weight loss or tracking activities to generate better habits (Davenport 2015). Or, in medicine, patients monitoring their own symptoms at home rather than being monitored by professionals in hospital (Farmer et al. 2007; Carter 2015). Moreover, insurance companies now encourage users to share QS personal data, because an accurate indication of customer activities and lifestyle choices can help to customise policies (see Newman 2014; Shemkus 2015).

Alongside such motivational processes, the collection and use of QS data are taking increasingly diverse forms. For instance, sexual health has been quick to embrace the many potentials of self-tracking, and critical enquiry has presented some very insightful commentary on issues of conception and sexual performance (Lupton 2013, 2014, 2016). A male user, for instance, typically records performance, such as duration or frequency of activity and follows a distinctly competitive or comparative agenda. Whereas, female QS recording tends to concentrate on reproduction, ovulation, menstruation—responses focal to bodily functions, sensations and rhythms. Lupton (2016, 2015) argues that the juxtapositions and tensions, evident in moments of quantifying bodily functions, perform an ordering of the 'dis-ordered' body. QS goals and their attainment move towards cultivating homogenous standards of, for instance, body shapes or bodily performances (Lupton 2013). Equally, continuously recording activities may hinder enjoyment or spontaneity. Neither the body or the self can be fully extrapolated from the data, and an over-reliance on the power of the data may affect internalised norms, personal understanding, habitualisation of use, the standardisation of data sets and so on (Gilmore 2015; Schüll 2016).

There is little doubt QS data provide many beneficial outcomes for users, particularly as a form of motivation or offering insights into personal knowledge (Suel 2013; Choe et al. 2014). The data produced are informative not least because they often play a distinctive role in knowledge creation (Ruckenstein and Pantzar 2015). 'Self-hacking' is a key term here and refers to how users analyse their own data, as well as how they amend behaviours because of their data. Incentives to hack often centre on desires to 'optimise' data, as individuals work to overcome lifestyle issues or knowledge gaps (Nafus and Sherman 2014). Collecting and visualising personal data in such a way present robust verification of the activities that may have happened and possibly those that need to happen. Other factors may also emerge, such as neuroticism and/or senses of belonging to a QS group as well as benefits of sharing with like-minded users (Choe et al. 2014). However, there are fissures evident in the literature, namely around QS data ownership and its use (Fuchs 2011; Adage 2013; Gao et al. 2014).

Privacy remains lightly analysed in the literature, especially when one considers the sensitive nature of some QS data (Gold 2015). For us, it is the ownership and privacy of this information that is of consequence. Selective issues concerning QS data have been considered; for

example, there has been some analysis on difficulties in gaining access to data (Fotopoulou 2014), how users can analyse data (Lukas 2014), the security and risks inherent in QS data (Barcena et al. 2014) and getting permissions of those whose data have been captured (Ye et al. 2014). Others emphasise how users can take control of their own data (Haddadi et al. 2013) or highlight the farming of data by large multinationals (Tene and Polonetsky 2013; Bland 2014; Newman et al. 2014). Where much of the work is strong is in the control, ownership and use of QS produced data (Swan 2012; Gurrin et al. 2014). However, as we argue there are ambivalences in the evaluations of privacy for those who participate in QS.

WATCHING VIDEOS AND TALKING TO USERS

Our empirical work began with viewing recorded talks from the London QS Meet-up. The talks are freely available online (http://vimeo.com/channels/londonqs), and we selected ten talks that gave a clear overview of QS users. The intention of the exercise was to gain a better understanding of those who practice QS. Findings from the videos not only helped to identify how users understood aspects of privacy but also presented to us further privacy questions. Therefore, we conducted ten semi-structured interviews: five high-frequency users were recruited from the London QS meet-ups. QS meet-ups provide monthly opportunities for users to share QS experiences (Butterfield 2012; Choe et al. 2014). During the meet-ups, members present 10-minute talks on their experiences of collecting and using data. The format of the talks follows a standard practice, one replicated in QS meet-ups across Europe and North America, for example, members speak to three questions: (1) what did you do?; (2) how did you do it?; and (3) what did you learn? Talks vary widely, from the more frivolous (tracking the number of push-ups a person achieved in a year) to the medical (monitoring bodily function in relation to a cancer diagnosis). A keen function of the discussion is often the lack of clarity provided by off-the-shelf forms of measuring, and the QS meet-ups, to some degree, rally against baselines or presumed averages in delivering personalised and bespoke readings of what users may be attempting to achieve.

In addition, five 'less' enthusiastic QS users were interviewed, the only stipulation here was that these participants had not been involved in the London meet-ups and must have been collecting their personal data

for a period of 6 months or more. Recruitment of this group stemmed from personal contacts (friends/colleagues/family) of research team members. The gender make-up of the high-frequency group comprised of males and the low-frequency group comprised of three females and two males. This was not selective, but rather interviews were conducted with those who responded quickest to our requests for participants. The interviews took place in coffee shops or places of convenience for participants. All of these interviews were recorded and transcribed: eight of the interviews were conducted face-to-face and used a semi-structured approach; one interview was conducted over the telephone and followed the same semi-structured format. This was then written up immediately following the interviews. The final interview was conducted over email, where the respondent answered the eight questions that had formed the basis of the semi-structured approach.

QS Privacy

Key to our conversations with participants was their motives to betterment, and we begin by offering some context as to why users participate in QS. The ethos of the 'meet-up', for instance, followed a philosophy of self-hacking where problems were solved through the 'power of numbers'. If off-the-shelf devices, apps and programs did not offer clarity or a complete data set, users then sought to expand how they could analyse their data and add to it. High-frequency users tended to use their data more proactively and were keen to promote what they had found and how it could benefit other users. As the following high-frequency user states, there are many sources and varieties of data:

so I measure weight, body fat. Blood pressure I measure on a fairly regular basis. Glucose is the thing I think I measure the most frequently, and the most interested in at the moment. I… things and renal lactose threshold, lactate threshold, VO2max, dual heart rate analysis while I'm running, although not that much anymore. I didn't find it to be hugely valuable. Fitbit, I use just activity measurements. I was a really early adopter of that. Did that … quite liked it for quite a long time then I feel off it and I'm thinking about getting back. I have one on right now. (High frequency user, male, 41–50, HU1)

For this user, QS allows and encourages an array of opportunities to improve on fitness and bodily functions. Pressing here is an experimental sense of trying new technological developments to enhance data collection (Suel 2013). However, as the user hints, this may often be short-lived, due to the lack of value in the data or possibly in a drive to experiment with ever-newer devices. Whereas, for low-frequency users, they, more often than not, use the template provided by device manufacturers, for instance, using the Jawbone platform to review the miles they have cycled. However, low-frequency users were not averse to comparing data sets to establish patterns in their data. The following participant states:

At first it was enough to simply record the info, that made me make better decisions, what gets measured gets managed. Then I started correlating certain elements e.g. I was trying to save money so kept a record of every penny I spent. At the same time I was also logging my food and mood. I realised that when I thought I was just having the odd cup or two a day, I was having up to 4 cups a day and I was buying them for whoever was with me too and I was often (about 50% of the time) buying a cake with it too. So, it was far more expensive and unhealthy that I had presumed. But the real clincher was that because I was recording my mood too, I was able to correlate my mood and I realised that all this coffee was clearly tying-in with feelings of anxiety. All that caffeine was making me feel shit! So I gave up coffee as a result. That was actually my first proper period of QS'ing and was what fired me on to do more. (Low frequency user, male, 41–50, LU5)

The participant draws their own conclusion by effectively combining two sources of information and realising that these are causing anxiety and making him feel poorly. Again, it is an experimental approach, and without the data, formal connections may not be recognised. The term 'what gets measured gets managed' may also be useful, because it is only through the collection, visualisation and comparability of data that associations are established. However, considerations of who has access to these data, for the same user, are regarded positively. The user suggests there are altruistic motives to sharing their data:

My data is private. But there's nothing compromising in it either. It's not something I worry too much about. I personally believe that if the world was more open it would be a better place. (Low frequency user, male, 41–50, LU5)

Perhaps there is a contradiction in data being private and shared. The user suggests their personal data could make a contribution to large or national databases and help formulate national standards of, for example, the average weight and activity of a UK 50-year-old man living in London. The user did elaborate that he did not remember ever signing up for his data to be used in relation to Big Data, population data or in a more open way. Yet, an assumption remained that the data would be used in this way.

In other instances, QS data are visibly displayed and mapped, for example, highlighting running routes in a specific area (Map My Run 2016). Users' recordings of distance covered, time taken and location are shared publicly. The following participant expresses her appreciation of the GPS function on Fitbit:

Well, with Fitbit the location can be on and I keep the workout public. I think there are real advantages to being public. (Low Frequency user, female, 31–40, LU2)

In this instance, the user is content because advantages initiated by her public display include an indicator to friends of her fitness performance. The participant also expressed how her runs were linked to GPS and her friends could view the 'cool' places she was running—as her job often took her to various countries. Equally, she liked to see what her friends were doing on their runs, as they also provided through a manufacture website their GPS movements. Nevertheless, evident in the following quote are expressions of irritation particularly if data are compromised or misused:

I don't mind people seeing my data. There's actually nothing in there that would particularly personally identify me. What would annoy me is if somebody [companies] took that data and did something with it .... That would piss me off, yes, because they're already making money out of me. If I haven't agreed to them selling that data on and making more money out of it, they shouldn't be doing. (High frequency user, male, 41–50, HU3)

As those we spoke to suggest, the underlying predisposition for users is that there is little to be compromised in sharing the data. For most, the data are of little value other than the support they relay in terms of

what they were designed to do—i.e. measure the distance of a run or mood when drinking coffee. For these users, sharing data presents a clear benefit, be it learning about themselves from their data or exchanging data for the 'good' of others and themselves. The following participant elaborates:

I share everything. I don't care. I am happy, like Google takes everything from me. It has got all my geo tagging and everything, because I think that is actually going to benefit me. So I can then go back and look at things and know exactly where I've been. I might look at a Google map and it will show you everywhere you've been.... But by having all that data I figure it serves you better but I don't have problems telling people where I am... (Low frequency user, female, 21–30, LU1)

The participant draws on her data as a work tool, the data provide a historical record that can be accessed with relative ease, in this case highlighting the cafes and restaurants, this food blogger has visited (Crete-Nishihata et al. 2012; Bellodi et al. 2012). What privacy and sharing serve to highlight are some of the values placed on QS data. On the one hand, the value of the data is clear in providing memory data-banks or triggers to remember events. However, if manufacturers 'make money' from user data without explicitly stating the fact, then this may be contentious. Again, users suggest this is sanctioned through a belief that amalgamated data houses potential for betterment, and that organisations will protect the privacy of users:

The way I think about it is that your personal data is much more valuable when it can be compared to population data, and if I can contribute in some way to making that population data better, which is what I'm doing ... they [QS manufacturers] may be monetizing it in other ways ... They've got a business to run and I think that they will make their best efforts to make it anonymous. (High frequency user, male, 41–50, HU1)

Solove's (2007) sentiments of 'I don't care' or 'it won't happen to me' flavour users' comprehensions of digital privacy, and as we have seen, if users get to record their activities and QS companies use the data in anonymised ways or for the greater good, then it all appears to be acceptable.

CONCLUSION: MANAGING QS DATA

The overarching theme in QS is improvement as well as having evidence to support and encourage physical behaviours, disciplining attitudes, medical monitoring or solving problems (Schüll 2016). In addition, fun and enjoyment, or the ease of showing off run times and places to eat, are part of the attraction of using digital devices (Bauman et al. 2014). Within a Euro-Western context, there is a growing predisposition to share information online (Leon et al. 2013). Instantly sharing and communicating QS scores, achievements or events have become normative practices within online environs (Boyd 2014). However, when disseminating information, there are a number of ways privacy can be compromised, for example, 'information processing' and 'secondary use' of data, when information is used for a purpose different to that from which it was collected (Solove 2006). All of which can produce a betrayal of expectations and, as we have seen, would 'piss off' some participants. Sensitivities often focus on the control and maintenance of QS data by trusted organisations and the owner of the data. Sharing QS data can include posting results on social media, giving medical staff your data or allowing the manufacturers of the devices the power to extract and use data. Despite the core motivations of users for self-improvement, there is an ambiguity as to how personal information is managed and utilised. The information for the most part is viewed with a casual demeanour and often expressed in terms of 'there's nothing compromising in it', which may suggest privacy is valued and understood. But QS data because of their low sensitive or restricted compromising potentials pose few difficulties. Nevertheless, what if, QS data were used to determine access to medical care for individuals or to limit the choices available to users, as it has been for some employees in US organisations (Newman 2014). Equally, what if, QS data were used to verify a person's whereabouts in a murder case (Scott 2015) or undermine claims of assault (Gutteridge 2015). What then?

As we have found, the advantages of openness have been expressed particularly in relation to how large anonymised data sets can be productive when highlighting, for example, health trends or competitive performance. There is also a clear indication that QS devices and QS data are facilitators in meeting the original goals and aspirations of users—i.e. collating the activities of users. Beyond its immediate use, it would appear QS data hold little value; how manufacturers or even law enforcement

(Scott 2015) use QS data is not a privacy concern for users. The experiences of the QS users, in this chapter, highlight how privacy is understood and valued. Clearly, there is an awareness of privacy, but much like Solove's observations, users are content to provide data to QS manufacturers and third parties. The premise of 'I have nothing to hide, nothing to fear' continues.

REFERENCES

Adage. 2013. Why Marketers Should Care About the Quantified Self. http://adage.com/article/glossary-data-defined/marketers-care-quantified/243840. Accessed 11 Feb 2016.

Advisory. 2014. Love your Fitbit? Be warned: Companies sell your data. https://www.advisory.com/daily-briefing/2014/04/23/love-your-fitbit-be-warned-companies-sell-your-data. Accessed 13 Jan 2017.

Barcena, Mario B., Candid Wueest, and Hon Lau. 2014. *How Safe is Your Quantified Self?*. Mountain View, CA: Symantec.

Barnett, Neil. 2003. Local government, New Labour and 'Active Welfare': A Case of 'Self Responsibilisation'? *Public policy and Administration* 18 (3): 25–38.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, and David Lyon. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8 (2): 121–144.

Bellodi, Luca, Radu Jasinschi, Gerard De Haan, and Murtaza Bulut. 2012. Dialogue support for memory impaired people. In *Signal & Data Processing Association Annual Summmit and Conference* (APSIPA ASC), 1–4, Asia-Pacific.

Bland, Jessica. 2014. *Refilling The Innovators Prescription: The New Wave of Medtech*. Silicon Valley comes to the UK Series. Nesta.org.uk.

Boyd, Danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. Boston: Yale University Press.

Butterfield, Adam D. 2012. *Ethnographic Assessment of Quantified Self Meetup Groups*. Unpublished Doctoral dissertation, San José State University.

Carter, Eric D. 2015. Making the Blue Zones: Neoliberalism and Nudges in Public Health Promotion. *Social Science and Medicine* 133: 374–382.

Choe, Eun K, Nicole B. Lee, Bongshin Lee, Wanda Pratt and Julie A. Kientz. 2014. Understanding Quantified-Selfers' Practices in Collecting and Exploring Personal Data. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*: pp. 1143–1152.

Crete-Nishihata, Masashi, Ronald M. Baecker, Michael Massimi, Deborah Ptak, Rachelle Campigotto, Liam D. Kaufman, Adam M. Brickman, Gary R. Turner, Joshua R. Steinerman, and Sandra E. Black. 2012. Reconstructing the Past: Personal Memory Technologies are not Just Personal and not Just for Memory. *Human-Computer Interaction* 27 (1–2): 92–123.

Davenport, Barrie. 2015. Quantified Self: 10 Ways Lifelogging Improves Your Quality Of Life. *LiveBoldandBloom*. http://liveboldandbloom.com/09/productivity/quantified-self-lifelogging#sthash.ReclLlNI.dpuf. Accessed 21 Nov. 2007.

Farmer, Andrew, Alisha Wade, Elizabeth Goyder, Patricia Yudkin, David French, Anthea Craven, Rury Holman, Ann-Louise Kinmonth, and Andrew Neil. 2007. Impact of Self Monitoring of Blood Glucose in the Management of Patients With Non-Insulin Treated Diabetes: Open Parallel Group Randomised Trial. *BMJ* 335 (7611): 132.

Fitbit Privacy Policy. 2016. http://www.fitbit.com/uk/privacy. Accessed 16 Jan 2016.

Fotopoulou, Aristea. 2014. The Quantified Self Community, Lifelogging and the Making of 'Smart' Publics. *Open Democracy*. https://www.opendemocracy.net/participation-now/aristea-fotopoulou/quantified-self-community-lifelogging-and-making-of-%E2%80%9Csmart%E2%80%9D-pub. Accessed 17 Nov 2015.

Fuchs, Christian. 2011. Web 2.0, Prosumption, and Surveillance. *Surveillance and Society* 8 (3): 288–309.

Gao, Yue, Fanglin Wang, Huanbo Luan, and Tat-Seng Chua. 2014. Brand Data Gathering From Live Social Media Streams. In *Proceedings of International Conference on Multimedia Retrieval* ACM, pp. 169–174.

Gilmore, James N. 2015. Everywear: The Quantified Self and Wearable Fitness Technologies. *New Media and Society* 18 (11): 2524–2539.

Gold, Ashley. 2015. Would You Tell Apple When You've Had Sex? BBC. http://www.bbc.co.uk/news/technology-33291119. Accessed 11 Feb 2016.

Gurrin, Cathal, Rami Albatal, Hideo Joho, and Kaori Ishii. 2014. A Privacy by Design Approach to Lifelogging. *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*. Berlin: IOS Press.

Gutteridge, Nick. 2015. Woman Accused of False Rape Claim After Fitness Watch Proved She Wasn't Dragged From Bed. *Express*. http://www.express.co.uk/news/world/587899/Woman-accused-false-rape-claim-Fitbit-fitness-watch-proved-not-dragged-from-bed. Accessed 15 Jan 2017.

Haddadi, Hamed, Richard Mortier, Derek McAuley, and Jon Crowcroft. 2013. Human-data interaction. Technical Report no. 837, Computer Laboratory, University of Cambridge.

Leon, Pedro Giovanni, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. What Matters to Users?: Factors That Affect Users' Willingness to Share Information With Online Advertisers. *Proceedings of the ninth symposium on usable privacy and security*.

Lukas, Andrea. 2014. The Self in Quantified Self. Paper presented at JRC workshop, March 2014, Ispra Italy.

Lupton, Deborah. 2013. Understanding the Human Machine. *Technology and Society Magazine* 32 (4): 25–30.

———. 2014. You are Your Data: Self-Tracking Practices and Concepts of Data. http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2534211. Accessed 15 Jan 2016.

———. 2015. Quantified Self: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps. *Culture, health and sexuality* 17: 4440–4453.

———. 2016. *The Quantified Self: A Sociology of Self-Tracking*. Cambridge: Polity Press.

Map My Run. 2016. http://www.mapmyrun.com/gb/. Accessed 12 May 2016.

Moore, Phoebe, and Andrew Robinson. 2015. The Quantified Self: What Counts in the Neoliberal Workplace. *New Media and Society* 18 (11): 2774–2792.

Nafus, Dawn, and Jamie Sherman. 2014. Big Data, Big Questions This One Does Not Go Up To 11: The Quantified Self Movement as an Alternative Big Data Practice. *International Journal of Communication* 8 (11): 1784–1794.

Newman, Joe, Joseph Jerome, and Christopher Hazard. 2014. Press Start to Track?: Privacy and the New Questions Posed by Modern Videogame Technology. *American Intellectual Property Law Association (AIPLA) Quarterly Journal*.

Newman, Lilly. 2014. Insurance Companies Want to Use Your Personal Data to Determine Your Premiums. *Future Tense*. http://www.slate.com/future_tense/2014/09/11/insurance_companies_are_using_quantified_self_data_for_accountability_tracking.html. Accessed 11 Feb 2016.

Olson, Parmy. 2014a. Jawbone Jumps Into Employee Monitoring. *Forbes*. http://www.forbes.com/sites/parmyolson/2014/12/11/jawbone-employee-fitness-monitoring/. Accessed 21 Nov 2015.

———. 2014b.The Quantified Other: Nest And Fitbit Chase A Lucrative Side Business. *Forbes*. http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/. Accessed 11 Feb 2016.

Ruckenstein, Minna and Mika Pantzar. 2015. Beyond the Quantified Self: Thematic Exploration of a Dataistic Paradigm. *New Media and Society*, early view:1–18.

Schüll, Natasha Dow. 2016. *KEEPING TRACK: Personal Informatics, Self-Regulation, and the Data-driven life*. New York: Farrar, Straus, and Giroux.

Schumer, Charles E. 2015. Press Release: New York Senator Charles E. Schumer. https://www.schumer.senate.gov/newsroom/press-releases. Accessed 21 Nov 2015.

Scott, Glorianne. 2015 Fitbit Data Increasingly Used as Court Evidence. http://www.examiner.com/article/fitbit-data-increasingly-used-as-court-evidence. Accessed 15 Jan 2017.

Shemkus, Sarah. 2015. Fitness Trackers are Popular Among Insurers and Employers – But Is Your Data Safe? The Guardian. April 17. http://www.theguardian.com/lifestyle/2015/apr/17/trackers-wearables-insurance-employees-jobs-health-data. Accessed 15 Jan 2017.

Solove, Daniel J. 2006. A Taxonomy of Privacy. University of Pennsylvania law review. 154 (3): 477–564.

Solove, Daniel J. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego law review. 44: 745.

Suel, Marcus. 2013. Datarizing the Self: Reconstructing Identities Through Self-Quantifying Practices. Undergraduate Thesis, McGill University, Montreal.

Swan, Melanie. 2012. Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and The Quantified Self 2.0. Journal of Sensor and Actuator Networks 1 (3): 217–253.

Swan, Melanie. 2013. The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. Big Data 1 (2): 85–99.

Tene, Omer, and Jules Polonetsky. 2013. Theory of Creepy: Technology, Privacy and Shifting Social Norms. A Yale JL and Tech. 16: 59.

Till, Chris. 2014. Exercise as Labour: Quantified Self and The Transformation of Exercise into Labour. Societies 4 (3): 446–462.

Whitson, Jennifer R. 2013. Gaming the Quantified Self. Surveillance and Society 11 (1/2): 163–176.

Wilkins, Richard G. 1987. Defining the Reasonable Expectation of Privacy: an Emerging Tripartite Analysis. Vanderbilt Law Review 40: 1077–1129.

Ye, Teng Qi, Brian Moynagh, Rami Albatal and Cathal Gurrin. 2014. Negative FaceBlurring: A Privacy-By-Design Approach to Visual Lifelogging With Google Glass. In Proceedings of the 23rd ACM International Conference on Conference on Data and Knowledge Management. pp. 2036–2038.

CHAPTER 9

Communal Self-Tracking: Data Philanthropy, Solidarity and Privacy

Btihaj Ajana

Abstract The 'self' is often an overemphasised part of self-tracking culture. However, self-tracking is not restricted to individualised forms, but is increasingly becoming a socialised phenomenon, whereby users are incited to share with others information about their physical activities and biodata via social media and dedicated platforms. This chapter builds on previous sections, looking at the 'communal' aspect of self-tracking while questioning the 'solidaristic' dimension of data sharing. It considers this communal aspect as a form of digital biosociality and links the discussion to debates on 'data philanthropy'. In doing so, this chapter explores some of the ideological functions of data donation and its philanthropic discourses, highlighting the emerging tensions between data ownership, data sharing and privacy issues in the context of self-tracking practices and data.

B. Ajana (✉)
Digital Humanities, King's College London, London, UK;
Aarhus Institute of Advanced Studies, Aarhus University, Aarhus, Denmark
e-mail: btihaj.ajana@kcl.ac.uk