The transparent self

Ethics Inf Technol (2016) 18:9–16
DOI 10.1007/s10676-016-9396-y

ORIGINAL PAPER

The transparent self

Marjolein Lanzing[1]

Published online: 2 April 2016

Abstract This paper critically engages with new self-tracking technologies. In particular, it focuses on a conceptual tension between the idea that disclosing personal information increases one's autonomy and the idea that informational privacy is a condition for autonomous personhood. I argue that while self-tracking may sometimes prove to be an adequate method to shed light on particular aspects of oneself and can be used to strengthen one's autonomy, self-tracking technologies often cancel out these benefits by exposing too much about oneself to an unspecified audience, thus undermining the informational privacy boundaries necessary for living an autonomous life.

Keywords Quantified self · Self-tracking · Transparency · Informational privacy · Autonomy

Introduction

Wearable computing, automated data gathering and larger and less expensive data storage capacity have spurred the practice of self-tracking. Self-trackers wear digital self-tracking devices that measure and monitor aspects of their bodies and everyday activities.[1] The data is stored and can be shared, monitored and interpreted by the user, which gives rise to a new 'range of relations to the self': the 'quantified self (QS)'.[2] Self-tracking is promoted as a means to self-knowledge, self-improvement and self-control: as strengthening autonomy.[3]

Yet, the notion of 'self-tracking' is somewhat misleading. Although self-tracking appears to merely entail self-surveillance, it also involves co-veillance and surveillance. Sharing one's data with peers is encouraged and producers of self-tracking devices often track what these devices are recording by default. Moreover, the data produced by self-tracking is increasingly shared and used outside its usual contexts. Therefore, self-tracking raises normative questions. How should we interpret technologies that encourage and facilitate extended transparency? Self-trackers celebrate the potential for self-governance by disclosing their personal information. I argue that there is tension between the idea that one should disclose personal information in order to gain more self-control and the informational privacy one needs to live an autonomous life.

I proceed in four steps. First, I describe the cultural phenomenon of self-tracking, including some of its promises. Second, I argue that self-tracking should not be perceived as 'keeping a digital diary' and should not be understood in terms of conventional, contextual expectations regarding informational disclosures belonging to the medical context. Third, I argue that the culture of self-

✉ Marjolein Lanzing
M.lanzing@tue.nl

[1] Section of Philosophy and Ethics, Department of Industrial Engineering & Innovation Sciences, University of Technology Eindhoven, Het Eeuwsel 57, IPO 1.13 5600 MB, Postbus 513, 5612 AZ Eindhoven, The Netherlands

[1] Till (2014).

[2] Lupton (2013).

[3] This paper makes a general assumption that self-control, self-knowledge, self-improvement and the popular notion of 'empowerment' often employed by self-trackers are notions that are strongly related to and important for the concept of autonomy.

tracking fosters "decontextualization". Fourth, I explain why this is problematic from a privacy perspective. It is because the culture of self-tracking breaks down informational privacy boundaries that otherwise enable autonomous self-presentation within different social contexts.

Quantified self: the practice and promise of self-tracking

Self-tracking is often referred to as 'quantification of the self': a means to grasp insights about one's self based on objective data, generated by quantifying aspects of your self with the assistance of digital devices and applications that measure aspects of one's body and activities. The data is recorded, stored, monitored and interpreted by the user.[4] This paper focuses specifically on self-tracking technologies that generate health and fitness data. These are highly popular with users and attract the attention of employers, insurance companies and public health officials. At the same time, health data is generally considered private and highly sensitive.

The use of self-tracking devices and apps is proliferating and the market is growing.[5] The popularity and evolution of self-tracking devices has enabled the rise of the Quantified Self Movement (QSM), an expansive self-tracking community founded in 2007 by Kevin Kelly and Gary Wolf.[6] The QSM consists of a diverse group of people, including visionaries, patients, researchers, engineers and entrepreneurs.[7] Tracking is within the reach of more people, now that the supporting devices have become less expensive and easier to use.[8] Devices have become less obtrusive, wearable and subsequently secured a positive consumer image as 'cool tech toys'.[9]

Self-tracking devices come in all shapes and sizes. In addition to the smartphone or tablet on which you can download self-tracking apps, there are many wearables and 'smart' objects that enable self-tracking. There are clip-on cameras, wristbands and headbands with embedded sensors that automatically record the user's movements and biometrics such as brain activity, blood pressure, heart rate and temperature. Many self-tracking devices appear to be ordinary objects or accessories such as watches, rings, glasses or even menstrual cups. Some devices have multiple parts: a FitBit-bracelet is wirelessly connected to a scale that correlates one's fitness data with one's weight.

Not surprisingly, the QSM employs the slogan *'self-knowledge through numbers'*. 'Numbers' refers to daily activities and bodily functions translated into raw data. New possibilities for tracking, collecting and analysing data facilitate new perspectives on the Self:

> Now much of the data-gathering can be automated, and the record-keeping and analysis can be delegated to a host of simple Web apps. This makes it possible to know oneself in a new way.[10]

This quote implies an underlying idea about self-tracking: collecting more data from your activities will make you more transparent to yourself. Meticulous self-surveillance will provide a new (complementary) 'narrative' about the self. This increases one's (accurate) self-knowledge, -awareness and -understanding.[11]

Nevertheless, the goal of self-tracking is not merely to collect vast amounts of personal data. The trend and primary function of new self-tracking technologies 'is less to enlighten users with information than to prod them to change', thus controlling, changing and improving users' behaviour based on the insights derived from the data.[12] Making the self transparent through numbers will offer the user the tools to change, improve and control the self:

> … there will be a certain segment of the population that will be into the self-improvement side of things, using analytics to learn about ourselves. [W]e may have a vague sense about something, but when the pattern is explicit, we can decide, "Do we like that behavior, do we not?"[13]

The promise that technologies could extend our will is also gaining traction in the philosophical domain. Hall et al. see 'undeniable power for self-discovery in the external tools that enable the systematic gathering and processing of the data'.[14] Personal data mining could empower humans. Under the computerized auspices of an external 'third eye', we could greatly influence our level of self-control.

Although concrete empirical evidence regarding the effectiveness of self-tracking is presently lacking, some studies show that accurate monitoring reduces failures of self-control.[15] Moreover, being aware of the fact that

[4] Lupton (2013): 25.

[5] Research and Markets, Dublin (2015).

[6] It is important to stress that there are many individual self-trackers who track a particular aspect of their life but who do not identify with the community of the QSM. See Neff and Nafus (2016).

[7] Fotopoulou (2014).

[8] Lupton (2013): 29.

[9] Hill (2011): 100–101.

[10] Wolf (2014).

[11] See Nafus and Sherman (2014), Lupton (2014) and Barta and Neff (2016) for detailed (ethnographic) research on the different practices, values and motives of the QSM.

[12] Singer (2015).

[13] Regalado (2013).

[14] Hall et al. (2013): 495.

[15] Fogg (2003).

others monitor one's behaviour adds another layer of externalized control and disciplining power.

One could easily imagine that this would give us an epistemic advantage. Self-tracking could reduce confabulation, biases, illusions and ignorance. Like a diary, self-tracking could be an illuminating self-help tool in gaining accurate information about our selves and aid reflection. Additionally, self-tracking might improve efficient decision-making. These devices may encourage and enforce desired behaviors in line with users' life choices.

A new medium, a changed practice

Self-tracking devices are often perceived as self-help tools and conceptualized as digital diaries or journals. Moreover, they are understood in terms of contextual expectations belonging to the traditional medical context. Yet, should they be conceived as such?

Motivational efficacy, self-control and access to (minimally) accurate information are all important dimensions of autonomy.[16] We use strategies to obtain access to accurate information about ourselves in order to increase self-control and become more effective in carrying out our plans every day.[17] One of these strategies is keeping a diary.

Medical professionals often ask their patients to keep a (medical) diary to record their eating habits, moods, physical exercises, absence or presence of pain. Scrupulous self-monitoring can prove incredibly valuable for self-help and empowerment. At a QS conference one participant shared a successful experience in which she felt more empowered. As a Parkinson's patient, she had been in and out of hospitals for a great part of her life. Through self-tracking, she was able to contribute data about her body to the meetings with her neurologist and physician. Based on the insights drawn from the data, she was able to increase her autonomy in deciding the doses of her medication.[18]

Self-tracking is often understood as the digital equivalent or the evolved practice of keeping a diary or journal.[19] Typically, a diary is characterized as an individual project meant to privately record one's intimate reflections, feelings, experiences and logging of daily (personal) facts—hence the symbolic lock that often adorns the artifact. Since self-tracking enables disclosure of one's personal information, it would be counterintuitive to parallel the practices. Yet, historically, there exist many different forms of the ego-document including diaries as communal means of expression and therefore not at all 'private' or 'intimate' in the sense of being strictly accessible to the author. In fact, 'an essential feature of all diaries is their addressee'.[20] This would be an argument supporting the claim that self-tracking devices are similar to diaries.

Nevertheless, conceptualizing self-tracking as a digital way to keep a diary is misleading:

> Cultural practices or forms never simply adapt to new technological conditions, but always inherently change along with the technologies and the potentialities of their use.[21]

As I will argue, the potentialities of self-tracking technologies facilitate, enable and encourage informational disclosures to an unspecified audience rather than directed disclosures at particular addressees. Contrary to a written diary, the terms and measures we employ to self-monitor are not selected by the user, but part of the design of the device. A self-tracker cannot control or be sure that third parties will not access her data. Ignoring the change of the cultural practice along with new technological potentialities of self-tracking devices contributes to misconceptions about the way information is collected, shared and stored. Let us keep this in mind and now explore the particular domain of health and lifestyle where self-tracking devices are increasingly used.

Intimate informational disclosures concerning our behaviour and bodies were formerly confined to the confidential, legally protected medical setting where one interacts with one's doctor. Within this context a person can reasonably expect that her well-being is the number one priority and that any information shared within this sphere will not be shared in different contexts without her knowledge and without her consent. In their role, doctors are subjected to social norms for the medical setting and legally bound to protect confidentiality and trust. A breach of patient confidentiality is experienced as a violation of a special social relationship and the trust that accompanies it. It is the transgression of a social norm, in fact, of an informational privacy norm: a common, contextual understanding about what to disclose to whom and to what extent.

New self-tracking technologies for health and fitness can create confusion because they change the social practices within this particular social context. These new technologies enable informational disclosures not directed at specific audiences. It might be unclear who will have (future) access to the generated information and what their interests may be. Before, a patient could rely on legal

[16] Christman (2004): 333.

[17] Heath and Anderson (2010).

[18] QS Europe conference, Amsterdam September 18th, 2015. Breakout session 'Talking Data With Your Doctor'.

[19] Lupton (2014): 3.

[20] Van Dijck (2004): 2.

[21] Van Dijck (2004): 1.

protection, informed consent, codes of conduct, social norms, even the physical boundaries such as the structure of the physician's office as a closed-off space. Now, these boundaries are difficult to enforce because they are completely lacking or not yet adapted to the new technological possibilities of self-tracking.

Common informational privacy norms regarding data use or distribution do not necessarily apply in the 'cloud'. Nevertheless, users of self-tracking devices do uphold contextual (and conventional) expectations regarding how their health data is used and shared, often based on their experiences with the social conventions of the physician's office. This, along with the failure to re-interpret the practice of self-tracking as a new cultural form, may explain why users are prone to many misconceptions with regard to the ubiquity, granularity, frequency and comprehensiveness of health data collection.[22] And yet, as I will argue in the next section, the culture of self-tracking (actively) stimulates disclosure and discourages regulated disclosure.

Techno-norms of disclosure

The culture of self-tracking stimulates informational disclosure.[23] I argue that the design of self-tracking technologies plays a significant role in enabling, encouraging and implementing new norms of handling information flows. Also, I argue that the community of self-trackers and the enterprises producing self-tracking technologies are equally influential in co-creating, embedding and shaping new techno-norms of disclosure. I will first describe the self-tracking community.

The values of self-tracking are rooted in Web 2.0, which originated at the beginning of the millennium as the egalitarian ideal of the Internet as a participatory, interactional space in which users are both consumers and contributors that create content such as blog posts, forum discussions and websites.[24] Self-trackers are such 'prosumers': they produce data and mutually consume each other's data. Through aggregation of individual data collections, broader conclusions are produced that are useful for all self-trackers. Self-experimentation, learning by doing, sharing the (self-) knowledge gleaned from self-tracking, exchanging ideas about how users can make their data more meaningful and sharing self-tracking methods in order to gain self-control are topics that can be found across the QS website, blogs, regular meetings and annual conferences in the US and Europe.[25] The idea that self-disclosure is linked to empowerment is pervasive within the community:

> At the conference, I not only saw a community 'in love' with numbers, but also people engaging in radical acts of self-disclosure. Standing on stage they talked about painful episodes in their lives (depression, anxiety); they showed their bodies virtually (in every sense of the word) naked; they showed their dreams, their diary entries and their meditation practices, and they talked about their physical diseases and their struggles against overweight.[26]

Of course, many individual self-trackers do not share their data. But merely consuming and not producing is not stimulated within the culture of self-tracking. In her 2004 analysis of lifelogging, José van Dijck remarked that 'although reciprocation is certainly not a condition for participating in the blogosphere, connecting and sharing is definitely written into the technological condition'.[27] This can easily be applied to the culture of self-tracking anno 2015.

Consider now two self-tracking technologies, namely the immensely popular FitBit and Strava fitness-bracelets. First of all, self-tracking devices can be defined as scaffolding technologies, technologies that use environmental, psychological or social strategies in order to overcome deficiencies of the user's willpower. Self-tracking relies on the assumption that willpower is distributed and that self-control can be found in more than one place, even outside the individual's mental realm.[28] I will now present three examples of scaffolding strategies, as features of FitBit and Strava, where information disclosure figures prominently.

Firstly, FitBit and Strava are designed as environmental strategies. They are artifacts that structure the user's environment. Their design, such as being waterproof, inconspicuous and wearable (day and night), enables and stimulates continuous use. It makes the device part of one's daily routine. Users experience a certain loss when they take off their devices, because their data might become incomplete.[29] Users grow attached to the device, regarding

[22] Patterson (2013): 37.

[23] (Informational) disclosure is the revealing of information. It may imply information-sharing, like when a technology automatically uploads the 'uncovered' or collected information or when the user decides to share her (personal) information with others. I view norms of informational disclosure as 'norms of privacy' or 'privacy boundaries' since privacy norms are dynamic social norms that govern information-flows (what to disclose, to what extent and to whom) within, and therefore play an important role in mediating, different social relationships and contexts. I will speak of norms of disclosure and privacy norms interchangeably.

[24] van Dijck (2013): 10.

[25] Fotopoulou (2014).

[26] Zandbergen (2013).

[27] Van Dijck (2004): 11.

[28] Heath and Anderson (2010): 9.

[29] Foss (2014).

it as belonging to their bodies. Through this attitude they become vulnerable to constant monitoring.[30]

Secondly, FitBit and Strava incorporate psychological strategies such as reward and warning systems, combining pleasant and unpleasant tasks and visualizing realistic targets. For instance, Strava motivates its users by turning a solitary exercise into an exciting game with both known (peers) and unknown (e.g. based on age, location, sex) competitors.[31] Through features of scoring (leaderboards) and reward (awards, badges), Strava motivates users to improve their performances and to log their performances.[32] The game elements motivate users to share more data with Strava and other Strava-users: users are constantly stimulated to compete with others and themselves, thus generating more data.

Finally, Fitbit and Strava employ social strategies. Through these strategies the user authorizes someone else to exercise control over her.[33] Examples of social strategies are deadlines, teamwork and seeking out the 'right' company to support the desired behavior. Fitbit and Strava offer social media options, forums and groups where users can share information with anyone ranging from 'friends' to virtual strangers. Hence users can check on and encourage each other.[34]

Many self-trackers proudly share their personal information. Yet, many of them are concerned about privacy. Producers of self-tracking technologies have an interest in encouraging disclosures of personal information; selling aggregated personal health data is a lucrative business. Cooperations with (medical) insurance agencies, research-institutions, employers and governmental institutions are currently explored.[35] 'Pushed self-tracking' is an increasingly common type of self-tracking in which 'self-monitoring might be taken up voluntarily, but in response to external encouragement or advocating rather than as a wholly self-generated and private initiative'.[36] Companies such as FitBit and AppleHealth facilitate 'pushed self-tracking' and encourage users to share and connect their data. Apple's HealthKit allows developers of self-tracking apps and devices and/or doctors to access users' health information automatically. It also allows users to connect and exchange the data of different self-tracking devices:

> With HealthKit, developers can make their apps even more useful by allowing them to access your health data, too…. you choose what you want shared. For example, you can allow the data from your blood pressure app to be automatically shared with your doctor. (…) When your health and fitness apps work together, they become more powerful. And you might, too.[37]

This quote suggests that by sharing data, apps and devices become more powerful when they know more about the user. They then empower the user with personalized advice. However, it is important to realize that companies can share user information at whim:

> Self-tracking companies can share user information with business associates, data brokers, marketers, insurance plans, employers, or even law enforcement, subject only to self-directed, self-imposed restrictions on the information flow practices decided internally and spelled out to users, often opaquely, in privacy policies. [O]nce information has reached second and third parties, there is very often no way to predict where it will land.[38]

Self-disclosure is part and parcel of the culture of self-tracking. While self-disclosure is not problematic per se, self-tracking pushes users to disclose personal information outside its usual context. Self-tracking fosters decontextualization: a blurring of common privacy boundaries—consisting of particular informational privacy norms—by collapsing social contexts. This causes information that was formerly confined to and aimed at a particular social context or relationship to transgress its usual borders.[39] In the next section I will explain why decontextualization is problematic by explaining the value of privacy.

Privacy: controlling one's self-presentation

Alan Westin classically defined informational privacy as the control individuals, groups and institutions have over determining how, when and to what extent information is distributed to and, ultimately accessed by, others.[40] When one's privacy is violated, for instance by information-distribution to the state, commercial companies, an employer, classmates or unknown third parties without someone's consent, this results in a violation of the very conditions required for autonomy.[41]

[30] Patterson (2013): 25.

[31] Lupton (2013): 28.

[32] Hill (2011): 101.

[33] Heath and Anderson (2010): 15.

[34] For the idea that monitoring or peer pressure has a disciplining effect see Foucault (2007). Foucault discusses a type of *sur*veillance that becomes internalized and thus disciplines the subject. Self-tracking is a form of *self*-surveillance (watching oneself from a third person perspective) and (*social*) surveillance at the same time.

[35] Lupton (2014): 7.

[36] Lupton (2014): 7.

[37] http://www.apple.com/ios/whats-new/health/.

[38] Patterson (2013): 10.

[39] Nissenbaum (2010), Patterson (2013).

[40] Westin (1967).

[41] Roessler (2005): 112.

Many scholars have argued that informational privacy, or controlled disclosures, enables one to mediate different social relationships.[42] Information shared with (say) a physician should not be passed on to someone's employer. It would be a gross violation of privacy and a violation of the patient-doctor relationship if the physician would communicate this knowledge to the patient's employer. Informational privacy norms demarcating the context of the doctor's office define the relationship. When such informational privacy norms are transgressed, one loses the ability to form reasonable expectations and assessments of who has access to one's information. Different social contexts require different behaviour and different expectations from us. We rely on these all the time. A violation of these expectations is a violation of contextual integrity.[43] To foster and maintain different meaningful social relationships within distinct social contexts, one must be able to mediate different levels of disclosure.[44] Privacy norms embody dynamic social negotiations of access and withdrawal.[45]

Self-disclosure may alienate one from oneself when disclosures that formerly took place within one context are disseminated to other contexts. When a teenager's diary is secretly read by her best friend who then tells her classmates about certain passages behind her back, various relationships become distorted due to the loss of control over this information. Beate Roessler argues that without informational privacy and controlled self-disclosure, authentic behaviour and identification with a certain conception of the good life become problematic:

> (…) self-chosen diversity in one's relations would not be possible. Nor, therefore, would self-determined, context-dependent, authentic behaviour towards others, or the variety of self-chosen forms of interaction with others, or communication and reflection on self-chosen problems and issues, graded, as it were, according to the relation in question. Nor would it be possible to find an answer authentically, to the question of how one wants to live.[46]

When self-disclosures are disclosed to an unspecified and even 'unknown' audience, as in the case of the classmates that secretly have access to information not intended for them, it becomes difficult for the discloser to behave in an authentic way. She loses her ability to form adequate expectations about who has access to her information and to what extent. According to Roessler, when someone cannot control who has access to her personal information, this reduces her freedom in determining her own behaviour and self-presentation in different contexts, which results in inauthentic interaction.[47] Roessler states that a person can only be fully autonomous when she is able to present oneself in a self-chosen way in a self-chosen context, performing self-determined actions fitting with one's expectations about the context in question.

Here is a fictitious, but realistic case that most would categorize as a clear violation of privacy.[48] First, consider covert observation. Imagine that Charles has logged all of his activities and biometrics onto his self-tracking device. Charles received the wearable from his employer as a playful encouragement to improve his lifestyle in exchange for free health insurance. Charles expects his medical information to remain private or be shared with his personal physician. Unbeknownst to Charles, his employer keeps track of his data and discovers that Charles is in fact a diabetic. Perceiving this as a 'risk' and fearing high medical costs, the employer searches for an appropriate pretext to fire Charles.

This can be perceived as deliberate deception. Facts that could have led Charles to choose a different course of action were kept from him. He engaged in self-tracking based on prevalent assumptions and expectations about informational flows in the social context of the workplace. Though he was under the impression that he had control over the knowledge others had of him, he did not.[49]

> Covert observation – spying - is objectionable because it deliberately deceives a person about this world, thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice.[50]

This quote from Stanley Benn clearly states that to respect Charles as a person, one should perceive him as an actual or potential chooser, an agent: a person trying to plan his own life, adjusting his behavior as his perception of the world changes. To interfere with his autonomous choices is to violate his privacy. Authentic behavior is problematized: the deceived, spied-upon person acts on reasons that 'cannot be his reasons', because they are the deceiver's. Without privacy, a person can never fully and confidently claim that she has acted on reasons she has selected herself and fully identifies with.

[42] Fried (1984), Rachels (1975).

[43] Nissenbaum (2010).

[44] Altman (1975), Greene et al. (2006), Goffman (1959).

[45] Steeves (2009).

[46] Roessler (2005): 116.

[47] Roessler (2005): 115.

[48] It is not my intention to resolve or address the concrete harms of this particular case by proposing alterations of design, policy or law, but rather to use this example to point out the very insidious, subtle and more abstract trend of decontextualization that is often not recognized as such because it does not directly cause demonstrable harm.

[49] Roessler (2005): 116.

[50] Benn (1971): 230.

Let me now present the case from a different angle. If Charles discovers that his employer is monitoring his data, he has three options. First, he can stop his self-tracking activities as a response. Second, he can continue tracking, but adjust his privacy settings or limit the activities and biometrics he is tracking, taking the potential 'audience' into account. Thirdly, he can mess up the data he is collecting by cheating, for instance, by letting other people wear the device. In all three cases, Charles is forced to see himself, his activities, thoughts and feelings through the eyes of another and to adjust his activities according to this audience. Charles sees himself as the object of constant examination, which changes his perception of himself and the nature of his activity.[51]

Whether the monitoring is covert or not, Charles' autonomy is compromised because his employer controls the technological means and the information that it generates. Charles is subjected to the control of others and, as a consequence, his self-perception may change. Even if the employer does not actually access and disclose the information, the power imbalance is such that she could easily do so whenever she wishes to. As a result, it becomes extremely difficult for Charles to autonomously control his self-presentation within this context.

Conclusion

Many privacy scholars have located the value of privacy in autonomy, arguing that it is necessary for freely fostering close relationships, individual choice, creativity and other aspects of an autonomous life.[52] Autonomous agents a re able to shape their lives according to those desires, beliefs and values judge to be good reasons for action. They should be able to identify with their actions and decisions. As Roger Crisp states: 'part of what makes life worth living is running one's own life for oneself'.[53]

As the practice of self-tracking becomes increasingly institutionalized, users will increasingly be able to "outsource" their self-government, as Valdman puts it, to devices and those who control and access them by making visible what was not visible before.[54] My thesis is that extended transparency conflicts with the informational privacy norms necessary for full autonomy. Success stories about empowerment, self-control and self-improvement camouflage the reality of decontextualization, where we expose too much to an undefined (future) audience, which limits our capacity to run our lives for ourselves.

Self-tracking technologies could be valuable tools for strengthening one's self-control. For instance, a user may gain more control over her body weight by tracking and sharing her calorie intake and athletic performances. Yet, the way many of these self-tracking devices and apps are currently designed and used, combining self-surveillance, co-veillance and surveillance, cancels out these promising results. Beyond her control, the information collected through self-tracking exposes her geo-location, her consumer and exercising behaviour, the time she spends in and outside of her office or home and many more variables to an unidentified audience. One can deduce many insights about a user's personal life from the data gathered. Altogether, this constitutes a violation of her privacy that can undermine her autonomy on a more fundamental level.

Then, how should we deal with this in practice? The broader privacy problem of decontextualization deserves further normative scrutiny, yet, we must also think about how to practically negotiate the tension between transparency and limits on disclosure. Users should be educated about digitalization of cultural practices, information flows of emerging self-tracking technologies, potential purposes of one's information and potential audiences. Furthermore, we should critically evaluate the design features of self-tracking technologies and offer alternatives, beyond the mere option for 'consent', whereby users have granular control over the flow of their information and the potential audiences that may be able to access their data. Users should also be able to anonymize or delete their data. It is particularly important to reconsider the institutionalization of commercial self-tracking devices within the health care sector.

I have argued that informational privacy is an important condition for leading an autonomous life. Users should be able to negotiate and control informational disclosures. Otherwise, I doubt we could interpret self-tracking as a normatively significant contribution to autonomy.

Acknowledgments I would like to thank Beate Roessler, Anthonie Meijers, Philip Nickel, Sven Nyholm, Bart van der Sloot and Priscilla Regan for their immensely valuable and helpful comments on earlier drafts of this article. I am also grateful for the comments and questions raised by the audience and participants of the "Robots, Telecare and Health Data: Interdisciplinary Perspectives" workshop (University of Eindhoven, April 2015), the MANCEPT "Privacy and Transparency" workshop (University of Manchester, September 2015), and the "Value and Ethics of Privacy" track at the Amsterdam Privacy Conference (University of Amsterdam, October 2015).

[51] Benn (1971): 230.

[52] Benn (1971), Fried (1984), Inness (1992), Rachels (1975), Roessler (2005).

[53] Crisp (1997): 61.

[54] Valdman (2010).

References

Altman, I. (1975). *The environment and social behavior*. Monterey: Brooks/Cole.

Barta, K., & Neff, G. (2016). Technologies for Sharing: Lessons from Quantified Self about the political economy of platforms. *Information, Communication and Society, 19*, 4.

Benn, S. I. (1971). Privacy, freedom and respect for persons. In F. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press.

Christman, J. (2004). Autonomy, self-knowledge and liberal legitimacy. In J. Christman & J. Anderson (Eds.), *Autonomy and the challenges to liberalism*. Cambridge: Cambridge University Press.

Crisp, R. (1997). *Mill on utilitarianism*. New York: Routledge.

Fogg, B. J. (2003). *Persuasive technology: Using computers to change what we think and do*. San Francisco: Moran Kaufmann.

Foss, J. (2014). The tale of a fitness-tracking addict's struggles with strava. *WIRED*. October 3. http://www.wired.com/2014/10/my-strava-problem/.

Fotopoulou, A. (2014). The Quantified Self community, lifelogging and the making of 'smart' publics. *openDemocracy*. https://www.opendemocracy.net/participation-now/aristea-fotopoulou/quantified-self-community-lifelogging-and-making-of-%E2%80%9Csmart%E2%80%9D-pub. Accessed 10 Sept 2014.

Foucault, M. (2007). *[1975] Discipline, toezicht en straf*. Groningen: Historische Uitgeverij.

Fried, C. (1984). Privacy: A moral analysis. In F. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press.

Goffman, E. (1959). *The presentation of self in everyday life*. Garden City: Doubleday.

Greene, K., Derlega, V., & Mathews, A. (2006). Self-disclosure in personal relationships. In A. Vangelisti & D. Perlman (Eds.), *Cambridge handbook of personal relationships*. Cambridge: Cambridge University Press.

Hall, L., Johansson, P., & de Léon, D. (2013). Recomposing the will: Distributed motivation and computer mediated extrospection. In T. Vierkant, A. Clark, & J. Kiverstein (Eds.), *Decomposing the will*. Oxford: Oxford University Press: Philosophy of Mind Series.

Heath, J., & Anderson, J. (2010). Procrastination and the extended will. In C. Andreou & M. D. White (Eds.), *The thief of time*. New York: Oxford University Press.

Hill, K. (2011). Taking my measure. A track-your-life revolution has begun. Can Managing your Personal Data make you Happier, Healthier and Wealthier? *Forbes*. April 25.

Inness, J. (1992). *Privacy, intimacy and isolation*. New York: Oxford University Press.

Lupton, D. (2013). Understanding the human machine. *IEEE Technology and Society Magazine*. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6679313. Accessed 28 March 2015.

Lupton, D. (2014). Self-tracking modes: Reflexive self-monitoring and data practices. Available at SSRN: http://ssrn.com/abstract=2483549 or http://dx.doi.org/10.2139/ssrn.2483549.

Nafus, D., & Sherman, J. (2014). This one does not go up to eleven: The Quantified Self movement as an alternative big data practice. *International Journal of Communication*, *8*.

Neff, G., & Nafus, D. (2016). *Self-tracking*. Cambridge: MIT Press.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Palo Alto: Stanford University Press.

Patterson, H. (2013). Contextual expectations of privacy in self-generated health information flows. TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. SSRN: http://ssrn.com/abstract=2242144 or http://dx.doi.org/10.2139/ssrn.2242144.

Rachels, J. (1975). Why privacy is important. In F. Schoeman (Ed.), *Philosophical dimensionsof privacy: An anthology*. Cambridge: Cambridge University Press.

Regalado, A. (2013). Stephen wolfram adds analytics to the quantified-self movement. *MIT Technology Review*. http://www.technologyreview.com/news/514356/stephen-wolfram-on-personal-analytics/. 8 May.

Research and Markets, Dublin. (2015). http://www.prnewswire.com/news-releases/global-smartwatch-market-2013-2020-samsung-pebble-garmin-nike-sony-fitbit-and-casio-dominate-the-32-billion-industry-300033591.html.

Roessler, B. (2005). *The value of privacy*. Cambridge: Polity Press.

Singer, N. (2015). Technology that prods you to take action, not just collect data. *The New York Times*. http://www.nytimes.com/2015/04/19/technology/technology-that-prods-you-to-take-action-not-just-collect-data.html. 18 April.

Steeves, V. (2009). Reclaiming the social value of privacy. In I. Kerr, V. Steeves, & C. Lulock (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society*. Oxford: Oxford University Press.

Till, C. (2014). Exercise as labour: Quantified Self and the transformation of exercise into labour. *Societies, 4*(3), 446–462.

Valdman, M. (2010). Outsourcing self-government. *Ethics, 120*(4), 761–790.

Van Dijck, J. (2004). Composing the self: Of diaries and lifelogs. *The Fibreculture Journal*, *1*(3).

van Dijck, J. (2013). *The culture of connectivity*. New York: Oxford University Press.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Wolf, G. (2014). Quantified Self | Antephase. http://antephase.com/quantifiedself. Accessed 22 Oct 2014.

Zandbergen, D. (2013). Data confessions of the quantified self. http://www.leidenanthropologyblog.nl/articles/data-confessions-of-the-quantified-self. Accessed 1 Feb 2015.