Modifying Consent Procedures to Collect Better Data: The Case of Stress-Monitoring Wearables in the Workplace

Stéphanie Gauttier(✉)

University of Twente, Drienerlolaan 5, 7522NB Enschede, The Netherlands
s.e.j.gauttier@utwente.nl

Abstract. Smart wearables can be used in the workplace for organisations to monitor and decrease the stress levels of their employees so they can work better. Such technologies record personal data, which employees might not want to share. The GDPR makes it compulsory to get employees' consent in such a scenario, but is seen as asking a yes/no question. We show that implementing this consent procedure is not enough to protect employees and make them adopt devices. Based on interviews, we argue that more control must be given to employees on which data is collected and why through an ongoing engagement and consent procedure. It could lead to higher technology adoption rates and data quality.

Keywords: Consent · Digital organisations · Smart wearables · Ethics · Technology acceptance · Human enhancement

1 Introduction

Microchips implants to control the environment [9], piercing like implants to get new senses[1], wearable devices to manage our stress [15], some have started to propose the use of cyborg-like technology to individuals and organisations. While individual use of such technologies can be seen as an application of the right to morphological freedom [20], their use under the impulse of an employer is more problematic as employees might not have a choice but to change themselves for the purpose of better work performance. Indeed, these technologies are meant to increase the physical, cognitive, and psychological abilities of the individuals so that they reach higher levels of happiness than confined in the natural limits of their bodies [14]. They have only an indirect impact on work as they are targeting generic abilities and designed to benefit to the individual, at work and after work when doing multiple different tasks. It is because I perceive directions better that I perform better in orientation tasks, it is because I have a microchip that I open door without movement and am faster in carrying elements. Completing tasks faster, better, in new ways is seen as intelligence augmentation [6] and is a promise of increased productivity in the workplace.

[1] https://www.theguardian.com/technology/2017/jan/06/first-humans-sense-where-north-is-cyborg-gadget.

W. Abramowicz and R. Corchuelo (Eds.): BIS 2019, LNBIP 353, pp. 350–360, 2019.
https://doi.org/10.1007/978-3-030-20485-3_27

Notwithstanding the possibility offered by enhancement technologies to create value for business, and it being a market in itself, the use of enhancement technologies at work raises both moral and legal issues. These technologies can record personal data. In such a case, issues related to the ownership of the data and to the respect of the employees' privacy arise.

Since 2018, in Europe it is compulsory to ask for specific and explicit consent when recording personal data as per the General Data Protection Regulation (GDPR). Personal data is interpreted as being anything which relates to or allows to identify an individual. This leads to a series of yes or no question in research protocols or before users can use a new technology or service. It allows individuals to decide how their personal data is handled and so to ensure their privacy is respected as much they can.

In many ways, one could argue that users of human enhancement technologies proposed by their organisation should be given the same right to give consent and that their interests would be protected by it. Companies themselves insist on having given a choice to employees and on that use is voluntary [9]. However, there are several challenges attached to gaining meaningful specific consent when considering the use of human enhancement technologies in the workplace. Firstly, these technologies are considered as emerging: the consequences of their use are not revealed yet, and not all of them can be anticipated. This means it can be difficult to obtain informed consent. Secondly, the use of these technologies in the workplace, a social and political environment, raises issues in terms of (perceived) pressure to consent. The interests of the employees might not be protected by simply asking for consent. Privacy has been shown to have an impact on technology acceptance in other domains [23], suggesting that individuals might consider ethical issues when choosing to use a technology. Implementing a consent procedure that reassures potential users about what can be done with their personal data is required. How can the limits of consent be overcome so as to guarantee a protection of the interests of the employees? Can it also improve the quality of the data gathered?

The thesis outlined in this paper is that to preserve the autonomy of participants, it is necessary to go beyond the formality of seeking consent. Rather, one needs to increase the control that the participants have over the course of the experiment on the data collected and its use.

Firstly, we analyse the concept of consent and show that seeking consent is meant to protect autonomy. Then, we present the case of an ongoing research project where hospitals are to ask their staff to use wearable technologies to monitor physical indicators of stress where the different approaches to consent prove to be ineffective in protecting the participants' autonomy. Thirdly, we introduce how displacing the focus from consent to control is more satisfactory in ensuring the participants' autonomy efficiently, in spite of its costs.

2 Seeking Consent as a Procedure to Protect Autonomy

The concept of consent is most discussed in the sphere of bioethics, from which we will draw in this section. Indeed, historically, the notion of consent, i.e. that an individual agrees to take part in a (medical) procedure, appeared during the Nuremberg trials and

was set out in the 1947 Nuremberg code as a way to protect individual's autonomy. Seeking consent is needed in order to make sure that individuals are not subject to procedures they do approve. Going further, Beauchamp and Childress [3] define personal autonomy as when '*The autonomous individual acts freely in accordance with a self-chosen plan, analogous to the way an independent government manages its territories and establishes its policies'* (pp 99–100). Protecting the personal autonomy of individuals requires giving them the opportunity to evaluate how a proposed course of action fits with their own desired trajectory. In this paper, we will consider only the case when individuals with capacity to give consent, i.e. adults with the needed cognitive abilities, are asked for consent or dissent. This means the individuals we consider are able to set their plans and evaluate options.

To achieve a form of consent which does protect the personal autonomy of such individuals, it is necessary to add two conditions: the consent must be properly informed and freely given (1964 Helsinki Declaration). This means that seeking consent is more than asking a yes or no question but is a process throughout which individuals get information on the purposes, procedures, of the research they are taking part in. This information must not be deceitful and must be provided in a language intelligible to the individuals whose consent is sought. Furthermore, this process must be implemented so that there are no threats, coercion, or persuasion to agree. While in the light of history some may read the requirement for no pressure and violence as the absence of physical coercion, this concept must be understood more broadly as there can be a form of psychological pressure to agree, depending on social pressure. Individuals are not isolated when they make their decision to consent or dissent and this social context, with its emotional and embodied aspects, needs to be considered. Since the 70s, there is a turn towards such a form of relational autonomy. The place of individuals or groups who have a responsibility in engaging with the individuals to inform their decision is to be considered. Protecting their autonomy, in this relational view, means that paternalistic approaches where an organisation would decide a priori what is the course of action to follow, are prohibited as each individual has a pre-established plan and can reject propositions which divert from the plan. Surrogate decisions and paternalism are to be avoided here and a principle of non-domination is to be followed. The absence of coercion, persuasion or threats also means that individuals must not face only bad alternatives if they dissent. Consent allows a sense of personal integrity as it enables the individual to follow their plan for themselves and their bodies. Consent is related to the concept of self-ownership [12], implying that we have ownership over our bodies and selves, and perhaps our data.

While asking for consent is an additional procedure, it can reinforce trust. The relationship between trust and consent is seen as positive [16] as it means that one can trust that the researcher will respect the terms of consent and the trust put in him by the individual, so no abuses will occur.

Consent can take different forms. It can be broad, or specific. Specific forms of consent are to be sought in current legislation (GDPR). This means that individuals are asked for consent on each aspect of the procedure or data collection which involves their personal data. They can object to certain tools (being recorded, with voice being personal data), while still giving consent to be part of a research project on a given topic. This means that more flexibility is required from the side of the researcher or of

any organisation collecting personal data. Consent can also be sought at multiple times in order to verify that the individual still agrees to continuing the procedure.

3 Seeking Consent Is not Enough to Protect Autonomy: The Case of Stress-Monitoring Wearables in the Workplace

The literature shows that such conceptions of consent do not allow to protect autonomy and self-ownership in the case of the use of wearables at work, even though seeking consent as mentioned in the law is seen as a solution to avoid ethical issues in practice.

3.1 Wearables at Work: A New Take on Consent Is Needed

We investigate how hospitals consider these stress-monitoring wearables and how nurses could be asked to use them. The Information System literature looking at technology acceptance in hospitals does not consider the use of wearables for physicians, but the use of tools used to cure patients or wearables for patients. Given the fundamental difference between the types and aims of the technologies explored in these cases and the one we are investigating, we do not base our argument on this previous research. There is little evidence of the impact of smart wearable technologies [7]. Extant research in the domain of consumer wearables has also put the emphasis on privacy and data security [1]. Literature on the use of wearables at work emphasizes the risks of surveillance [17, 24].

The extant literature on wearables at work shows that gaining meaningful consent is difficult. While the literature does not tackle consent directly, we look at consenting to participation is as a form of technology acceptance. In the acceptance of wearable, perceived benefits outweigh perceived risks, so that users might be incentivized to surrender their data and privacy for a greater benefit [25]. When thinking of the workplace, benefits might be tangible and take the form of securing a job or a monetary compensation. Privacy trade-offs and impacts on health however, might not be recognized by employees early on but rather through long term use. This means that consent cannot be meaningfully given at the beginning of an experiment or when a technology is just introduced as the individuals do not realize what they are consenting to.

This is made even more significant considering the effectual approach followed by the project, which is often seen in entrepreneurship and innovation and characterizes cases where organisations try to put a means to an end. It implies that the organisation must make decisions looking at what it can afford, but also at the risks individuals are ready to take [21]. Effectual reasoning is related to overtrust in the project in organisations. In our case, we look at a situation where the use of technology is suggested, but the organisation still has to make sense of how to make the technology useful for its own purposes and to think about how to implement it an efficient and ethical manner so that individuals use it. This means that the organisation has to reflect on how to appropriate the technology along the way and how employees can use this technology. It makes it difficult to ask for specific consent in the first place, as the possibilities coming from the use of the technologies are still to be discovered. Options can be given to individuals, but they risk being meaningless as they have not been tested beforehand.

Finally, users appropriate a system through time [5, 13, 19] and learn how to use it, so that their attitudes can change overtime: they can pause their usage or segment it [10]. As a reaction to automation, individuals can also misuse, disuse or abuse the device purposefully [4, 18]. Seeking consent at only one moment does not address the actual behaviors of users who change opinions over time.

Consent could be offered at several moments so that individuals have the possibility to withdraw. However, this is not the optimal solution for several reasons. Firstly, a withdrawal might intervene after a problematic situation has occurred and trust decreased. Secondly, there might be felt-pressure not to withdraw due to social pressure as described above. Thirdly, this would mean a total non-use of the system, while solutions to adapt uses could be found so that the investment in the information system can still bring some returns (even though not at the scale at which it was thought at first).

Turning towards the ethics literature on consent for the use of mobile health devices highlights that translating the notion of consent, born in the medical and bioethical realms, to medical technologies requires adjustments which imply more extensive procedures and less authority for individual laypersons [2]. The technology we intend to use deals with medical data (stress and mental health, but also as it captures data on heartbeat, blood pressure, skin conductivity), and is of mobile nature, suggesting that the extant literature on the limits of consent apply and, given the sensitivity of the data, more extensive procedures to inform and collect consent are needed. Because the use of the technology is not vital in our case, laypeople can have more control in deciding what technology to use and when. Doing otherwise, especially in a hierarchical setting like in a company would act paternalistically. This can be revisited in different contexts, given the expertise and ability to assess the technology of individuals.

An additional difficulty is added by the workplace setting. Indeed, the workplace also refers to a setting where autonomy is socially-embedded, and where the decision not to participate in the use of a technology can be meaningful and stigmatizing. For instance, [9] shows that employees proposed the use of microchip implants refer to the need to protect their image and not to be laggards when they are interrogated about their attitude towards the microchips. There needs to be a process where users have the possibility to influence the implementation plan and make decisions, rather than having to withdraw from the process totally.

We have shown that regular consent procedure might not be enough to protect the autonomy of employees. To gain meaningful consent, procedures coming from bioethics need to be adapted: the focus should be displaced from personal autonomy to relational autonomy. These procedures also need to take into account the hierarchical relationship at play and employees should be given control over the use of the technology. In practice, not so much thought is given to the informed consent procedure, even if managers are aware of the sensitivity of the data.

3.2 An Illustrated Case: The Role of Consent in the Implementation of Wearables for Stress-Monitoring Purposes

The first step of this research consisted in exploratory interviews with 10 managers of a hospital in Italy and 5 managers of a rehabilitation center in the Netherlands. These

'managers' span from administrative staff to scientific and medical staff. The interviewees were asked what the sources of stress in their organisations are, what form of data would be useful to fight stress, how it could be used for management, what could be consequences for employees, and how they would get employees to wear and use the device. For the purpose of this conference paper, we performed a preliminary analysis of the transcripts looking at (1) how sensitive is the data to be collected perceived to be and (2) what are the ethical concerns identified by the managers, including how to get consent.

Interviewees proceeded by themselves to an assessment of the potential benefits and harms of introducing stress-monitoring wearables for the organisation (see Table 1). It implicitly mentioned the need for fairness in the representation of stress through the data (the word fairness was not used but the concept was described). These potential harms underline that the data to be collected could span outside of working hours and that the organisation would get a database from which the health status of individuals could be inferred. Rules on what needs to be inferred to protect employees (detect the premises of a heart attack) or what should not be known by the hospital are difficult to establish. Rules on how to handle the needs for reorganization are also needed. Involving the employees in shaping the policies around what is meant to be done with their data could be a way to avoid backlash.

Table 1. Potential benefits and harms of the stress-monitoring wearables

Potential Benefits	Potential Harms
Less sick leaves, less burn outs	More complaints which are difficult to handle, demands to change wards
Better team management	Unfairness of the data (measuring stress objectively might not be possible), making it difficult to use
Less errors	Difficulty to explain the organisation will never be stressless – how to divide stressful times (night shifts) fairly
Better communication	Difficulty to separate stress coming from personal situations and stressing coming from work
Less stress	Difficulty in deciding how the data could be analysed for maximum usefulness
Possibility to prove stress	Inferring elements about employees' health
Possibility to use the device to regain control over work conditions	

This is not to say that all potential harms were listed. Indeed, they were focusing on what could happen to the organisation rather than the individual. They were also adopting a consequentialist perspective, without consideration of other approaches to assessing the technology (deontological, virtue-based approaches for instance). Besides, it can be difficult to forecast risks. Recent literature suggests that new frameworks are required in order to proceed to the ethical assessment of technologies for cognitive enhancement [8], and that approaches going beyond the traditional use of

checklist-based technology assessments are required as they do not allow to account for the new issues that can arise with emerging technologies [11]. It is difficult to predict what can occur once data is aggregated from several users or an intermediary service or party appears to process the data. There is a need for a dynamic procedure, where users can shape the extent of consent as they are in the experiment and discover potential issues.

However, there is an awareness that stress comes from work, but also from personal situations at home, and so measuring stress levels might be an inquiry in the personal sphere of the individual. Without the device, stressed nurses can be talking to their Head and decide to divulge a problem, which is not the same as the organisation wondering about the data collected and, potentially, scheduling an appointment to discuss someone's stress. The origin of the conversation and the dynamic of how one can decide to retain or share information is different.

Interviewees are also aware that stress is related to personality as it is subjectively felt: some individuals are stressed in a situation A when others are not, perhaps because they have developed better coping mechanisms. Monitoring stress levels, be it for research within an organisation or as a part of the regular functioning of the organisation, is not a trivial undertaking as it allows to record data on the personal experience that one has at work and how this experience is dealt with. It is recording deeply-personal data.

Furthermore, the wearable aims at, ultimately, being able to manage stress. The impact of the device is on the employees, not only on a task (as would be for a regular work tool). For an organisation to decide unilaterally that its employees need compulsory support in this domain could be seen as a paternalistic decision. Besides, the recording of personal data requires asking for consent[2].

Enthusiasm about the device is expressed by employees only when thinking about how it can be used to show to managers how one works best, and the thought that these might not be followed up on raises skepticism on the device. Having individuals defining the purposes of the data collection seem rather important.

Even if these elements seem to point at the need to ask for thorough consent, the notion of consent was mentioned just a few times and only to be rapidly dismissed. For instance, managers from different sections explain that "*As you as you ask for consent, it's okay, no problem"*, and another one says that "*If you ask for consent, it's legal, the rest is a moral problem but legally we are fine"*. It was assumed by participants that asking for consent and staying in the legal limits for hours of monitoring were the only elements they had to comply with to avoid legal and ethical issues. Consent was discussed broadly, even though this does not mean that specific consent was not considered. Rather, the project being at an initial phase, the participants could not yet dwell on details and discuss specific areas where consent would be needed.

The interviews show that for the device to bring the desired outcome, which is reducing stress, devices have to be worn by teams and monitor stress throughout time, possibly at work and outside of work. It gives to the organisation data that can be used

[2] This holds to be true regardless of the format taken by the device: it could be embedded in uniforms, without making the collection of data active by default.

to infer elements about the health of employees, and not only to potentially manage them better. This makes the use of the device sensitive. In order to protect the autonomy of the employees and ensure that they consent to a use of the data that will not trigger harmful consequences for them, we need to find ways to give employees control over what data they want to contribute and to what aim. What is at stake is to avoid the exploitation of employees by organisations. Other fields, such as biobanking, have pushed towards engagement and stakeholder participation for consent [22] for similar reasons. We propose in the next section some reflections on what the ongoing engagement can concern.

4 From Consent to Control

4.1 More Control for More Autonomy

One way to overcome the issues identified in the literature and through the interviews is to give control back to the employees over the usage of the device and of the data that is being collected through the design of flexible data collection plans. Before going further in explaining why this might be beneficial, a few examples illustrating what is meant here by control and flexibility must be given:

- The users decide what hypotheses they want to check with the data that will be collected: they might want to measure their stress levels before and after certain events, in specific team configurations, which they know could be useful in order to obtain useful and meaningful data, i.e. data that can be used to inform workflow management;
- The users have control over the duration of use of the device during the day;
- The users have control over the choice of moments when they want to use the device, and so can stop their use when their experience of the device gets in the way of their work and priorities;
- The users have control over who sees their data;
- The procedure is ongoing and the person responsible for the technology implementation checks at regular intervals how the technology is used by surveying individuals.

This approach requires an ongoing engagement of the (potential) users with the purposes of the data collection. In this way, they can evaluate what are the purposes to be pursued with the data collection in order to protect or increase their autonomy, even though the data collected might be seen as a way of controlling employees[3]. The process, as it is ongoing, allows the users to reflect on the unintended consequences of the data collection and the data aggregation so that they can adapt their use. This can prevent rejecting the system, which comes at cost when it occurs have an organisation has invested in an information system.

[3] This paradox between autonomy and control has been described in the literature (Gilbert and Sutherland, 2013).

For the organisation, giving control to the users (or here research participants) is rather scary. Indeed, it implies the risk of having data that is not easily comparable or statistically significant. Synergies and insights that would make sense at scale might not be revealed by scattered patterns of use. However, it can allow to increase trust significantly: trust in the data as it is willingly given by the employees without forms of misuse[4]; trust in the employees can be perceived as higher as they are given control by the employer; trust in the employer can rise as employees feel heard and respected. Going one step further, the trustworthiness of the employer could increase as the organisation made itself vulnerable to the employees' willingness to collect useful data. These hypotheses are to be validated. Finally, the data collected might be more relevant: instead of relying on data science to identify patterns and potential managerial solutions, such an approach relies on the instincts and needs of workers themselves, who know their own stress and the elements in their work conditions which can be changed (and the ones which cannot). The aggregation of data might help to identify how to compose balanced-teams, or when authorized by the employee, to check whether hypotheses valid for others are also true in their cases. There is a shift between inductive and deductive logic that occurs in how the data is analysed, due to the constraints around consent, which may appeal more to the users as it allows them to use the technology, rather than having the technology use their data to do its work.

4.2 Limits

While such an approach opens new research opportunities as mentioned above, it also raises questions.

Firstly, there are costs due to the organisation of such a process, which are incumbent to the organisation. Indeed, such a scenario comes with more control for users, but is also more demanding of them. It requires that individuals take responsibility about their usage and engage time and cognitive resources in order to understand the information system, its risks and potential advantages, so that they can truly take control over it. This can be a source of stress due to the mismatch between the competencies required from the job and the competencies required to understand the information system. It can be a cost for the organisation as it implies providing training to employees.

Secondly, it needs to be considered whether such an approach is viable through time or if it is meant as a transitory process before gaining a better understanding of how the technology can benefit both employees and the organisation. If it is a transitory process, then the autonomy of employees joining after this initial test phase might be negatively impacted because they had other plans for themselves than the individuals who did participate. As mentioned above, autonomy is socially-embedded and relational, and so mechanisms need to be designed to consider both this social and the

[4] Examples of misuses could be measuring indicators of stress when going up and down the stairs to have a higher heart beat rate and thus give data which might indicate stress which is not related to work.

personal aspects of autonomy. If it is a transitory process, then it becomes difficult to adapt the practice of the technology to the changing environment.

Thirdly, there might be individuals who consent but do not engage fully with the process, so that their point of view is not represented even though from a procedural perspective, these individuals participate.

Fourthly, what about the individuals who decide to not participate and how is their opinion considered?

In such a scenario where the technology might affect work conditions, relationships, is it realistic to proceed without everyone participating? Indeed, we saw earlier that autonomy is socially-embedded, but in many ways also relational. If one person decides to participate, this participation can have an impact on the job conditions of the other person who does not participate, so that non-participation is not a guarantee of status quo. Similarly, when individuals do not participate, the value of the others' participation can decrease as the data is not big enough in order to draw conclusions.

5 Conclusions

We have shown that the simple act of asking for employees' consent to the use of a stress-monitoring wearable is not enough to protect the autonomy of the employees. It is therefore failing at meeting its goal. We introduced the idea of moving from asking consent to giving control to employees themselves by engaging continuously them with the ways in which the data collection occurs and the purposes in which it occurs. This is different from a repeated consent as introducing control gives agency to the individuals. Such approaches can be particularly helpful in order to assess how an existing technology can be used by surveying how it is experienced and best implemented. It is an approach that can be helpful in organisations in order to ensure that technologies are used in a way that solves employee's issues, instead of creating new ones. It might also allow technologies perceived as controlling to help employees to regain more autonomy. The impact of introducing such a process onto trust and trustworthiness need to be assessed, as well as the impact on technology adoption.

Acknowledgements. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 795536. The author also thanks colleagues from 4TU.Ethics Life Science and Healthcare Technology Taskforce and their input during the workshop on the limits of consent.

References

1. Amyx, S.: Privacy dangers of wearables and the internet of things. In: Identity Theft: Breakthroughs in Research and Practice, pp. 379–402. IGI Global (2017)
2. Asveld, L.: Informed consent in the fields of medical technological practice. Techne Res. Philos. Technol. **10**(1), 16–29 (2006)
3. Beauchamp, T.L., Childress, J.F.: Principles of Biomedical Ethics, 6th edn. Oxford University Press, Oxford (2008)

4. D'Arcy, J., Devaraj, S.: Employee misuse of information technology resources: Testing a contemporary deterrence model. Decis. Sci. **43**(6), 1091–1124 (2012)
5. DeSanctis, G., Poole, M.S.: Capturing the complexity in advanced technology use: adaptive structuration theory. Organ. Sci. **5**(2), 121–147 (1994)
6. Engelbart, D.C.: A research center for augmenting human intellect. In: Proceedings of the 9–11 December 1968, Fall Joint Computer Conference, Part I, AFIPS 1968 (Fall, Part I), pp. 395–410. ACM, New York (1962)
7. European Commission. Smart Wearables: Reflection and Orientation Paper (2016)
8. Forsberg, E.-M., Shelley-Egan, C., Thorstensen, E., Landeweerd, L., Hofmann, B.: Evaluating Ethical Frameworks for the Assessment of Human Cognitive Enhancement Applications. SE. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-53823-5
9. Gauttier, S.: I've got you under my skin'–The role of ethical consideration in the (non-) acceptance of insideables in the workplace. Technol. Soc. **56**, 93–108 (2019)
10. Jauréguiberry, F.: Retour sur les théories du non-usage des technologies de communication. In: Proulx, S., Klein, A. (eds.) Connexions: communication numérique et lieu social, pp. 335–350. Presses universitaires de Namur, Namur (2012)
11. Kiran, A.H., Oudshoorn, N., Verbeek, P.P.: Beyond checklists: toward an ethical-constructive technology assessment. J. Responsible Innov. **2**(1), 5–19 (2015)
12. Locke, J.: Two Treatises of Government (1689)
13. Mackay, H., Gillespie, G.: Extending the social shaping of technology approach: ideology and appropriation. Soc. Stud. Sci. **22**(4), 685–716 (1992)
14. More, M.: The philosophy of Transhumanism. In: More, M., Vita- More, N. (eds.) The Transhumanist Reader: Classical and Contemporary Essays on the Science, Technology, and Philosophy of the Human Future, 1 edn. Wiley-Blackwell, Chichester (2013)
15. Muaremi, A., Arnrich, B., Tröster, G.: Towards measuring stress with smartphones and wearable devices during workday and sleep. BioNanoScience **3**(2), 172–183 (2013)
16. O'neill, O.: Autonomy and Trust in Bioethics. Cambridge University Press, Cambridge (2002)
17. O'Connor, S.: Wearables at work: the new frontier of employee surveillance. Financial Times (2015)
18. Parasuraman, R., Riley, V.: Humans and automation: use, misuse, disuse, abuse. Hum. Factors **39**(2), 230–253 (1997)
19. Riemer, K., Johnston, R.B.: Place-making: a phenomenological theory of technology appropriation. In: ICIS Orlando (2012)
20. Sandberg, A.: An overview of models of technological singularity. In: More, M., Vita-More, N. (eds.) The Transhumanist Reader: Classical and Contemporary Essays on the Science, Technology, and Philosophy of the Human Future, 1 edn. Wiley-Blackwell, Chichester (2013)
21. Sarasvathy, S.D.: Effectual reasoning in entrepreneurial decision making: existence and bounds. In: Academy of Management Proceedings, vol. 2001, no. 1, pp. D1–D6. Academy of Management, Briarcliff Manor, August 2001
22. Solberg, B.: Biobank consent models—are we moving toward increased participant engagement in biobanking. J. Biorepository Sci. Appl. Med. **3**, 23–33 (2015)
23. Vijayasarathy, L.R.: Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. Inf. Manage. **41**(6), 747–762 (2004)
24. Weston, M.: Wearable surveillance–a step too far? Strateg. HR Rev. **14**(6), 214–219 (2015)
25. Yang, H., Yu, J., Zo, H., Choi, M.: User acceptance of wearable devices: an extended perspective of perceived value. Telematics Inf. **33**(2), 256–269 (2016)