Step into "The Circle"—A Close Look at Wearables and Quantified Self

Tim Jülicher and Marc Delisle

Abstract Wearables are body-attached computers, such as fitness wristbands, intelligent glasses, or even smart clothes. Approximately 14% of Germans use wearables—particularly to track their personal activity and fitness or to optimize their lives. Related terms are "Quantified Self" and "lifelogging". Not only users, but also manufacturers, service providers, and insurance companies are interested in data collected by wearables. It enables corporate actors to offer individualized insurance tariffs or personalized health services. Important questions do not only relate to data protection and aspects of IT-security, but also to data quality, liability and data portability. However, many users blank out problematic issues of data protection and IT-security—or apply specific strategies of legitimation. For some users, permanent self-tracking is a source of motivation while others feel restricted, overwhelmed, or pressured by it.

1 Introduction

Are you sleeping well? Do you know your blood pressure? And when have you been to see the doctor lately?

Imagine your doctor presents you with a new wristband displaying all your vital functions at a glance. Additionally, you would get a green smoothie containing a tiny, organic sensor. This sensor could transmit essential data like heart rate,

T. Jülicher (✉)
Institute for Information, Telecommunication and Media Law (ITM), University of Münster, Münster, Germany
e-mail: tim.juelicher@uni-muenster.de

M. Delisle
Department for Technology Studies, University of Dortmund, Dortmund, Germany
e-mail: marc.delisle@tu-dortmund.de

T. Hoeren and B. Kolany-Raiser (eds.), *Big Data in Context*,
SpringerBriefs in Law, https://doi.org/10.1007/978-3-319-62461-7_10

blood pressure, cholesterol, calorie consumption, quality of sleep, nutritional efficiency and much more directly to your wristband.[1]

This self-tracking scenario marks the beginning of the dystopian novel "The Circle". In reality, one does not need a green smoothie or an organic sensor. Actually, a huge number of so-called wearables already exists—most of them are able to collect and analyze vital data in real-time. Likewise, data-collecting health and fitness apps are no rarity anymore. But which challenges come along with this development?

To answer this question, we will shed light on some areas of application and focus on the potentials and risks in the age of big data.

2 What Are Wearables?

When companies such as Pulsar and Casio released the first calculator watches in the 1970s and 80s, the term wearable computer did not exist yet. Back then, it was only a niche product at the most. Today—40 years later—wearables have arrived in the mainstream due to wireless data transfer (Bluetooth, WiFi, cellular) and the constantly growing power of processors. Wearables are body-attached computers. They are part of the internet of things and therefore contribute to ubiquitous computing. Nowadays, there are different types of wearables:

- *Smartwatches*, i.e. wristwatches with computer functionality, sensors and smartphone connectivity
- *Activity trackers*, in particular fitness wristbands: recording activity and health data (for example the daily number of steps, heart rate, energy consumption)
- *Glasses* with computer functionality und connectivity showing information in the (peripheral) field of vision (for instance Google Glass, Recon Snow2).

These examples correlate with the prediction of the American computer scientist Mark Weiser, who stated in 1991: "In the 21st century the technology revolution will move into the everyday, the small and the invisible." In fact, the current development shows that the next generation of wearables will be even more inconspicuous, efficient and body-integrated:

- Google and Novartis are working on an *intelligent contact lens* (so-called smart lens), that can measure the level of blood sugar on the basis of tear fluid and shall balance age-related debility of sight.[2]

[1] Eggers 2013, The Circle, p 154 et seqq.

[2] King 2014, Forbes Tech July 2015, http://www.forbes.com/sites/leoking/2014/07/15/google-smart-contact-lens-focuses-on-healthcare-billions/.

- *Biosensors* shall enable the analysis of sweat flow[3] and *smart tattoos* are supposed to provide the necessary electricity for wearables, smartphones and other devices directly out of the sweat.[4]
- *Intelligent socks, gloves and textiles* promise an improvement in medical precaution, for example both in the area of early detection of breast cancer[5] or amputations due to diabetes.[6] Another field of improvement lies in the care sector, fostering the supervision of Alzheimer's patients.[7]

All wearables have in common that they collect and process user-specific data. The scope of processing may vary from visual illustration to user feedback or even concrete recommendations for action.

3 Facts and Figures

According to a recent consumer survey of the Federal Ministry of Justice and Consumer Protection, approximately 14% of Germans use wearables and apply them for activity and fitness tracking.[8] Most of the gadgets are lifestyle products targeting the consumer market. Therefore, the digital industrial agency BITKOM classifies them as consumer electronics. The association estimated that 1.7 million gadgets were sold in 2015.[9]

However, wearable technology should no longer be seen as a mere lifestyle trend but as an influencing factor for a change of self-awareness. The underlying movement is called Quantified Self and aims at gaining knowledge from data with the objective of improving quality of life.[10]

4 Kinds of Data Generated

While using wearables, huge amounts of data are generated. They can be distinguished as follows:

[3] Gao et al. 2016, Nature 529(7587), p 509 et seqq.

[4] Jia et al. 2013, Angewandte Chemie 52(28), p 7233 et seqq.

[5] Almeida 2015, UbiComp/ISWC'15 Adjunct, p 659.

[6] Perrier et al. 2014, IRBM 2013(35), p 72.

[7] Scheer/Sneed 2014, Sci Am 311(4), p 20.

[8] BMJV 2016, Wearables und Gesundheits-Apps, p 4 et seq.

[9] Börner 2015, Marktentwicklung und Trends in der Unterhaltungselektronik, p 12 et seq.

[10] Kamenz (2015), Quantified Self, p 2.

4.1 Usage Data

Usually, to register and configure a wearable gadget you will have to enter certain personal details, such as name, sex, weight and an invoice address. This kind of (static) information is mostly mandatory to create a user profile. While using the gadget, more and more (dynamic) information will be gathered about the user by using cameras, sensors or user input. In case of wristbands or intelligent textiles, this could be vital data, location data, or acceleration data for instance.

From this data pool, conclusions can be drawn about calorie consumption or physical fitness. At the same time, there is an underlying risk of creating movement profiles and unwanted insights into personal habits, preferences and behavioral patterns. Gadgets that do not only monitor the user himself but also his surroundings (for instance through video cameras, audio recordings or temperature measurements) go far beyond this.

4.2 Metadata

Metadata in the context of wearables are device-specific data (producer, model or identification number), communications data (IP-address or connection time) and information about the duration of use and its intensity. Even without consideration of the aforementioned usage data, metadata often allow the (re-)identification of a user and monitoring his individual usage behavior.

5 What Is the Data Used for?

The collection of bio-signals such as heart rate, blood sugar level, or brain activity makes it possible to discover new patterns that are invisible so far. Algorithms allow for the analysis of physical performance and may lead to a better understanding of the own body. The data generated by wearables can be divided into two categories:

Body & health data and *presence & absence data.*[11] Body and health data focus on vital monitoring of the own body by comparing individual values with default and average values. The aim is to define risks and limits and, if necessary, to propose a behavioral change. However, in most cases it is very difficult for users to understand how standard values are determined.[12] The guiding principle is to make the own life even more perfect, more streamlined and more efficient and to try to free oneself from the trap of dependence on conventional medicine.[13]

[11] Selke 2014, Lifelogging, p 177.

[12] Leger et al. 2016, Datenteilen, p 11.

[13] Selke 2014, Lifelogging, p 178.

Thereby, wearables can motivate generally healthy users to stay or get active. Another promise of wearables is to simplify medical monitoring for patients who suffer from chronic conditions such as diabetes or apnea.[14]

A similar type of wearable device that is being developed currently addresses the early detection of Parkinson by means of microanalysis.[15]

While wearables are becoming increasingly popular with private individuals to optimize their own performance, the field of professional application—especially with regard to medical scenarios—is rather limited so far. Most of the solutions mentioned above are at an early developmental stage and far off from being approved for medical use.[16] Furthermore, there are few reliable studies regarding the quality of data (see below). Even though wearables allow a more autonomous access to body knowledge without relying on medical and scientific staff, users have no influence on the interpretation and evaluation of their data. Thereby, a core piece of the whole process is still controlled by others.

Further questions regarding the impact on the user’s individual health and wellbeing remain to be assessed.[17] When it comes to potential addictions to devices, a false sense of security or the risk of false self-diagnostics, further research is needed.[18] Likewise, negative consequences like discomfort and (perceived) restrictions, generated by wearables, are discussed.[19]

Alongside body data, many wearables record location and geo data—often unnoticed by the users. These sources can be used to calculate the distance travelled, to determine the user’s location or for surveillance purposes. Together with the aforementioned metadata, this poses a challenge for present data protection measures. De Montjoye et al. have shown that four location-time-points are sufficient to identify a person.[20]

6 Legal and Social Implications

In legal terms, the use of wearables constitutes two dimensions:[21] Voluntarily used devices that are restricted to self-monitoring affect the freedom of action and the right to informational self-determination (Art. 2 par. 1, Art. 1 par. 1 GG). The situation is different with devices that are used (a) involuntarily and/or (b) to monitor not only the user but also his surroundings. In this case, there is a risk of

[14] Piwek/Ellis/Andrews/Joinson 2015, PLoS Med 13(2), p 3.

[15] Arora et al. 2014, IEEE 2014, p 3641 et seqq.

[16] Piwek et al. 2015, PLoS Med 13(2), p 4.

[17] Piwek et al. 2015, PLoS Med 13(2), p 4.

[18] Goyder/McPherson/Glasziou 2009, BMJ 2010 (340), p 204 et seqq.

[19] O’Kane et al., BMJ 2008 (336), p 1174.

[20] De Montjoye/Hidalgo/Verleysen/Blondel 2013, Scientific Reports 3, p 1376.

[21] Zoche et al., White Paper, p 28 et seq.

violating the user's and other individuals' personal rights. Apart from this underlying risk of exposure, the use of wearable devices raises legal questions, inter alia, within the following areas:

6.1 Data Protection

From a privacy perspective, the huge number of actors involved poses a significant challenge: The use of wearable devices does not only involve the owner/user, but also the manufacturer, third-party providers and most likely other intermediaries (such as insurance companies, scientists or advertising companies). To make things worse, data is often not stored locally or processed by the device itself, but forwarded to a cloud service that is possibly located in non-European countries.

Since user data has to be considered as personal data in terms of sections 3 subs. 1 BDSG[22] and Art. 4 no. 1 GDPR,[23] this issue is governed by German and European data protection law. Therefore, processing the data is only lawful if the data subject (i.e. the user) has given consent or if it is in compliance with a statutory permission (cf. section 4 subs. 1 BDSG and Art. 6 para. 1 GDPR). But even those users who take it upon themselves to read multi-page privacy policies have difficulties to assess what actually happens to their data. That challenges core principles of data protection such as purpose limitation, transparency, and data minimization considerably.

In addition, special requirements must be met in order to lawfully process health-concerning data collected by fitness devices. Depending on the field of application, further requirements have to be taken into consideration. That applies particularly to wearables in the employment context[24] as well as health and fitness apps.[25]

Even if most users are aware of these issues, they legitimate their quantified self through various strategies:

First of all, they split the data into parts worth protecting and not worth protecting—more specifically personal and non-personal data. These individual decisions may differ from legal definitions. Leger et al. state that private e-mails, Facebook messages, private photos and body data, such as blood pressure and pulse, are classified as personal data.[26] In contrast, most users would consider the disclosure of non-personal data, such as the running track or the daily calorie consumption, as unproblematic. This may cause problems when the device collects data that are regarded worth protecting. In this case, many users construct an overpowering and pervasive counterpart that seems to know everything about them.

[22] German federal data protection act.

[23] EU General Data Protection Regulation.

[24] Kopp/Sokoll, NZA 2015, p 1352.

[25] Jandt/Hohmann, K&R 2015, p 694.

[26] Leger et al. 2016, Datenteilen, p 6.

Against this background tracking and quantifying oneself would not make any difference. If this argument were followed strictly, the only way to protect private data would be the unconditional non-use of cross-linked devices.[27]

Another reason for the practice of sharing data—regardless of a certain level of problem awareness—is the facilitation of quantified self through wearables.[28] Apps in general and wearables in particular offer a noticeable degree of convenience in measuring activities that could otherwise only be recorded with great effort. In this regard, Hänsel et al. point out the influence of gamification, i.e., the application of typically game-related elements in different contexts.[29] The integration of playful elements appeals to both intrinsic driving forces, such as joy, and extrinsic motivational incentives, such as rewards or awards, that lead to a use of wearables and the (voluntary) disclosure of data.[30] In this context, users consider the provision of data as a sort of payment for the (usually free) apps and services.

Besides, engaging in a comparison to others is seen as a mandatory and objective standard to assess one’s performance. Thus, own data must inevitably be revealed to enable a comparison with oneself, with others and with standardized indices.[31]

While wearables pose a number of questions with regard to privacy, users appear to have developed strategies in order to justify the practices of sharing and analyzing data for themselves.

6.2 Liability

Wearable devices raise a number of questions with regard to liability. That relates to product and manufacturer’s liability in particular.

In 2014, US authorities ordered a recall of the popular fitness wristband Fitbit Force as it caused allergic reactions with several users.[32] Beyond such rather ordinary problems, we face specific liability scenarios: Where datasets from wearable devices are used to calculate insurance rates or to monitor vital functions, accuracy and reliability are crucial factors. In these cases, inaccurate information can give rise to both contractual and tortious liability claims. Loss and abuse of (personal) data as well as making it available to third parties are further problems that need to be considered carefully.

[27] Heller 2011, Post-Privacy, p 14.

[28] Leger et al. 2016, Datenteilen, p 8; Lupton (2015), Culture, Health & Sexuality 2015(17), p 1352 et seqq.

[29] Hänsel 2016, arXiv:1509.05238, p 1 et seqq.

[30] Hänsel 2016, arXiv:1509.05238, 2; Robson et al. (2015), Business Horizons 2015(58), p 412 et seqq.

[31] Gilmore 2015, new media & society 2015, p 5 et seqq.; Leger et al., Datenteilen; Püschel (2014), Big Data und die Rückkehr des Positivismus.

[32] Kim 2016, Business Law Journal, https://publish.illinois.edu/illinoisblj/2016/02/29/new-legal-problems-created-by-wearable-devices/#_ftn25.

Apart from civil claims, there is a significant risk of criminal liability for manufacturers as devices may malfunction or misinterpret data.[33]

6.3 IT Security

According to an investigation by the cybersecurity company Symantec, many wearables do not meet common safety standards. The data are often transferred unencrypted between terminal devices (e.g. wearable and smartphone) and may therefore be visible to third parties. Sometimes, not even the connection between smartphone and server is encrypted sufficiently.[34] The manufacturers should therefore take adequate technical measures to guarantee that data is collected, transferred and processed securely (particularly by end-to-end encryption). This counts even more, when data are transmitted abroad.

6.4 Data Quality, Portability and Property

Professional users often criticize the quality of the data collected by wearable devices. Some medical professionals have even gone so far as to say that tracking data in patient files would be nothing but "data garbage".[35] Actually, wrong measurements are widely perceived as problematic[36] and indeed, a large number of fitness wristbands, smartwatches and the like provide rather unreliable data.[37]

Furthermore, many manufacturers use proprietary systems to collect and process data, which leads to interoperability issues. For users who want to switch their provider or use another system, it is difficult to find out where the data is stored. Fortunately, the General Data Protection Regulation will improve the user's legal position by introducing a right to data portability (Art. 20 par. 1 GDPR). While the scope of this right remains to be discussed, its implementation certainly promotes the discussion about economic value of data, data ownership, and power of disposition.[38]

[33] Kim 2016, Business Law Journal, https://publish.illinois.edu/illinoisblj/2016/02/29/new-legal-problems-created-by-wearable-devices/#_ftn25.

[34] Symantec 2014, How safe is your quantified self? http://www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech.

[35] Becker 2016, Süddeutsche Zeitung vom 9 Feb 2016, p 1.

[36] BMJV 2016, Wearables und Gesundheits-Apps, p 9.

[37] Case et al., The Journal of the American Medical Association 2015 (313), p 625 et seq.

[38] Jülicher/Röttgen/v. Schönfeld 2016, ZD 6(8), p 358 et seqq.; Moos (2016), E-Commerce Law & Policy 18(2), p 9 et seq.

7 Conclusion

A growing number of people are using wearables. So far they have been perceived primarily as fitness and lifestyle gadgets. However, their potential lies in professional and medical areas of application—for instance in preventing diseases. Even though many people can imagine a scenario in which their vital data is transmitted to a doctor, many express their skepticism. About one third of the German population emphasizes: "My health data is nobody's business but mine".[39]

Notwithstanding this skepticism, we can observe that a vast majority of users already uses sharing features—rather to share their data with device manufacturers, service providers and third parties than with their doctors. This paradox—as it seems—requires a public discourse about which data are regarded worth protecting and how the individual user can be safeguarded by legal measures. Particularly, developers and producers have to figure out ways to provide adequate IT security standards. Moreover, they should enter into an active dialogue with users and other stakeholders.

References

Almeida T (2015) Designing intimate wearables to promote preventative health care practices. In: UbiComp/ISWC'15 Adjunct, pp 659–662. doi: 10.1145/2800835.2809440

Arora S et al. (2014) High accuracy discrimination of Parkinson's disease participants from healthy controls using smartphones. In: 2014 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE

Becker K (2016) Kassen wollen Daten von Fitness-Armbändern nutzen. Süddeutsche Zeitung, 9 Feb, p 1

BMJV (2016) Wearables und Gesundheits-Apps. https://www.bmjv.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/YouGov.pdf. Accessed 4 Apr 2017

Börner M (2015) Marktentwicklung und Trends in der Unterhaltungselektronik. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/09-September/Bitkom-Praesentation-PK-CE-01-09-2015.pdf. Accessed 4 Apr 2017

Case M, Burwick H, Volpp K, Patel M (2015) Accuracy of smartphone applications and wearable devices for tracking physical activity data. J Am Med Assoc 313(6):625–626

De Montjoye Y-A et al (2013) Unique in the crowd: the privacy bounds of human mobility. Sci Rep 3:1376

Eggers D (2013) The circle. Random House, New York

Gao W et al (2016) Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis. Nature 529(7587):509–514. doi:10.1038/nature16521

Gilmore JN (2015) Everywear: the quantified self and wearablefitness technologies. New Media Soc doi: 10.1177/1461444815588768

Goyder C et al (2009) Self diagnosis. BMJ 339(1):b4418

Hänsel K et al (2016) Wearable computing for health and fitness: exploring the relationship between data and human behaviour. arXiv preprint arXiv:1509.05238

Heller C (2011) Post-privacy: prima leben ohne Privatsphäre. CH Beck, München

[39] BMJV 2016, Wearables und Gesundheits-Apps, p 10.

Jandt S, Hohmann C (2015) Fitness- und Gesundheits-Apps—Neues Schutzkonzept für Gesundheitsdaten? K&R 2015(11):694–700

Jia W, Valdés-Ramírez G, Bandodkar A, Windmiller J, Wang J (2013) Epidermal biofuel cells: energy harvesting from human perspiration. Angew Chem 52(28):7233–7236. doi:10.1002/anie.201302922

Jülicher T, Röttgen C, van Schönfeld M (2016) Das Recht auf Datenübertragbarkeit—Ein datenschutzrechtliches Novum. ZD 6(8):358–362

Kamenz A (2015) Quantified Self Anspruch und Realität

Kim Y (2016) New legal problems created by wearable devices. Illinois Bus Law Journal. https://publish.illinois.edu/illinoisblj/2016/02/29/new-legal-problems-created-by-wearable-devices/#_ftn25. Accessed 4 Apr 2017

King L (2014) Google smart contact lens focuses on healthcare billions. Forbes Tech July 15. http://www.forbes.com/sites/leoking/2014/07/15/google-smart-contact-lens-focuses-on-healthcare-billions/. Accessed 4 Apr 2017

Kopp R, Sokoll K (2015) Wearables am Arbeitsplatz—Einfallstore für Alltagsüberwachung? NZA 32(22):1352–1359

Leger M et al (2016) Ich teile, also bin ich—Datenteilen als soziale Praktik. Daten/Gesellschaft, Aachen

Lupton D (2015) Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. Culture Health Sex 17(4):440–453

Moos F (2016) The troubling reach of the GDPR right to data portability. E-Comm Law Policy 18 (2):9–10

O'Kane MJ et al (2008) Efficacy of self monitoring of blood glucose in patients with newly diagnosed type 2 diabetes (ESMON study): randomised controlled trial. BMJ 336(7654): 1174–1177

Perrier A, Vuillerme N, Luboz V et al (2014) Smart diabetic socks: embedded device for diabetic foot prevention. IRBM 2013(35):72–76

Piwek L et al (2015) The rise of consumer health wearables: promises and barriers. PLoS Med 13 (2):e1001953. doi:10.1371/journal.pmed.1001953

Püschel F (2014) Big Data und die Rückkehr des Positivismus. Zum gesellschaftlichen Umgang mit Daten. http://www.medialekontrolle.de/wp-content/uploads/2014/09/Pueschel-Florian-2014-03-01.pdf. Accessed 4 Apr 2017

Robson K et al (2015) Is it all a game? Understanding the principles of gamification. Bus Horiz 58 (4):411–420

Scheer R, Sneed A (2014) Safety in a sock. Sci Am 311(4):20

Selke S (2014) Lifelogging als soziales Medium?—Selbstsorge, Selbstvermessung und Selbstthematisierung im Zeitalter der Digitalität. Technologien für digitale Innovationen. Springer, Wiesbaden, pp 173–200

Symantec (2014) How safe is your quantified self? Tracking, monitoring, and wearable tech. http://www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech. Accessed 4 Apr 2017

Author Biographies

Tim Jülicher B.A., Dipl.-Jur., research associate at the Institute for Information, Telecommunication and Media Law (ITM) at the University of Münster. He holds degrees in law and political sciences from the University of Münster.

Marc Delisle Dipl.-Ökon., research associate at the Department for Technology Studies at the University of Dortmund. He completed his studies in economics and social science at the University of Dortmund.