Step Into »The Circle« – Wearables und Selbstvermessung im Fokus

Marc Delisle, Wirtschafts- und Sozialwissenschaftliche Fakultät, Technische Universität Dortmund, &
Tim Jülicher, Institut für Informations-, Telekommunikations- und Medienrecht (ITM),
Westfälische Wilhelms-Universität Münster

1 Einführung

Schlafen Sie gut? Kennen Sie Ihren Blutdruck? Und wann waren Sie eigentlich das letzte Mal beim Arzt? Stellen Sie sich vor, Ihr Arzt würde Ihnen ein neues Armband präsentieren, mit dem Sie sämtliche Vitalfunktionen im Blick hätten. Dazu erhielten Sie noch einen grünen Smoothie, mit dem Sie einen winzigen, organischen Sensor aufnähmen. Dadurch könnten Daten über Herzfrequenz, Blutdruck, Cholesterin, Kalorienverbrauch, Schlafqualität, Verdauungseffizienz und vieles mehr direkt an ihr Armband übertragen werden (Eggers 2014: 154ff.).

Was im Roman „The Circle" den Auftakt zu einer Dystopie der Selbstüberwachung bildet, erfordert in der Realität noch nicht einmal einen grünen Smoothie, geschweige denn einen organischen Sensor. Tatsächlich gibt es bereits eine ganze Reihe sogenannter Wearables, die Vitaldaten erfassen, aufzeichnen und analysieren können. Auch Gesundheits-, Wellness- und Fitness-Apps sind heutzutage keine Seltenheit mehr. Doch welche Herausforderungen gehen mit dieser Entwicklung einher? Hierzu sollen im Folgenden ausgewählte Anwendungsbereiche vorgestellt und ein Schlaglicht auf die Potentiale und Risiken im Zeitalter von Big Data geworfen werden.

2 Was sind Wearables?

Als die Unternehmen Pulsar und Casio in den 1970er und 80er Jahren die ersten Taschenrechner-Uhren auf den Markt brachten, gab es den Begriff des Wearable Computers noch nicht. Damals handelte es sich allenfalls um ein Nischenphänomen. Heute – vierzig Jahre später – sind Wearables dank kabelloser Daten-

Auf einen Blick: Wearables

- Wearables bezeichnen am Körper getragene Computer wie etwa Fitnessarmbänder, intelligente Brillen oder neuerdings auch smarte Kleidungsstücke.
- **Rund 14% der Deutschen nutzen Wearables**, vor allem zum persönlichen Aktivitäts- und Fitnesstracking sowie zur Optimierung des eigenen Lebens. Experten sprechen von Quantified Self, Life Logging und Selbstvermessung.
- Nicht nur Nutzer, sondern auch Hersteller, Dienstleister oder Versicherungen haben Interesse an den Nutzerdaten. So lassen sich beispielsweise individualisierte Versicherungstarife anbieten oder maßgeschneiderte Gesundheitsdienstleistungen realisieren.
- Wichtige Fragen betreffen nicht nur den **Datenschutz** und Aspekte der **IT-Sicherheit**, sondern auch Fragen der **Datenqualität**, der **Haftung** und der **Datenübertragbarkeit.**
- Die Fragen des Datenschutzes und der IT-Sicherheit werden von einem Großteil der Nutzer durch verschiedene **Legitimierungsstrategien** entschärft.
- Die permanente Selbstvermessung wirkt auf einen Teil der Nutzer motivierend, während andere sich eingeschränkt und unter Druck gesetzt fühlen.

übertragung (Bluetooth, Wifi, Mobilfunk) und stetig wachsender Prozessorleistung im Mainstream angelangt. Es handelt sich um am Körper getragene Geräte, die Teil des Internets der Dinge (Internet of Things) und Ausdruck der Allgegenwart von Computern (Ubiquitous Computing) sind. Mittlerweile sind die Erscheinungsformen von Wearables im Konsumentenbereich vielfältig:

- **Smartwatches**: Armbanduhren mit Computerfunktionalität, Sensoren und Smartphone-Konnektivität
- **Activity Tracker**, insbesondere Fitnessarmbänder: Aufzeichnung aktivitäts- und gesundheitsbezogener Daten (z.B. Schrittzahl, Herzfrequenz oder Energieumsatz)
- **Brillen** mit Computereigenschaften und -konnektivität, die Informationen im (peripheren) Sichtfeld einblenden (z.B. Google Glass, Recon Snow2), teils mit eingebauter Digitalkamera

Tatsächlich sind diese Beispiele nicht weit entfernt von der Prognose des US-amerikanischen Informatikers Mark Weiser, der 1991 feststellte: „In the 21st century the technology revolution will move into the everyday, the small and the invisible." Und die aktuelle Entwicklung zeigt, dass die nächste Generation der Wearables noch unscheinbarer, leistungsfähiger und körperintegrativer sein wird:

- Google und Novartis arbeiten an einer **intelligenten Kontaktlinse (Smart Lens)**, mithilfe derer sich der Blutzuckerspiegel anhand der Tränenflüssigkeit messen und Sehschwächen im Alter ausgleichen lassen sollen (King 2014).
- **Biosensoren** sollen die Analyse des Schweißflusses ermöglichen (Gao et al. 2016: 509) und **„smarte Tattoos"** die notwendige Elektrizität für Wearables, Smartphones und Co. direkt aus dem Schweiß liefern (Jia et al. 2013: 7233).
- **Intelligente Socken, Handschuhe und Textilien** versprechen eine Verbesserung der medizinischen Vorsorge, etwa im Bereich der Brustkrebsfrüherkennung (Almeida 2015: 659) oder diabetesbedingter Amputationen (Perrier et al. 2014: 72), sowie bei der Betreuung und Pflege von Senioren, beispielsweise bei der Überwachung von Alzheimer-Patienten (Scheer & Sneed 2014: 20).

Allen Wearables ist gemein, dass diese nutzerspezifische Daten erheben und auswerten. Die Auswertungsergebnisse reichen dabei von einer schlichten visuellen Aufbereitung der Daten über Feedback bis zu konkreten Handlungsempfehlungen.

3 Daten, Fakten und Trends

Nach einer repräsentativen Verbraucherbefragung des Bundesjustiz- und Verbraucherministeriums **nutzen rund 14% der Deutschen Wearables** und setzen diese vor allem zum Aktivitäts- und Fitnesstracking ein (BMJV 2016: 4f.). Die meisten Geräte zielen insoweit auf den Privatkundenmarkt ab und werden primär als Lifestyle-Produkte wahrgenommen. So zählt sie der Branchenverband BITKOM zum Bereich der Unterhaltungselektronik und rechnete für 2015 mit 1,7 Millionen verkauften Geräten (Börner 2015: 12f.).

Die oben beschriebenen Technologien entwickeln sich darüber hinaus derzeit von einem Lifestyle-Produkt zu einer eigenen Bewegung, die sich als **Quantified Self** bezeichnet. Das oberste Ziel dieser Quantified Self-Bewegung ist der Erkenntnisgewinn aus Daten und die damit verbundene Hoffnung auf eine höhere Lebensqualität (Kamenz 2015: 2).

4 Welche Daten werden generiert?

Bei der Verwendung von Wearables fallen zahlreiche Daten an. Sie lassen sich grundsätzlich wie folgt unterscheiden:

a) Nutzungsdaten

Zur Registrierung und Konfiguration der Geräte sind regelmäßig Angaben zur Person (z.B. Name, Geschlecht, Geburtsdatum, Gewicht, Rechnungsanschrift) erforderlich, die in einem Nutzerprofil gespeichert werden. Im Zuge der Gerätenutzung werden sodann durch Kame-

ras, Sensoren oder Benutzereingaben kontinuierlich weitere Informationen über den Träger und seine Umgebung erfasst und analysiert. Bei Fitnessarmbändern und intelligenten Textilien können dies etwa Vital-, Standort- oder Beschleunigungsdaten sein. Aus ihnen lassen sich beispielsweise Rückschlüsse auf den Kalorienverbrauch und die körperliche Fitness ziehen. Zugleich erlauben sie aber auch die Erstellung von Bewegungsprofilen und geben Einblick in persönliche Lebensgewohnheiten, Präferenzen und Verhaltensweisen. Geräte, die nicht nur den Nutzer selbst, sondern auch dessen Umgebung überwachen (etwa durch Videokameras, Audioaufnahmen oder Temperaturmessungen), gehen darüber weit hinaus.

b) Metadaten

Zu den sog. Metadaten zählen im Kontext von Wearables insbesondere gerätespezifische Daten (Hersteller, Modell, Identifikationsnummer), Kommunikationsdaten (IP-Adresse, Verbindungsdauer) und Informationen zur Nutzungsdauer und -intensität. Sie erlauben nicht selten – unabhängig von den zuvor genannten Nutzungsdaten – die Identifikation des Trägers und eine Überwachung seines Nutzungsverhaltens.

5 Verwendungszwecke

Durch die Erfassung von Bio-Signalen wie Herzfrequenz, Blutzuckerspiegel oder Gehirnaktivitäten sollen bislang unsichtbare Muster und Regelmäßigkeiten der leiblichen Performanz offengelegt werden, die zu einem besseren Verständnis des (eigenen) Körpers führen sollen. Die aus Wearables gewonnen Daten lassen sich in zwei Kategorien einteilen: Körper- und Gesundheitsdaten sowie An- und Abwesenheitsdaten (Selke 2014: 177). Bei den Körper- und Gesundheitsdaten stehen die Vitaldaten des eigenen Körpers im Mittelpunkt. Diese werden mit Norm- und Mittelwerten abgeglichen, um Risiko- und Grenzwerte zu definieren und gegebenenfalls eine Verhaltensänderung vorzuschlagen. Allerdings bleibt für den Nutzer häufig unklar, wie die Normwerte zustande kommen (Leger et al. 2016: 11). Der Leitgedanke zur Erhebung dieser Daten ist sowohl „[…] das eigene Leben noch perfekter, stromlinienförmiger und effizienter gestalten zu können[…]“ als auch der Versuch der „[…] Befreiung aus der Abhängigkeitsfalle von der Schulmedizin“ (Selke 2014: 178).

Damit können Wearables einerseits prinzipiell gesunde Nutzer durch die Quantifizierung ihrer Aktivtäten motivieren, weiter aktiv zu bleiben bzw. zu werden. Andererseits versprechen Wearables – unter anderem aufgrund ihrer geringen Größe – Nutzern, die beispielsweise an Diabetes oder Schlaf-Apnoe erkrankt sind, eine vereinfachte und wenig anspruchsvollere Überwachung ihrer Symptome (Piwek et al. 2015: 3).

Zusätzlich werden derzeit Wearables entwickelt, die eine Früherkennung von Parkinson anhand von Mikroanalysen ermöglichen sollen (Arora et al. 2014). Während Wearables sich im privaten Bereich zur Optimierung der eigenen Leistungsfähigkeit immer größerer Beliebtheit erfreuen, bleiben die Einsatzmöglichkeiten in medizinischen Fällen limitiert. Die meisten der oben genannten Lösungen befinden sich noch in der Entwicklungsphase und sind noch nicht für den medizinischen Gebrauch zugelassen (Leger et al. 2016; Piwek et al. 2015). Auch gibt es bislang wenige reliable Studien bezüglich der Datenqualität (s.u.). Auch wenn Wearables einen autonomeren Zugang zu Körperwissen, ohne auf ärztliches oder medizinisch-wissenschaftliches Personal angewiesen zu sein, ermöglichen, bleibt die Interpretation und Auswertung der Daten weiterhin außerhalb der Einflussnahme der Nutzer. Damit liegt ein zentraler Teil des gesamten Prozesses noch in den Händen anderer.

Auch sind weitere Fragen, die einen Einfluss auf die Gesundheit und das Wohlbefinden der Nutzer bislang ungeklärt (Piwek et al. 2015: 4). Dies betrifft etwa die mögliche Gefahr einer Abhängigkeit der Nutzer von den Geräten, ein eventuelles falsches Gefühl von Sicherheit oder das Risiko von falschen Selbstdiagnosen (Goyder et al. 2009). Ebenso werden negative Konsequenzen, wie Unwohlsein und (gefühlte) Einschränkungen durch Wearables, diskutiert (O'Kane et al. 2008)

Neben den Körperdaten erfassen viele Wearables – teilweise von den Nutzern unbemerkt – Orts- und Geodaten. Diese können zur Berechnung der zurückgelegten Strecke, zur einfachen Standortbestimmung oder zum Schutz bzw. zur Überwachung von Personen ge-

nutzt werden. Besonders diese, in Verbindung mit den erzeugten Metadaten (s.o.), stellen bisherige Maßnahmen zum Datenschutz wie Anonymisierung vor Herausforderungen. De Montjoye/Hidalgo et al. (2013) haben gezeigt, dass vier Raum-Zeitpunkte ausreichen um eine Person zu identifizieren.

6 Rechtliche und soziale Implikationen

In rechtlicher Hinsicht sind zwei Dimensionen der Nutzung von Wearables zu unterscheiden (Zoche et al. 2015: 28f.): Ein Gerät, das freiwillig eingesetzt wird, um zum Zwecke der Selbstoptimierung Daten über den Träger zu sammeln und zu analysieren, berührt zunächst einmal nur den Schutzbereich der allgemeinen Handlungsfreiheit und des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Anders verhält es sich dagegen bei Geräten, die (a) nicht aus freien Stücken getragen werden und/oder (b) nicht nur den Träger, sondern auch dessen Umfeld überwachen. Hier kann es allem voran zu einer Verletzung eigener und fremder Persönlichkeitsreche kommen. Im Übrigen wirft die Nutzung von Wearables Rechtsfragen u. a. in folgenden Bereichen auf:

a) Datenschutz

In datenschutzrechtlicher Hinsicht stellt zunächst die Vielzahl der beteiligten Akteure eine wesentliche Herausforderung dar: So sind neben dem Nutzer regelmäßig der Hersteller, Drittanbieter und unter Umständen weitere Intermediäre (wie etwa Versicherungsunternehmen, Wissenschaftler oder Werbeunternehmen) involviert. Die Daten werden oft nicht lokal auf dem Gerät, sondern dezentral in der Cloud – womöglich im außereuropäischen Ausland – gespeichert und verarbeitet. Im Grundsatz gilt dabei: Viele Nutzungsdaten sind als personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG bzw. Art. 4 Nr. 1 DSGVO zu qualifizieren, womit der Anwendungsbereich des deutschen bzw. europäischen Datenschutzrechts eröffnet ist. Dies ist per se nur mit einer Einwilligung des betreffenden Nutzers oder beim Eingreifen einer Erlaubnisnorm möglich (vgl. § 4 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. a DSGVO). Doch selbst für Nutzer, die sich mit mehrseitigen Datenschutzerklärungen auseinandersetzen, ist nicht immer ersichtlich, was mit ihren Daten geschieht und wo sie gespeichert werden. Zentrale Grundsätze des Datenschutzrechts (Zweckbindung, Transparenz, Datensparsamkeit) werden dadurch in Frage gestellt. Hinzu kommt, dass für die Verarbeitung von gesundheitsbezogenen Daten – wie sie etwa von Fitnessarmbändern gesammelt werden – besondere Anforderungen zu beachten sind. Je nach Einsatzbereich können weitere Zulässigkeitsvoraussetzungen zu berücksichtigen sein. Exemplarisch sei hier der Einsatz von Wearables in Beschäftigungsverhältnissen genannt (Kopp & Sokoll 2015: 1352). Ähnliches gilt für Gesundheits- und Fitness-Apps, die sich gegenwärtig noch in einer rechtlichen Grauzone bewegen (Jandt & Hohmann 2015: 694).

Auch wenn den meisten Nutzern die geschilderte Datenschutzproblematik durchaus bewusst ist, legitimieren diese ihre Selbstvermessung durch unterschiedliche Strategien.

Zunächst unterteilen sie die erhobenen Daten in für sie persönlich schützenswerte und nicht-schützenswerte Daten bzw. persönliche und nicht-persönliche Daten. Diese individuell getroffenen Unterscheidungen divergieren teilweise von juristischen Legaldefinitionen. Leger et al. (2016) konstatieren, dass private E-Mails, Facebook-Nachrichten, private Fotos und Körperdaten wie Blutdruck oder Puls als persönliche Daten eingestuft werden (6). Die Preisgabe von unpersönlichen bzw. nicht-schützenswerten Daten, wie bspw. der Laufstrecke oder dem täglichen Kalorienverbrauch, wird von den meisten Nutzern hingegen als unproblematisch angesehen. Dies kann dann jedoch zu kurz greifen, wenn von den Wearables als schützenswert angesehene Daten erhoben werden, dann konstruieren viele Nutzer ein übermächtiges und allgegenwärtiges Gegenüber, das bereits alles über einen wisse. Daher mache die Selbstvermessung keinen Unterschied mehr. Dieser Argumentation folgend, sei der einzige Weg zum Schutz privater Daten lediglich der Totalverzicht auf vernetzte Geräte (Heller 2011: 14).

Ein weiterer Grund für die Praktik des Datenteilens – trotz vorhandenen Problembewusstseins – ist die Erleichterung der Selbstvermessung durch Wearables

(Leger et al. 2016: 8; Lupton 2015: 6). Apps im Allgemeinen und Wearables im Speziellen bieten eine spürbare Erleichterung bei der Messung von Aktivitäten, die sonst nur mit relativ großem Aufwand erfasst werden konnten. Hänsel et al. (2016) weisen in diesem Zusammenhang auf den Einfluss von Gamification, der Anwendung von spieltypischen Elementen in anderen Kontexten, hin. Durch die Einbindung von spielerischen Elementen werden sowohl intrinsisch motivierende Treiber wie Freude, als auch extrinsische Motivationsanreize wie Belohnungen oder Auszeichnungen von Individuen angesprochen, die zu einer Nutzung von Wearables und (freiwilligen) Preisgabe von Daten führen (Hänsel et al. 2016: 2; Robson et al. 2015). In diesem Zusammenhang sehen Nutzer die preisgegebenen Daten als eine Art Bezahlung für die, ansonsten häufig kostenlosen, Apps und Services an.

Darüber hinaus wird der Vergleich mit anderen als nötiger und objektiver Maßstab angesehen, um die eigene Leistung beurteilen zu können. Damit müssen zwangsläufig (eigene) Daten preisgegeben werden, um einen Vergleich mit sich selbst, mit anderen Nutzern oder normierten Indizes zu ermöglichen (Leger et al. 2016; Gilmore 2015; Püschel 2014).

Während Wearables in datenschutzrechtlicher Hinsicht eine Reihe von Fragen aufwerfen, scheinen viele Nutzer Strategien entwickelt zu haben, diese Probleme zu relativieren und die Praktiken des Datenteilens und -auswertens für sich zu legitimieren.

b) Haftung

Wearables werfen auch haftungsrechtliche Fragen unterschiedlicher Natur auf. Dies betrifft vor allem den Bereich der zivilrechtlichen Produkt- und Produzentenhaftung. So sorgte etwa das Fitnessarmband eines amerikanischen Herstellers 2014 für Aufsehen, weil es bei zahlreichen Nutzern allergische Reaktionen hervorrief und zurückgerufen werden musste (Kim 2016). Daneben sind andere Haftungsszenarien denkbar: Wo Wearable-Daten genutzt werden, um Versicherungstarife zu berechnen oder Vitalfunktionen zu überwachen, ist die Richtigkeit der erhobenen Daten essentiell. Fehlerhafte Informationen können in solchen Fällen vertragliche und deliktische Haftungsansprüche auslösen. Datenverlust, Datenmissbrauch oder die Zugänglichmachung persönlicher Daten gegenüber Dritten sind weitere Problemfelder, die es zu bedenken gilt. Unabhängig von zivilrechtlichen Ansprüchen können strafrechtliche Haftungsrisiken bestehen, etwa im Fall der Fehlfunktion des Geräts oder einer Fehlinterpretation seiner Daten (Kim 2016).

c) IT-Sicherheit

Nach einer Untersuchung des Cybersecurity-Unternehmens Symantec genügen viele Wearables nicht den üblichen Sicherheitsstandards. So werden die Daten zwischen den entsprechenden Endgeräten (Wearable und Smartphone) häufig unverschlüsselt übertragen. Bisweilen ist sogar die Verbindung zwischen Smartphone und Server nicht verschlüsselt (Symantec 2014). Die Hersteller sollten daher adäquate technische Maßnahmen ergreifen, um eine sichere Datenerhebung, -übertragung und -verarbeitung zu gewährleisten (Ende-zu-Ende-Verschlüsselung). Dies gilt insbesondere dann, wenn die Daten ins Ausland übertragen werden.

d) Datenqualität, -übertragbarkeit und -eigentum

Professionelle Anwender kritisieren die Qualität der durch Wearables erfassten Daten. So halten manche Vertreter der Ärzteschaft die Tracking-Daten in Patientenakten sogar für „Datenmüll“ (Becker 2016: 1). Tatsächlich werden falsche Messwerte vielfach als Problem wahrgenommen (BMJV 2016: 9) und eine Reihe von Fitnessarmbändern, Smartwatches und Co. liefern in der Praxis nur unzuverlässige Daten (Case et al. 2015: 625). Hinzu kommt, dass viele Hersteller zur Datenerfassung und -verarbeitung proprietäre Systeme nutzen, womit es den Geräten häufig an Interoperabilität mangelt. Für Nutzer, die den Anbieter oder das System wechseln wollen, stellt sich damit die Frage nach dem Verbleib der mühsam kuratierten Daten. Hier wird die neue europäische Datenschutzgrundverordnung für Abhilfe sorgen, denn mit ihr soll dem Nutzer ein „Recht auf Datenübertragbarkeit“ eingeräumt werden (Art. 20 Abs. 1 DSGVO). Über die Reichweite dieser Datenübertragbarkeit wird zwar noch zu diskutieren sein, in jedem Fall rückt damit

aber die Frage nach der ökonomischen Dimension einer Dateninhaberschaft und -disponibilität weiter in den Fokus (Jülicher et al. 2016: 358 ff; Moos 2016).

7 Fazit und Ausblick

Mehr und mehr Deutsche nutzen Wearables. Wurden sie bis dato vor allem als Fitness- und Lifestyle-Geräte wahrgenommen, wird ihr künftiges Potential vor allem im professionellen und medizinischen Kontext – etwa zur Prävention von Krankheiten – gesehen. Zwar können sich viele Menschen vorstellen, ihre Vitalwerte an einen Arzt zu übermitteln, zugleich äußern sie aber auch eine gewisse Skepsis. So ist etwa ein Drittel der Bevölkerung der Auffassung: „Meine Gesundheitsdaten gehen niemanden etwas an." (BMJV 2016: 10).

Ungeachtet dieser oft formulierten Skepsis lässt sich jedoch feststellen, dass ein Großteil der Nutzer die Möglichkeiten des Teilens bereits nutzt – und dies nicht (nur) zur Übermittlung an Ärzte, sondern auch an die Anbieter der Wearables und weitere Dritte. Dieses Paradox – so scheint es – erfordert einen öffentlichen Diskurs darüber, welche Daten als schützenswert angesehen werden und ob und wie Nutzer durch den gesetzlichen Rahmen zu schützen sind. Für Entwickler und Hersteller bedeutet dies vor allem, dass sie nicht nur die notwendigen Sicherheitsstandards gewährleisten müssen, sondern auch in einen aktiven Dialog mit Nutzern und anderen Beteiligten treten sollten.

ABIDA (Assessing Big Data) Über die Dossiers

Das Projekt ABIDA, gefördert vom Bundesministerium für Bildung und Forschung, lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung. Dabei nähert ABIDA sich dem Thema Big Data aus einer grundlegend interdisziplinären Perspektive. Mehr Informationen finden Sie auf www.abida.de.

In den ABIDA-Dossiers werden regelmäßig ausgewählte Big Data-Themen kurz und prägnant dargestellt, um dem Leser einen Überblick zu liefern und einen Einstieg in die Thematik zu ermöglichen. Weitere Dossiers sind verfügbar unter www.abida.de/content/dossiers.

Vertiefungshinweise: Literatur und Links

- **Selke, S.** (2014). Lifelogging: Wie die digitale Selbstvermessung unsere Gesellschaft verändert. Ullstein eBooks.
- **Kamenz, A.** (2015). Quantified Self: Anspruch und Realität.
- **Hänsel, K. et al.** (2016). "Wearable Computing for Health and Fitness: Exploring the Relationship between Data and Human Behavior." arXiv preprint arXiv: 1509.05238.
- **Rosales, A. et al.** (2015). Beeping Socks and Chirping Arm Bands: Wearables That Foster Free Play. Computer June, pp. 41-48.
- **Bundesamt für Sicherheit in der Informationstechnik** (2015). Hinweise zur Sicherhit von Wearables.
- **Pitzer, J. W. et al** (2013). The Next Big Thing-Wearables Are in Fashion. Credit Suisse Technology Connections Series.

Literaturnachweise

Almeida, T. (2015). Designing Intimate Wearables to Promote Preventative Health Care Practices. UbiComp/ISWC'15 Adjunct, 659-662. doi: 0.1145/2800835.2809440

Arora, S., et al. (2014). High accuracy discrimination of Parkinson's disease participants from healthy controls using smartphones. Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on, IEEE.

Becker, K. (2016, 9. Februar). Kassen wollen Daten von Fitness-Armbändern nutzen. *Süddeutsche Zeitung, S. 1.*

BMJV (2016). Wearables und Gesundheits-Apps. Online verfügbar unter https://www.bmjv.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/YouGov.pdf.

Börner, M. (2015). Marktentwicklung und Trends in der Unterhaltungselektronik. Online Verfügbar unter https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/09-September/Bitkom-Praesentation-PK-CE-01-09-2015.pdf.

Case, M., Burwick, H., Volpp, K., Patel, M. (2015). Accuracy of Smartphone Applications and Wearable Devices for Tracking Physical Activity Data. *The Journal of the American Medical Association 313 (6), 625-626.*

De Montjoye, Y.-A., et al. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific reports 3.*

Eggers, D. (2013). The Circle. New York, NY: Random House.

Gao, W., et al. (2016). Fully Integrated Wearable Sensor Arrays For Multiplexed In Situ Perspiration Analysis. *Nature 2016 (529), 509-514.*

Gilmore, J. N. (2015). Everywear: The quantified self and wearable fitness technologies. *New Media & Society: 1461444815588768.*

Goyder, C., et al. (2010). Self Diagnosis *BMJ 2010 (340), 204-206.*

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.

Jandt, S., Hohmann, C. (2015). Fitness- und Gesundheits-Apps – Neues Schutzkonzept für Gesundheitsdaten? *Kommunikation & Recht 2015 (11), 694-700.*

Jia, W., Valdés-Ramírez, G., Bandodkar, A., Windmiller, J., Wang, J. (2013). Epidermal Biofuel Cells: Energy Harvesting from Human Perspiration. Angewandte Chemie 2013 (52), 7233-7236. doi: 10.1002/anie.201302922

Jülicher, T., Röttgen, C., v. Schönfeld, M. (2016). Das Recht auf Datenübertragbarkeit – Ein datenschutzrechtliches Novum. *ZD 2016, 358-362.*

Kamenz, A. (2015). Quantified Self Anspruch und Realität.

Kim, Y. (2016). New Legal Problems Created by Wearable Devices. Illinois Business Law Journal. Online verfügbar unter https://publish.illinois.edu/illinoisblj/2016/02/29/new-legal-problems-created-by-wearable-devices/#_ftn25.

King, L. (2014). Google Smart Contact Lens Focuses On Healthcare Billions. Forbes Tech July 15. Online verfügbar unter http://www.forbes.com/sites/leoking/2014/07/15/google-smart-contact-lens-focuses-on-healthcare-billions/.

Kopp, R., Sokoll, K. (2015). Wearables am Arbeitsplatz – Einfallstore für Alltagsüberwachung? *Neue Zeitschrift für Arbeitsrecht 2015 (22), 1352-1359.*

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

Lupton, D. (2012). Medicine as culture: Illness, disease and the body. Sage.

Lupton, D. (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, health & sexuality 17(4): 440-453.*

Moos, F. (2016). The troubling reach of the GDPR right to data portability. *E-Commerce Law & Policy 18 (2).*

O'Kane, M. J., 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 Medicine.

Püschel, F. (2014, 30.10.2015) Big Data und die Rückkehr des Positivismus. Zum gesellschaftlichen Umgang mit Daten. Online verfügbar unter http://www.medialekontrolle.de/wp-content/uploads/2014/09/Pueschel-Florian-2014-03-01.pdf.

Robson, K., et al. (2015). Is it all a game? Understanding the principles of gamification. *Business Horizons 58(4): 411-420.*

Scheer, R. & Sneed, A. (2014). Safety in a Sock. Scientific American, October 2014, 20.

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

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

Zoche et al.(2015). Das Versteckte Internet. Zu Hause-Im Auto-Am Körper. White Paper Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt 2015. Online verfügbar unter https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/White –Paper-2-Final_17.07.15-Druckversion.pdf