MARKTWÄCHTER
DIGITALE WELT

verbraucherzentrale

WEARABLES, FITNESS-APPS UND DER DATENSCHUTZ:

Alles unter Kontrolle?

Eine Untersuchung der Verbraucherzentralen – April 2017

WEARABLES, FITNESS-APPS UND DER DATENSCHUTZ

ABBILDUNGEN UND TABELLEN

1. PROBLEMSTELLUNG

Die Digitalisierung des Alltags, innerhalb dessen Menschen „Knotenpunkte im Internet der Dinge werden“[1], schreitet stetig voran. Selbstvermessungstechnologien wie Wearables und Fitness-Apps können hilfreiche Alltagsbegleiter sein, die ein Mehr an Autonomie und Kontrolle über Körper und Gesundheit bedeuten können. Damit Verbraucher[2] langfristig von dieser Entwicklung profitieren und nicht zu Verlierern innerhalb einer mittels Algorithmen gesteuerten Welt werden, müssen Nutzungsrisiken aufgedeckt und begrenzt werden. Denn: Die im Zuge der Wearable-Nutzung entstehenden Daten wecken Begehrlichkeiten externer Akteure – wie Werbeindustrie oder auch Krankenkassen.

Im Folgenden werden zentrale datenschutzrelevante Aspekte bei der Nutzung von Wearables und Fitness-Apps beleuchtet. Neben einem kurzen Marktüberblick (Abschnitt 1.1) wird insbesondere die potenzielle gesellschaftliche Bedeutung von derlei Technologien diskutiert (Abschnitt 1.2). Basierend auf Überlegungen zum Recht auf informationelle Selbstbestimmung werden die Forschungsfragen der Untersuchung abgeleitet (Abschnitt 1.3) und die Methoden erläutert, die zu ihrer Beantwortung ausgewählt wurden (Abschnitt 1.4). Hierbei handelt es sich um eine technische Prüfung von zwölf Wearables (Kapitel 2), eine rechtliche Einordnung dazu, wie Anbieter mit geltenden Datenschutzbestimmungen umgehen (Kapitel 3) sowie eine Verbraucherbefragung (Kapitel 4).

1.1 WEARABLES IM ÜBERBLICK

Wearable Computing Devices (Wearables) sind am Körper tragbare, elektronische Kleingeräte, die einerseits über einen oder mehrere Sensoren zur Messung körperlicher Aktivitäten und Vorgänge verfügen und andererseits über eine digitale Schnittstelle (zumeist Bluetooth, teilweise auch Near Field Communication (NFC) oder WLAN).[3] Diese ermöglicht eine Übertragung der von den Sensoren gemessenen Daten an ein Smartphone oder Tablet. Auf diesem ist in der Regel eine entsprechende Anwendung (Applikation, App) installiert, die die vom Wearable erhobenen Rohdaten aggregiert und aufbereitet. Verbraucher werden somit in die Lage versetzt, die eigenen Körperaktivitäten überwachen zu können (sog. Self-Tracking). Hierbei werden nicht nur dem Verbraucher diese Daten angezeigt – auch die jeweiligen Wearable-Anbieter können die generierten Inhalte erheben, speichern und nutzen.[4]

Der Begriff Wearables ist als Sammelkategorie für eine Reihe verschiedener Ausführungsformen zu verstehen, die sich beispielsweise darin unterscheiden, wo genau das jeweilige Gerät am Körper getragen wird. Kommerziell am weitesten verbreitet sind Wearables, die am Handgelenk getragen werden (sog. Wristwear, in der Regel als Smartwatches oder Fitness-Armbänder).[5] Darüber hinaus werden derzeit Datenbrillen und „smarte“ Kontaktlinsen entwickelt oder bereits angeboten (sog. Eyewear), ebenso wie Kopfhörer mit digitaler Schnittstelle (sog. Earwear) oder „smarte“ Alltagskleidung in Form von T-Shirts, Schuhen oder auch Babykleidung, die es Eltern ermöglicht, Atmung und Schlaf ihres Säuglings via Smartphone ständig zu überwachen.[6] Insofern sind Wearables ein Beispiel für die fortschreitende Vernetzung von Alltagsgegenständen – ein generelles Phänomen, das oft als „Internet der Dinge“ bezeichnet wird.[7]

Weiterhin unterscheiden sich Wearables in ihrer konkreten Ausstattung, das heißt, welche Sensoren verbaut sind und entsprechend welche Daten erzeugt werden. In der Mindestausstattung verfügen die meisten Wearables über einen Beschleunigungssensor, der auch minimale Bewegungen registriert. Auf Basis der vom Sensor gemessenen Rohdaten wird beispielsweise die Anzahl der gegangenen Schritte ermittelt und

1 Lupton, 2014, S. 15 (eigene Übersetzung).
2 Aus Gründen der besseren Lesbarkeit wird in der vorliegenden Arbeit mit „Verbraucher“ eine verkürzte geschlechtsneutrale Formulierung verwendet. Der Text richtet sich daher sowohl an Verbraucherinnen als auch an Verbraucher. Diese Formulierungsregel gilt für die gesamte vorliegende Arbeit (z. B. auch in Bezug auf die Verwendung des Begriffs „Internet-Nutzer“).
3 Delisle, 2016, S. 1; Goldhammer, 2016, S. 4.
4 Unter „Wearable-Anbietern“ wird im Rahmen der vorliegenden Untersuchung das Unternehmen verstanden, dass das Wearable unter seiner Marke vertreibt. Dieses kann sowohl die Produktion der Hardware als auch die Programmierung einer kompatiblen Fitness-App an externe Dienstleister ausgelagert haben.
5 Ballhaus, Song, Meyer, Ohrtmann, & Dressel, 2015, S. 9; Steinbrunn & Dominsky, 2016, S. 23.
6 Selke, 2015, S. 46; s. auch http://www.baby-wearables.de/baby-wearable-als-strampler-mimo-ueberwacht-schlaf-und-atmung/.
7 Delisle, 2016, S. 2.

Kalorienverbrauch oder Schlafdauer und -qualität algorithmenbasiert berechnet.[8] Höherklassige und neuere Wearables verfügen meistens über zusätzliche Sensoren, zum Beispiel zur Messung von Puls, Herzfrequenz, Körpertemperatur, Hautleitfähigkeit sowie zur Bestimmung des Aufenthaltsorts (meist via GPS).[9]

Sowohl die in Wearables verbauten Sensoren als auch ihre digitalen Schnittstellen werden vermutlich immer energie-und platzeffizienter werden, sodass sich die Technologie zukünftig noch unauffälliger in den Alltag integrieren lassen wird.[10] So werden derzeit Bio-Tattoos (sog. Tech Tats) entwickelt: Diese haben ähnliche Funktionen wie Wearables am Handgelenk, die Sensoren werden jedoch mittels Tinte in die Haut implantiert.[11] Zusätzlich scheinen Wearables über die bloße Messung von Körperdaten hinaus zukünftig mit ihren Nutzern außerhalb der Bedienungsoberfläche interagieren zu können. Beispielsweise können Sensoren, die über ein elektronisches Pflaster auf dem Rücken befestigt werden, die Nutzer über ein Vibrieren daran erinnern, ihre Sitzhaltung zu korrigieren.[12]

Die stetig präziser und invasiver werdende Sensortechnik ermöglicht immer weitreichendere Rückschlüsse auf traditionell intime Lebensbereiche. Mittelbar können die gesammelten Daten, zum Beispiel Daten über das Schlafverhalten einer Person, nicht nur Rückschlüsse auf die körperliche Gesundheit zulassen, sondern – beispielsweise über die Messung von Hauttemperatur und Schweißdrüsenaktivität – auch auf psychische Zustände (z. B. Stress).[13] Dies ist vor allem der Fall, wenn eine Kombination verschiedener solcher Daten über einen längeren Zeitraum getrackt und von einer App ausgewertet wird. Da dies in der Regel Sinn und Zweck des Self-Trackings ist, sind die von Wearables gemessenen Daten als Gesundheitsdaten zu werten,[14] die im Sinne des Bundesdatenschutzgesetzes (BDSG) besondere personenbezogene Daten sind (s. Abschnitt 3.1).[15]

8 Schumacher, 2016, S.42.
9 Global Positioning System.
10 Z. B. Wiggers, 2016.
11 Goldhammer, 2016, S. 4.
12 Z. B. www.uprightpose.com.
13 Umann, Tuscher, Buchmann, & Bosch, 2016, S. 132-133.
14 Artikel 29 Datenschutzgruppe, 2015.
15 § 3 Abs. 9 und §§ 4, 4a Abs. 3 BDSG; s. Kapitel 3.

Während 14 Prozent der deutschen Internetnutzer angeben, derzeit ein Wearable zu nutzen,[16] scheint das Marktpotenzial für derlei Technologien weitaus größer zu sein. So gaben in einer bevölkerungsrepräsentativen Telefonumfrage des Digitalverbandes *Bitkom* (2015) vierzig Prozent der Befragten an, sich zumindest für die Nutzung einer Smartwatch zu interessieren, auch wenn sie zum Zeitpunkt der Befragung noch keine aktiven Nutzer waren.[17] Die wachsende Beliebtheit von Wearables spiegelt sich außerdem in weltweit steigenden Absätzen wider: Bis zum Jahr 2018 wird ein Marktwachstum von jährlich 21 Prozent prognostiziert.[18]

Darüber hinaus gibt es eine unüberschaubare Menge an Fitness-Apps, die – wenn auch eingeschränkt – ohne die zusätzliche Wearable-Hardware Körperdaten über die Sensoren des Smartphones messen und berechnen. Wearables und Fitness-Apps sind insbesondere bei jüngeren Verbrauchern verbreitet, die diese zur Überwachung körperlicher Aktivitäten und zur Optimierung von Fitness und Gesundheit nutzen.[19]

1.2 SELBSTVERMESSUNG: VERBRAUCHER ZWISCHEN EIGEN- UND FREMDMOTIVATION

Wearables und Fitness-Apps werden in der Regel zu Zwecken der Selbstvermessung, Selbstüberwachung und Selbstoptimierung genutzt.[20] Der Begriff „Selbstvermessung“ umschreibt Praktiken, die der Quantifizierung der eigenen körperlichen und geistigen Zustände dienen. Meist beinhaltet dies das Messen und Aufzeichnen verschiedener Aktivitäten sowie den Wunsch, sich selbst in bestimmter Hinsicht verbessern zu wollen.[21] Selbstvermessung betrifft also zunächst die selbstgesteuerte (intrinsische) Motivation, ein auf die ein oder andere Art und Weise „besseres“ und gesünderes Leben zu führen.[22]

16 YouGov, 2016.
17 Lutter, Pentsi, Poguntke, Böhm, & Esser, 2015, S. 32.
18 Ballhaus et al., 2016, S. 5.
19 Z. B. YouGov, 2016, S. 5.
20 Abril, 2016.
21 Ehlert et al., 2015, S. 30-31; ausgeschlossen hiervon sind Selbstvermessungspraktiken, die eine lebenswichtige Notwendigkeit darstellen; eine Diskussion soziologischer Aspekte von Selbstvermessung und -optimierung kann z. B. nachgelesen werden bei En & Pöll, 2016; Selke, 2016.
22 Lupton, 2014, S. 6; Meißner, 2016, S. 219.

Während die Praktik des Selbstvermessens an sich unabhängig von der dafür angewandten Methode ist, erleichtert die Digitalisierung die Integration der Selbstvermessung in den Alltag – denn Wearables und Fitness-Apps können die relevanten Daten automatisiert und weitestgehend unbemerkt in Echtzeit aufzeichnen.[23] Insofern werden derlei Technologien auch als eine Erweiterung der Autonomie und Kontrolle über den eigenen Körper und die eigene Gesundheit verstanden.

Die Grundidee, dass Menschen sich selbstverantwortlich um ihre Gesundheit kümmern sollen, ist außerdem in einem volkswirtschaftlichen Kontext zu sehen – denn gesunde Menschen verursachen dem Gesundheitssystem weniger Kosten als Kranke. Der Slogan „Sitzen ist das neue Rauchen“[24] fasst die in diesem Zusammenhang zentrale Annahme zusammen, die die Nutzung von Wearables außerhalb eines individuellen Wunsches nach Fitness interessant macht: Ein aktiver Mensch, der sich ausreichend viel bewegt, soll eine geringere Wahrscheinlichkeit haben, zukünftig krank zu werden.[25]

Obwohl nicht abschließend geklärt ist, inwieweit Wearables und Fitness-Apps Menschen tatsächlich zu einem gesünderen Lebensstil motivieren,[26] werden sie als Instrumente vermarktet, die Menschen zu mehr Bewegung und einem insgesamt gesünderen Lebensstil über äußere Anreize (extrinsisch) motivieren sollen. Daran haben beispielsweise Arbeitgeber Interesse, die über eine geringere Anzahl von Krankheitsfällen in ihrem Unternehmen Kosten einsparen und ihre Produktivität erhöhen wollen. So setzen bereits verschiedene Unternehmen in den USA (u. a. *BP*) Wearables und Fitness-Apps ein, um die Aktivität ihrer Mitarbeiter zu überwachen und sie bei ausreichender Bewegung zu belohnen, beispielsweise mit „Wellness-Punkten“.[27] Innerhalb des Versicherungssystems der USA können derlei Punkte einen Einfluss auf die Höhe des Versicherungsbeitrags haben. Führende Wearable-Anbieter wie *Fitbit* oder *Jawbone* bewerben auf ihrer Webseite entsprechende auf Arbeitgeber zugeschnittene Angebote.[28] Die App *Soma Analytics* übermittelt sogar den Gemütszustand von Mitarbeitern an deren Arbeitgeber, beispielsweise über die Auswertung ihrer Stimme und Smartphone-Nutzungsmuster.[29]

Obwohl die breite Masse der Wearables und Fitness-Apps im Bereich dieses zweiten Gesundheitsmarktes anzusiedeln ist, werden sie in Dienstleistungen des ersten Gesundheitsmarktes – der die klassische medizinische Versorgung durch private und gesetzliche Krankenversicherungen umfasst – mittlerweile mit eingebunden.[30] So sehen Versicherungsdienstleister in der Selbstvermessungstechnologie eine Möglichkeit, nicht nur Krankheitsintervention zu verbessern, sondern Wearables zur Gesundheitsvorsorge im Rahmen von Bonusprogrammen einzusetzen, wodurch eine langfristige Kosteneinsparung angestrebt wird.[31] Vorreiter hierbei ist der private Versicherungsdienstleister *Generali*, der mit *Vitality* seit Juli 2016 eine eigene Fitness-App anbietet.[32] Die Nutzung der App stellt den Versicherten je nach Bewegungsleistung Rabatte auf Versicherungsprodukte oder Sachprämien in Aussicht.

Auch gesetzliche Krankenkassen, die sich von privaten Dienstleistern durch ihre Organisation nach dem Solidarprinzip[33] unterscheiden, zeigen Interesse an dem beschriebenen Geschäftsmodell. Allerdings verbieten ihnen gesetzliche Regelungen grundsätzlich, personenbezogene Daten ihrer Mitglieder zu erheben, die über das für die Vertragserfüllung erforderliche Maß hinausgehen. Eine Anpassung des Versicherungstarifs auf Basis der von Wearables und Fitness-Apps erhobenen Daten ist ihnen somit untersagt.[34] Dennoch können Bestrebungen seitens gesetzlicher Versicherungen

23 Selke, 2016, S. 3.
24 z. B. Raether, 2013.
25 Sjögren et al., 2014.
26 Dies betrifft mHealth-Anwendung übergreifend; Tomlinson, Rotheram-Borus, Swartz, & Tsai, 2013.
27 Christl, 2014, S. 40.
28 https://www.fitbit.com/de/group-health# [Stand: 31.01.2017].
29 http://soma-analytics.de/; Klofta & Rest, 2015.
30 Der erste Gesundheitsmarkt umfasst in erster Linie Leistungen von staatlichen und öffentlichen Einrichtungen, wie beispielsweise die Leistungen und Angebote gesetzlicher Krankenversicherungen. Die Angebote des zweiten Gesundheitsmarktes beziehen sich hingegen auf individuelle Gesundheitsleistungen, wie beispielsweise Wellness-Reisen oder Fitness-Kurse. Die Definition des zweiten Gesundheitsmarktes ist schwierig, weil dieser sehr heterogen ist und teilweise Verbindungen zum ersten Gesundheitsmarkt bestehen (z. B. Fitness-Kurse, die von gesetzlichen Krankenversicherungen finanziell bezuschusst werden). Damm, Kuhlmann, & von der Schulenburg, 2010, S. 2.
31 Gigerenzer, Schlegel-Matthies, & Wagner, 2016, S. 1; Lupton, 2015, S. 3; zur Bewertung von Bonusprogrammen, s. auch Verbraucherzentrale NRW, 2015.
32 https://www.generali-vitalityerleben.de/ [Stand: 30.01.2017].
33 Burkhardt, 2013.
34 Z. B. BMJV, 2016.

in diesem Kontext beobachtet werden. So bietet die *AOK Nordost* seit Januar 2016 die kostenlose Fitness-App *FitMit AOK* an, die laut Versicherung als „digitales Bonusheft" zu verstehen ist: Gegen Vorlage guter Aktivitätsdaten können die Versicherungskunden auf unterschiedliche Bargeld- oder Sachprämien zurückgreifen.[35] Auch der Chef der *Techniker Krankenkasse (TK)*, Jens Baas, hat angekündigt, dass Fitness-Armbänder und andere Wearables zukünftig eine Rolle in dem Bonusprogramm der *TK* spielen könnten.[36]

Aus Sicht des Verbraucherschutzes werfen derlei Anreize die Frage auf, inwieweit die Entscheidung, ein Wearable zu nutzen, langfristig freiwillig bleibt, denn Rabatte und Prämien könnten wirtschaftlichen Druck auf Verbraucher ausüben. Handlungsfreiheit wäre dann nur noch für solche Verbraucher eine realistische Option, die es sich finanziell leisten könnten auf die in Aussicht gestellten Vergünstigungen zu verzichten, wohingegen zum Beispiel gesundheitlich beeinträchtigte Menschen nicht von Bonusprogrammen profitieren könnten – eine indirekte Form gruppenspezifischer Diskriminierung.[37] In Bezug auf Tarife gesetzlicher Krankenkassen wurde daher bereits verschiedentlich vor einer Aufweichung des Solidarprinzips gewarnt, da Menschen mit gesundheitlichen Problemen innerhalb eines ausgeweiteten Bonus-Systems benachteiligt werden könnten.[38] Dies gilt in ähnlicher Weise auch für den systematischen Einsatz von Wearables in Betrieben. Das Arbeitgeber-Arbeitnehmer-Verhältnis ist darüber hinaus durch ein Machtgefälle gekennzeichnet, das Arbeitnehmern eine tatsächlich freie Entscheidung für oder gegen die Nutzung eines Wearables am Arbeitsplatz langfristig erschweren könnte.

1.3 RECHT AUF INFORMATIONELLE SELBSTBESTIMMUNG

Das Interesse externer Akteure an den von Wearables und Fitness-Apps generierten Daten ist groß (s. Abschnitt 1.2). Entsprechend ist aus Sicht des Verbraucherschutzes entscheidend, dass der einzelne Nutzer das Grundrecht auf informationelle Selbstbestimmung auch im Kontext der Wearable- und Fitness-App-Nutzung für sich beanspruchen kann. Dieses wird vom Bundesverfassungsgericht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG hergeleitet.[39] Es sieht vor, dass jeder selbst darüber bestimmen soll, welche Daten er von sich preisgibt, wie diese weiterverarbeitet werden und wer Zugriff darauf hat – ein Wunsch, den Verbraucher auch in Bezug auf ihre Gesundheits- und Fitnessdaten äußern.[40]

Die Realisierung dieser Selbstbestimmung ist in der Praxis jedoch von verschiedenen Voraussetzungen abhängig, die in der vorliegenden Studie mit dem Fokus auf Wearables und Fitness-Apps untersucht werden. Hierbei steht zunächst die Pflicht des Wearable-Anbieters im Vordergrund, verantwortungsvoll mit den Nutzerdaten umzugehen und die datenschutzrechtlichen Vorgaben einzuhalten (Abschnitt 1.3.1). Gleichermaßen spielt gerade im Kontext von Wearables und Fitness-Apps auch eine Rolle, wie Verbraucher zu datenschutzrelevanten Aspekten stehen (Abschnitt 1.3.2).

1.3.1 Anbieterpflichten

Ein Großteil der über Wearables und Fitness-Apps generierten Daten ist personenbezogen. Laut § 3 Abs. 1 BDSG handelt es sich bei personenbezogenen Daten um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Weiter führt die Europäische Datenschutzrichtlinie in Art. 2 Buchst. a Richtlinie 95/46/EG aus, dass eine Person als bestimmbar angesehen wird, die direkt oder indirekt identifiziert werden kann. Dies kann insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen geschehen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Derlei Daten dürfen vom Anbieter[41] nur erhoben, gespeichert und genutzt werden, wenn eine gesetzliche Gestattung hierzu oder eine Einwilligung des Betroffenen vorliegt.[42]

35 https://www.fitmit-aok.de/ [Stand: 30.01.2017].
36 https://www.tk.de/tk/020-positionen/aktuelles/dpa-interview-fitness-tracker/889466 [Stand: 30.01.2017].
37 Z. B. Verbraucherzentrale NRW, 2015; Bundestags-Drucksache 18/9058, 2016, S. 1; Bundestags-Drucksache 18/9243, S. 1-4.
38 Jahberg et al., 2015; Verbraucherzentrale NRW, 2015.
39 sog. Volkszählungsurteil, BVerfG, Urteil vom 15. September 1983, 1 BvR 209/83.
40 YouGov, 2016, S. 10.
41 Auch in Fällen, in denen der Anbieter (s. auch Fußnote 2) nicht die datenverarbeitende Stelle ist, sondern hierfür einen Dienstleister beauftragt hat, ist er für den Umgang mit den personenbezogenen Daten verantwortlich, die in Zusammenhang mit der Nutzung seines Dienstes über seine Kunden erhoben, gespeichert und genutzt werden; § 11 Abs. 1 BDSG.
42 § 4 Abs. 1 BDSG, §12 Abs.1 TMG

Unabhängig von der gesetzlichen Gestattung gilt der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a BDSG, der für den gesamten Erhebungs- und Verarbeitungsprozess zu beachten ist: Das BDSG sieht vor, dass für die Vertragserfüllung durch technische Ausgestaltung von vornherein so wenige personenbezogene Daten wie möglich erfasst werden. Anbieter müssen mit anderen Worten eine sparsame Lösung zur Realisierung ihrer angebotenen Dienstleistungen implementieren und dürfen nicht mehr Daten erheben, als für die Erbringung ihrer Dienstleistung erforderlich ist.

Ein weiterer zu beachtender Grundsatz ist die Datensicherheit, die sich gemäß § 9 BDSG in Form von technischen und organisatorischen Maßnahmen niederschlägt. Ziel ist die Wahrung der *Verfügbarkeit*, *Unversehrtheit* und *Vertraulichkeit* von Informationen mittels Sicherheitsvorkehrungen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. Die für die Datenverarbeitung Verantwortlichen sind daher dazu verpflichtet, diese Daten vor dem Zugriff durch unbefugte Dritte zu schützen – eine Verpflichtung, der in der Vergangenheit nicht immer hinreichend nachgekommen wurde.[43] So können Unbefugte beispielsweise relativ mühelos Zugriff auf sensible Nutzerdaten erhalten, wenn die Datenübertragung zwischen Fitness-App und Anbieterserver nicht nach dem Stand der Technik gesichert ist. Bei unzureichender Sicherung der Geräteverbindung kann das Tragen eines Wearables außerdem dazu führen, dass Nutzer eindeutig über das Gerät identifizierbar sind. Dies wird beispielsweise in Szenarien relevant, in denen Einkaufszentren die Laufwege und das Kaufverhalten von Verbrauchern nachvollziehen wollen und sich dafür einer Bluetooth-Verbindung mit den Wearables ihrer Kunden bedienen – ohne deren Einverständnis.[44]

Insofern stellt sich die Frage, ob Wearables und Fitness-Apps auf technischer Ebene gängigen Datenschutzstandards genügen.[45] Zu untersuchen ist entsprechend zunächst, welche Daten vom jeweiligen Anbieter überhaupt erhoben, gespeichert und genutzt werden (**Forschungsfrage 1** zu Nutzerdaten, Tabelle 1) und inwieweit die erhobenen Daten vor dem Zugriff durch unbefugte Dritte geschützt sind (**Forschungsfrage 2** zu Datensicherheit).

Werden über die für die Dienstleistung erforderlichen Daten hinaus personenbezogene Daten erhoben, müssen diese nicht nur hinreichend gesichert sein. Es muss vor allem eine informierte Einwilligung des Nutzers eingeholt werden.[46] Für die Verwendung von *Gesundheitsdaten*, die von Wearables und Fitness-Apps gemessen werden können, ebenso wie für die Übertragung von Daten ins Nicht-EU-Ausland muss oftmals eine Einwilligung eingeholt werden (s. Abschnitt 3.1.1). Entsprechend stellt sich die Frage, inwieweit Wearable-Anbieter eine rechtskonforme Einwilligung einholen, insbesondere für die Verarbeitung von Gesundheitsdaten und die Übertragung von Daten ins Nicht-EU-Ausland (**Forschungsfrage 4** zu Einwilligung).

Durch die informierte Einwilligung sollen Nutzer eine freie Entscheidung für oder gegen die Preis- und Weitergabe ihrer Daten an Dritte treffen können. Ist die Entscheidung des Nutzers zur Einwilligung nicht frei, ist auch die erteilte Einwilligung unwirksam. Die Einwilligung ist in der Regel jedoch eine notwendige Bedingung dafür, dass ein Dienst überhaupt genutzt werden kann. Insofern ist die Entscheidung des Nutzers nur frei bezüglich der Frage, ob er den Dienst eines Wearables und der dazugehörigen App *nutzen* will. Ob er hingegen im Zuge der Nutzung bestimmte Daten preisgeben möchte oder nicht – insbesondere zu Zwecken, die sein eigentliches Ziel der Selbstquantifizierung übersteigen – kann er oft nicht entscheiden. Solange Nutzer also innerhalb der Dienstleistung keinen Einfluss darauf nehmen können, welche Daten erhoben, gespeichert und genutzt werden, steht die Freiwilligkeit der Einwilligung in Frage. Dies gilt insbesondere für solche personenbezogene Daten, die für die Inanspruchnahme der Dienstleistung nicht zwingend erforderlich sind. Aus Perspektive des Verbraucherschutzes ist daher zu klären, inwieweit Wearable-Anbieter ihren Nutzern Möglichkeiten zur Einflussnahme und Kontrolle ihrer Daten einräumen (**Forschungsfrage 3** zu Einflussnahme und Kontrolle).

43 Z. B. Ackerman, 2013; Clausing, Schiefer, Lösche, & Morgenstern, 2015; Hilts, Parsons, & Knockel, 2016; Stiftung Warentest, 2016a.

44 Hilts, Parsons, & Knockel, 2016, S. 26.

45 Im Rahmen dieser Untersuchung wird sich auf das geltende Recht zum Veröffentlichungszeitpunkt bezogen. Die benannten datenschutzrechtlichen Standards werden jedoch auch in der neuen europäischen Datenschutzgrundverordnung implementiert sein, die im Mai 2018 in Kraft tritt. Hierzu zählen beispielsweise Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht, vgl. auch Art. 5 DS-GVO.

46 § 4a BDSG; s. auch Hartge, 2012, S. 281.

1 FORSCHUNGSFRAGEN UND METHODEN

	Forschungsfragen	Methode
Kapitel 2	1 **Nutzerdaten** Welche Daten werden im Zuge der Wearable-Nutzung erhoben, gespeichert und genutzt?	 Technische Analyse
	2 **Datensicherheit** Inwieweit sind die im Rahmen der Wearable-Nutzung generierten Daten vor dem Zugriff durch Unbefugte geschützt?	
	3 **Einflussnahme und Kontrolle** Inwieweit räumen Wearable-Anbieter ihren Nutzern Möglichkeiten zur Einflussnahme und Kontrolle ihrer Daten ein?	
Kapitel 3	4 **Einwilligung** Wird eine wirksame Einwilligung für die Erhebung, Speicherung und Übertragung personenbezogener Daten eingeholt?	§ Rechtliche Analyse
	5 **Information** Wird der Nutzer hinreichend über den Umgang mit seinen personenbezogenen Daten unterrichtet?	
	6 **Textschwierigkeit** Ist die Datenschutzerklärung für Laien verständlich?	 Lexikalische Analyse
Kapitel 4	7 **Folgenbewertung** Wie bewerten Verbraucher mögliche Konsequenzen der Nutzung von Wearables und Fitness-Apps?	 Verbraucherbefragung
	8 **Datenschutzbedenken von Nutzern und Nicht-Nutzern** Unterscheiden sich Nutzer von Wearables und Fitness-Apps von Nicht-Nutzern in ihren generellen Datenschutzbedenken?	

Damit der Nutzer über den Umgang mit seinen Daten informiert ist, muss er darüber hinreichend unterrichtet werden. Da Informationen hierzu zunächst nur dem Anbieter vorliegen, ist dieser dazu verpflichtet, transparent darzustellen, welche Daten erhoben und in welcher Form sie weiterverarbeitet werden. Dies betrifft im Kontext von Wearables und Fitness-Apps – ähnlich wie bei der einzuholenden Einwilligung – insbesondere die Unterrichtung über die Erhebung, Speicherung und Nutzung von Gesundheitsdaten und die Verarbeitung dieser Daten im Nicht-EU-Ausland. Entsprechend stellt sich die Frage, inwieweit Anbieter ihre Nutzer hinreichend über den Umgang mit ihren Daten unterrichten (**Forschungsfrage 5** zu Information).

Um über den Umgang mit ihren Daten tatsächlich unterrichtet sein zu können, müssen Nutzer die vom Anbieter zur Verfügung gestellten Informationen lesen und auf Basis dessen verstehen können. Dementgegen stellen Angaben zum Datenschutz oft große Herausforderun-

gen an den Leser, da sie aufgrund der Vielschichtigkeit des zu beschreibenden Sachverhalts sehr umfangreich sein können und häufig komplexe Formulierungen verwenden.[47] Dies wirft die Problematik auf, dass – selbst wenn Anbieter rechtskonform und vollständig über den Umgang mit Nutzerdaten unterrichten – nicht sichergestellt ist, dass Nutzer über den Umgang mit ihren Daten tatsächlich informiert sind. Datenschutzerklärungen sollten daher trotz – beziehungsweise gerade wegen – der Komplexität des zu erklärenden Sachverhalts so einfach wie möglich geschrieben sein.[48] Insofern stellt sich die Frage, inwieweit die Datenschutzerklärungen der Anbieter für Laien einfach geschrieben sind und es somit Nutzern ermöglichen, sich anhand der zur Verfügung gestellten Angaben tatsächlich zu informieren (**Forschungsfrage 6** zu Textschwierigkeit).

1.3.2 Verbraucherperspektive

Entgegen dem weit verbreiteten Anspruch, dass Nutzer eigenverantwortlich mit ihren Daten umgehen und ihre Privatsphäre auch im Online-Bereich selbst regulieren können, ist diese Form des Selbstdatenschutzes sehr voraussetzungsreich.

Verbraucher scheinen Nachteile und potenzielle Risiken der Datenpreisgabe gegen die erhofften Vorteile zumindest implizit abzuwägen und auf Basis dessen eine Nutzungsentscheidung zu treffen.[49] Auch im Kontext von Wearables und Fitness-Apps müssen Verbraucher die kurz- oder langfristigen Folgen ihrer Entscheidung, derlei Technologie zu nutzen, *subjektiv* einschätzen, da ihnen eine objektive Informationsbasis naturgemäß fehlt.[50] Für die Einschätzung ist zum einen relevant, für wie *wahrscheinlich* das Eintreten einer (negativen) Konsequenz gehalten wird. Zum anderen spielt eine Rolle, inwieweit eine mögliche Folge inhaltlich akzeptiert wird.[51] So ist es beispielsweise denkbar, dass ein Wearable-Nutzer es für *wahrscheinlich* hält, dass sein Arbeitgeber künftig Prämien für besonders gesundheitsbewusste Mitarbeiter auszahlt. Er muss dies aber nicht notwendigerweise problematisch finden, zumal er selbst möglicherweise gar keinen direkt erfahrbaren Schaden davon trägt oder sogar vom eintretenden Ereignis profitieren kann. Zu klären ist entsprechend, wie Verbraucher mögliche (potenziell negative) Konsequenzen der Nutzung von Wearables und Fitness-Apps bewerten (**Forschungsfrage 7** zu Folgenbewertung).

Während systematische Erkenntnisse zur Risikobewertung bei der Nutzung von Wearables und Fitness-Apps noch rar sind, zeigen verschiedene Untersuchungen, dass Verbraucher den Umgang mit ihren Daten in diesem Zusammenhang durchaus als Problem betrachten. So erklärten in einer bevölkerungsrepräsentativen YouGov-Umfrage (2016) zum Thema Wearables und Gesundheits-Apps 41 Prozent der Befragten, dass die Nutzung der eigenen Daten durch Dritte für sie ein Problem darstelle. Neunundvierzig Prozent geben an, selbst bestimmen zu wollen, was mit ihren Gesundheitsdaten geschieht.[52] Unklar ist jedoch bislang, inwieweit Datenschutzbedenken einen Einfluss darauf haben, ob Verbraucher derlei Selbstvermessungstechnologien nutzen oder nicht. Übergreifend wird in diesem Zusammenhang das als paradox bezeichnete Verhaltensmuster beschrieben, dass Nutzer digitaler Technologien sich zwar um den Schutz ihrer Daten und ihre Privatheit sorgen, diese Sorgen sich jedoch nicht in ihrem tatsächlichen selbstoffenbarenden Verhalten widerspiegeln (sog. Privacy Paradox).[53] In Bezug auf Fitness- und Gesundheitsdaten konnten Dockweiler, Bocketta, Schnecke und Hornberg in einer Befragung deutschsprachiger Studenten zeigen, dass die Befragten zwar sensibilisiert für Datenschutzthemen waren, dies jedoch nicht deren Entscheidung zu beeinflussen schien, eine Fitness- oder Gesundheitsapp zu nutzen.[54] Insofern stellt sich die Frage, ob Wearable-Nutzer und Nicht-Nutzer sich in ihren generellen Datenschutzbedenken unterscheiden (**Forschungsfrage 8** zu Datenschutzbedenken von Nutzern und Nicht-Nutzern).

Forschungsfragen und Methoden, Tabelle 1.

1.4 METHODISCHER GESAMTÜBERBLICK

Die in Abschnitt 1.3 formulierten Forschungsfragen wurden mit Hilfe unterschiedlicher methodischer Herangehensweisen untersucht (Tabelle 1). Zunächst wurden zwölf Wearables mit den dazugehörigen Fitness-Apps

47 Z. B. McDonald & Cranor, 2009.
48 Sachverständigenrat für Verbraucherfragen, 2016; BMJV, 2008, Teil B; s. auch Plattform Verbraucherschutz in einer digitalisierten Welt, 2015.
49 Z. B. Dinev & Hart, 2006.
50 Acquisti, 2004; Tversky & Kahneman, 1974.
51 Für einen Überblick: Renn, 2008; Slovic, 2000.
52 YouGov, 2016, S. 9-10, Online-Interviews mit Personen ab 18 Jahren.
53 Z. B. Barnes, 2006; Norberg, Horne, & Horne, 2007.
54 Dockweiler, Boketta, Schnecke, & Hornberg, 2016.

ausgewählt und einer technischen Prüfung unterzogen. Hierdurch konnten Erkenntnisse zur Erhebung, Speicherung und zum Sendeverhalten der nutzergenerierten Daten sowie zu Einfluss- und Kontrollmöglichkeiten durch den Nutzer gewonnen werden. Andere für Verbraucher relevante funktionale Eigenschaften wie die Messgenauigkeit oder Handhabung der Geräte und Apps sind regelmäßig Gegenstand der Produkttests der Stiftung Warentest und nicht Bestandteil der vorliegenden Untersuchung.[55]

Weiterhin wurde geprüft, inwieweit Wearable-Anbieter ihre Nutzer hinreichend über den Umgang mit deren personenbezogenen Daten aufklären und – falls erforderlich – eine Einwilligung für die Nutzung und Weiterverarbeitung dieser Daten einholen. Die zur Verfügung gestellten Informationen wurden darüber hinaus hinsichtlich ihrer Schwierigkeit auf Textebene untersucht.

Im letzten Untersuchungsschritt wurde im Rahmen einer standardisierten, repräsentativen Befragung deutscher Internetnutzer erfasst, wie Verbraucher mögliche Folgen bei der Wearable-Nutzung bewerten und inwieweit sich Nutzer in ihren generellen Datenschutzbedenken von Nicht-Nutzern unterscheiden.

55 Stiftung Warentest, 2013, 2015, 2016a, 2016b.

2. TECHNISCHE PRÜFUNG

2.1 ANBIETER- UND GERÄTEAUSWAHL

Für die Untersuchung wurden Wearables von zwölf Anbietern ausgewählt (Tabelle 2). Die Auswahl umfasst zum einen diejenigen Anbieter, die von der International Data Corporation (IDC)[56] im Jahr 2015 in mindestens einem Quartal unter den Top fünf der globalen Wearable-Marktführer geführt wurden und eine an deutsche Verbraucher adressierte Internetseite haben. Dazu zählen: *Fitbit, Jawbone, Garmin, Apple* und *Samsung*.[57] Unter den Top fünf befindet sich außerdem der Anbieter *Xiaomi*, der keine Internetseite in deutscher Sprache anbietet, dessen Produkte jedoch mühelos von deutschen Verbrauchern über Online-Versandhändler bestellt werden können und ebenso mit in die Untersuchung aufgenommen wurde. Ausgewählt wurden außerdem Anbieter, deren Geräte in nationalen Online-Shops (*Otto*-Versand; betrifft die Anbieter *Polar, Striiv* und *Withings*) und Lebensmittel-Discountern (*Aldi, Lidl*; betrifft die Anbieter *A-Rival* und *Technaxx*) [58] vertrieben werden und somit eine große Zahl von Verbrauchern adressieren. Erfasst wurde außerdem der Anbieter *Runtastic*, der neben seiner vertriebenen Wearable-Hardware verschiedene Fitness-Apps anbietet. Diese belegen sowohl im *Google Play Store* als auch im *Apple Store* (iTunes) regelmäßig Platz eins der am häufigsten heruntergeladenen Fitness- und Gesundheits-Apps.[59]

Als einzige Fitness-App ohne eigene Anbieter-Hardware wurde *MyFitnessPal* mit in die Untersuchung aufgenommen. Diese ist nicht nur mit zahlreichen der getesteten Wearables kompatibel (u. a. *Withings, Garmin, Fitbit*) und wird teilweise auch entsprechend beworben, sondern wird ähnlich wie die *Runtastic*-App von Verbrauchern häufig heruntergeladen.[60]

Aufgrund ihrer großen Beliebtheit wurde ausschließlich Wristwear in die vorliegende Untersuchung mit einbezogen, das heißt Fitness-Armbänder und Smartwatches.[61] Wann immer möglich wurden hierbei Smartwatches getestet, die in der Regel mehr Funktionen als Fitness-Armbänder haben und dabei über die Möglichkeit verfügen, eine größere Fülle an schützenswerten Daten zu sammeln. Ausgewählt wurde dann jeweils dasjenige Modell, das, soweit über den Online-Auftritt des Anbieters ermittelbar, sich zum Zeitpunkt der Auswahl am kürzesten auf dem Markt befand. Hierdurch wurde sichergestellt, dass veraltete Modelle mit möglicherweise geringeren Datenschutzstandards nicht zu einer inaktuellen Bewertung der Anbieter führen konnten. Aufgrund begrenzter Ressourcen wurden keine Geräte untersucht, die über einem Preis von 500 Euro lagen, dies schränkte beispielsweise die Auswahl von Modellen des Anbieters *Apple* ein. Pro Anbieter wurde ein Gerät getestet: Verschiedene Modelle eines Anbieters können sich zwar hinsichtlich ihrer technischen Eigenschaften unterscheiden, es ist jedoch nicht anzunehmen, dass ein und derselbe Anbieter je nach Modell unterschiedlich mit den nutzergenerierten Inhalten umgeht.

In Kombination mit den Wearables waren auch die vom Anbieter empfohlenen Fitness-Apps Bestandteil der vorliegenden Untersuchung, jeweils für die Smartphone-Betriebssysteme iOS und Android. Ausnahmen hiervon waren die Apps von *Apple* und *Samsung*, die im ersteren Fall nur für iOS und im letzteren Fall zum Zeitpunkt der Prüfung nur für Android verfügbar waren.[62] Insgesamt wurden somit zwölf Wearables und 24 Fitness-Apps in die vorliegende Untersuchung mit einbezogen (Tabelle 2).

Übersicht der ausgewählten Wearables und Fitness-Apps, Tabelle 2.

56 IDC, 2016.

57 Nicht mit einbezogen wurde der Hersteller *BBT (XTC)*, da dieser eine ausschließlich auf dem asiatischen Markt zur Verfügung stehende und auf Kinder ausgerichtete Smartwatch anbietet.

58 Die Modelle dieser Anbieter waren zum Zeitpunkt der Auswahl im Lidl-Online-Shop sogar vergriffen (Stand: 12.05.2016).

59 Z. B. www.appannie.com; die kriteriengeleitete Auswahl nach App-Rankings wurde analog zu verschiedenen wissenschaftlichen Untersuchungen getroffen; z. B. Ackerman, 2013; Herrmann & Lindemann, 2016.

60 Z. B. www.appannie.com.

61 Ballhaus et al., 2015, S. 9.

62 Seit Anfang Januar 2017 ist die *Samsung Gear S2* auch mit iOS-Geräten kompatibel; Schwan, 2017.

2 ÜBERSICHT DER AUSGEWÄHLTEN WEARABLES UND FITNESS-APPS

Wearable	Art	Betriebssystem	App-Name	Version[b]
Apple Watch Sport	Smartwatch	iOS	Apple Health/ Activities[a]	9.3.2
A-Rival Qairós	Fitness-Armband	iOS	A-Rival	2.2
		Android	A-Rival Qairós	1.51
Fitbit Blaze	Smartwatch	iOS	Fitbit	2.24 (531)
		Android	Fitbit	2.28
Garmin Forerunner 735XT	Smartwatch	iOS	Garmin Connect Mobile	3.7
		Android	Garmin Connect Mobile	3.7.0.3
		iOS	MyFitnessPal	6.19.2
		Android	MyFitnessPal	5.12.2
Jawbone UP 3	Fitness-Armband	iOS	UP	4.20
		Android	UP	4.20
Polar V800	Smartwatch	iOS	Polar Flow	3.2.1
		Android	Polar Flow	3.2.1
Runtastic Moment Classic	Smartwatch	iOS	Runtastic Me	1.7.1
		Android	Runtastic Me	1.8
Samsung Gear S2	Smartwatch	Android	S Health	4.8.1.0025
Striiv Fusion Bio	Fitness-Armband	iOS	Striiv	2.2.302
		Andr	Striiv	1.0.1865p
Technaxx Classic TX-37	Fitness-Armband	iOS	Technaxx My Fitness	1.4.7
		Android	Technaxx My Fitness	1.2.1
Withings Uhr Activité	Smartwatch	iOS	Health Mate	2.14.0
		Android	Health Mate	2.16
Xiaomi Mi Band Pulse	Fitness-Armband	iOS	Mi Fit	2.1.4
		Android	Mi Fit	2.1.4

a *Apple Health* erlaubt das Erfassen und Auswerten von einer Vielzahl von Gesundheitsdaten, sowie das Verknüpfen von Daten aus Drittanbieter-Apps auf dem iPhone. *Apple Activities* erlaubt die Erfassung von Trainingseinheiten und -zielen.

b Die geprüften Apps wurden in der zu Beginn der Erhebungsphase aktuell verfügbaren Version getestet (Erhebungsphase: 01.Juli – 11. August 2016). Die Ergebnisse der technischen Prüfung beziehen sich nicht auf seitdem ggf. aktualisierte Versionen.

Die ausgewählten Wearables wurden mit den dazugehörigen Apps für iOS und Android einer technischen Prüfung unterzogen. Innerhalb dieser wurde die Bluetooth-Schnittstelle des Wearables, das Datenspeicherverhalten der App sowie insbesondere ihr Datensendungsverhalten untersucht.[63]

Geprüft wurde, welche Nutzerdaten erhoben, gespeichert und genutzt werden – das heißt, welche Daten wohin übertragen werden (Forschungsfrage 1) und inwieweit die Nutzerdaten sicher vor unberechtigtem Zugriff sind (Forschungsfrage 2). Hierbei wurde der Fokus auf den Schutz vor ungewollter Standortverfolgung (Tracking) und den sicheren Transport der Daten von der App zum Anbieter-Server gelegt.[64] Ebenso wurde geprüft, inwieweit Nutzer die Speicherung und Übermittlung der Daten durch die App beeinflussen können (Forschungsfrage 3).

Android-Apps wurden auf einem *LG Nexus 5* (Android 6.0.1) geprüft; für iOS Apps wurde ein *iPhone 6* (16 GB; iOS 9.3.2) eingesetzt. Die Prüfung wurde von der *datenschutz nord GmbH*[65] im Auftrag des Projekts Marktwächter Digitale Welt[66] zwischen dem 01. Juli und 11. August 2016 durchgeführt.[67]

Im Folgenden werden die Untersuchungsmethode und Ergebnisse jeweils gemeinsam für die Ebene der Bluetooth-Verbindung zwischen Wearable und Smartphone (Abschnitt 2.1), die Übermittlung (Abschnitt 2.2) und Speicherung (Abschnitt 2.3) personenbezogener Daten durch die App berichtet.

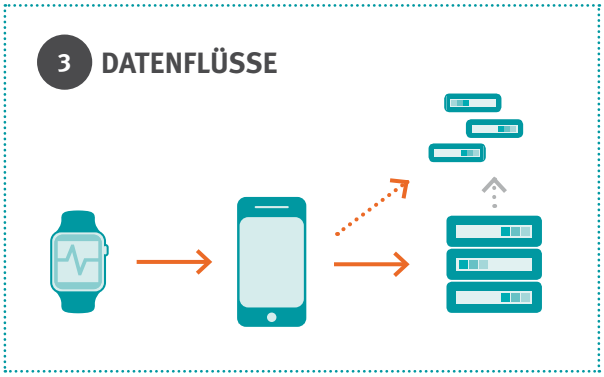
63 Die App *MyFitnessPal* wurde im Rahmen der Prüfung mit dem *Garmin Connect* Konto verbunden, da hierfür auf der Webseite von *MyFitnessPal* ausdrücklich geworben wird (Stand: 26.10.2016). Da die Ergebnisse für die Bluetooth-Verbindung jedoch Hardware-spezifisch sind und sich daher mit den Ergebnissen für die *Garmin*-Smartwatch decken, werden Ergebnisse der technischen Prüfung für *MyFitnessPal* nur für das Datensendungs- und -speicherverhalten der App berichtet.

64 S. auch Hilts, Parson, & Knockel, 2016.

65 www.datenschutz-nord-gruppe.de.

66 Im Projekt Marktwächter Digitale Welt beobachten und analysieren der Verbraucherzentrale Bundesverband (vzbv) unter Beteiligung der 16 Verbraucherzentralen den Markt in Deutschland, um Missstände früh zu erkennen und auf Fehlentwicklungen aufmerksam zu machen. Die Verbraucherzentrale NRW ist eine von fünf Schwerpunkt-Verbraucherzentralen im Projekt und beschäftigt sich mit Entwicklungen rund um das Thema Nutzergenerierte Inhalte.

67 Ein Überblick über die technischen Prüfpunkte ist abrufbar unter http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps.



2.2 BLUETOOTH-VERBINDUNG DES WEARABLES

Damit ein Wearable die gemessenen Daten an das Endgerät des Nutzers übertragen kann, müssen Wearable und Endgerät aktiv miteinander gekoppelt sein. Hierzu muss das Endgerät das Wearable innerhalb eines Netzwerks zunächst eindeutig erkennen können. Um dies zu ermöglichen, senden Wearables Datenpakete aus (sog. Advertising Packets). Diese Datenpakete enthalten verschiedene auslesbare Informationen, wie beispielsweise die einzigartige Hardware-Adresse des Wearables (sog. Media Access Control Adresse; MAC-Adresse).

Das Aussenden der Advertising Packets bietet gleichermaßen jedoch eine Angriffsfläche, denn die MAC-Adresse kann potenziell auch von fremden Geräten ausgelesen werden. Statische – das heißt sich nicht ändernde – MAC-Adressen lassen dann eine eindeutige Identifizierung des Geräts durch fremde Geräte zu, wodurch es über örtlich verteilte Messpunkte möglich wäre, Bewegungsprofile eines Nutzers zu erstellen und ihn somit anhand seines Wearables zu tracken.[68] Das Wearable sollte daher, wenn der Nutzer das Gerät einmal in Gebrauch hat, keine Daten über Advertising Packets mehr senden, anhand derer das Gerät für Fremde eindeutig identifizierbar ist.

Ist das Wearable aktiv an das Smartphone des Nutzers gekoppelt, muss es keine Advertising Packets mehr senden, da das ursprüngliche Ziel des Verbindungsaufbaus bereits erreicht wurde. Wird die Kopplung unterbrochen (inaktive Kopplung),[69] werden zwar

68 Z. B. Hilts et al., 2016; Di Luzio, Mei, & Stefa, 2016.

69 Dies ist beispielsweise der Fall, wenn das gekoppelte Smartphone ausgeschaltet ist, sich in zu großer Distanz zum Wearable befindet, oder seine Bluetooth-Funktion deaktiviert ist.

vermutlich wieder Advertising Packets gesendet, dort enthaltene Informationen wie die MAC-Adresse sollten dann jedoch anderweitig vor ungewolltem Tracking geschützt werden. Beispielsweise sind die getesteten Wearables Bluetooth Low Energy-Geräte, die technisch dazu in der Lage sind, ihre MAC-Adresse mit Hilfe eines privaten Schlüssels in regelmäßigen Abständen zu ändern (sog. MAC-Randomisierung). Der Schlüssel wird zwischen dem Wearable und dem gekoppelten Gerät ausgetauscht, sodass nur das gekoppelte Endgerät die MAC-Adresse des Wearables kennt. Das Wearable ist für fremde Geräte dann nicht mehr eindeutig identifizierbar.[70]

Wearables können jedoch nicht nur über ihre MAC-Adresse identifiziert werden: Im Zuge des ersten Verbindungsaufbaus sendet das Wearable innerhalb eines sogenannten GATT-Profils[71] weitere Informationen an das Endgerät, das beispielsweise Informationen wie die Seriennummer oder andere identifizierende Merkmale enthalten kann. Lässt das Wearable bei inaktiver Kopplung eine Verbindung mit fremden Geräten zu, können diese Informationen auch durch unbefugte Dritte ausgelesen werden. So wäre es möglich, dass ein Wearable zwar seine MAC-Adresse regelmäßig ändert, ein ungewolltes Tracking durch Dritte jedoch über die im GATT-Profil gespeicherten und auslesbaren Daten möglich bleibt.

Methode. Um zu überprüfen, inwieweit die getesteten Wearables sicher vor ungewolltem Tracking sind, wurden die Geräteinformationen der Wearables zu verschiedenen Testzeitpunkten abgefragt,[72] nämlich vor der Kopplung mit dem Smartphone, nach der Kopplung (aktive Kopplung) und bei deaktivierter Bluetooth-Verbindung des gekoppelten Smartphones (inaktive Kopplung). Überprüft wurde, zu welchen Messzeitpunkten Datenpakete gesendet wurden[73] und ob über den Zugriff auf das GATT-Profil weitere Daten auslesbar waren.

Ergebnisse. In aktiv gekoppeltem Zustand werden mit nur einer Ausnahme (*Technaxx*) keine Advertising Packets gesendet: Die Geräte sind dann weder über eine MAC-Adresse identifizierbar, noch können anderweitige Informationen über das GATT-Profil ausgelesen werden.

Bei inaktiver Kopplung sendet die Mehrzahl der Wearables Advertising Packets (Tabelle 4; Ausnahme: *Samsung Gear S2*). Insgesamt sind im Zuge dessen zehn von zwölf Geräten eindeutig über ihre MAC-Adresse identifizierbar (Tabelle 4; Ausnahmen: *Withings, Samsung*). Nur die *Withings Activité* randomisiert hierbei ihre MAC-Adresse. Die Adresse der *Apple Watch* ändert sich während des Installationsprozesses, bleibt jedoch zu weiteren Messzeitpunkten konstant.[74] Über das GATT-Profil sind bei inaktivem Kopplungszustand bei neun von zwölf Geräten weitere Daten auslesbar (Ausnahmen: *Polar, Samsung, Withings*).

Aussenden von Geräteinformationen via Bluetooth. Tabelle 4

2.3 DATENSENDUNGSVERHALTEN DER APP

In Bezug auf das Datensendungsverhalten der App wurde untersucht, welche Daten wohin im Zuge der Wearable-Nutzung von der App übertragen werden, und wie sicher die Datenverbindung zwischen der App und möglichen Empfänger-Servern ist.

Methode. Um das Datensendungsverhalten der Apps in möglichst alltagstypischen Situationen zu ermitteln, wurde der Datenverkehr während verschiedener Nutzungsphasen erfasst, wie beispielsweise dem Durchführen eines Trainings, dem manuellen Hinzufügen von Informationen (Wunschgewicht, Profilbild o. ä.) oder der Einladung eines Kontakts im Adressbuch.

Der Datenverkehr wurde jeweils vor und nach Registrierung eines neuen Benutzerkontos und der damit verbundenen Zustimmung zu Nutzungsbedingungen und gegebenenfalls den Datenschutzbestimmungen erfasst. Darüber hinaus wurde der Datenverkehr unter per Grundeinstellung vorgegebenen App-Berechtigungen

70 Lester & Stone, 2016; s. auch Wang, 2014. Die Randomisierung der MAC-Adresse kann die Bedienbarkeit des Wearables unter Umständen herabsetzen, wenn das Smartphone und das Wearable sich nach Änderung der MAC-Adresse jedes Mal neu koppeln müssen.

71 Generic Attributes Profile, https://www.bluetooth.com/specifications/generic-attributes-overview [Stand: 27.01.2017].

72 Hierzu wurde die Android-App nRF Connect Version 4.3.0 von *Nordic Semiconductor* eingesetzt.

73 Zur Verifizierung der Ergebnisse wurden die MAC-Adressen der Wearables einige Tage später erneut ausgelesen. Es ist möglich, dass sich die MAC-Adresse nach diesem Zeitpunkt noch geändert hat, dies wurde nicht überprüft. Der Inhalt der über ID-Variablen hinaus auslesbaren Rohdaten konnte mit dieser Methodik nicht ermittelt werden.

74 Für gegenteilige Ergebnisse für iOS-Geräte s. Hilts et al., 2016; Lester & Stone, 2016.

4 AUSSENDEN VON GERÄTEINFORMATIONEN VIA BLUETOOTH

	MAC-Adresse vor Kopplung	MAC-Adresse in Kopplungszustand		weitere Daten auslesbar in Kopplungszustand [b]	
Wearable		aktiv	inaktiv	aktiv	inaktiv
Apple Watch	5F:7D:01:02:B9:50	unbekannt	5F:7D:01:02:B9:50	nein	ja
A-Rival Qairós	F8:6B:33:C9:70:7B	unbekannt	F8:6B:33:C9:70:7B	nein	ja
Fitbit Blaze	F3:CF:9D:5B:3B:E7	unbekannt	F3:CF:9D:5B:3B:E7	nein	ja
Garmin Forerunner 735XT	F1:E5:74:51:7B:51	unbekannt	F1:E5:74:51:7B:51	nein	ja
Jawbone UP 3	F0:3A:E3:5D:F3:29	unbekannt	F0:3A:E3:5D:F3:29	nein	ja
Polar V800	00:22:D0:86:20:4E	unbekannt	00:22:D0:86:20:4E	nein	nein
Runtastic Moment	C2:9E:FF:69:D0:5D	unbekannt	C2:9E:FF:69:D0:5D	nein	ja
Samsung Gear S2	7C:91:22:AD:E1:C5	unbekannt	unbekannt	nein	nein
Striiv Fusion	D7:54:FA:AC:2A:CA	unbekannt	D7:54:FA:AC:2A:CA	nein	ja
Technaxx Classic TX-37	E0:E5:CF:8F:4D:E7	E0:E5:CF:8F:4D:E7	E0:E5:CF:8F:4D:E7	ja	ja
Withings Activité [a]	14:32:38:53:31:FA	unbekannt	33:AD:87:AE:07:56	nein	nein
Xiaomi Mi Band Pulse	C8:0F:10:7C:B7:B3	unbekannt	C8:0F:10:7C:B7:B3	nein	ja

a Zu beachten ist die veränderte MAC-Adresse vor Kopplung und bei inaktiver Kopplung.
b Im Rahmen des Projektes war es nicht möglich, für jedes Wearable den konkreten Inhalt der auslesbaren Rohdaten zu ermitteln.

einerseits und unter Entzug von App-Berechtigungen[75] andererseits ermittelt. Hierdurch konnte überprüft werden, welchen Einfluss dies auf das Datensendungsverhalten der App, im Vergleich zu den ursprünglich vorgegebenen Grundeinstellungen, hat. Über letztere fordern die getesteten Apps eine Vielzahl von Zugriffsberechtigungen – wie beispielsweise Zugriff auf die Kontakte des Nutzers oder den Speicher des Smartphones (Tabelle 5).

Auswahl angeforderter Zugriffsberechtigungen (Grundeinstellungen). Tabelle 5.

Um festzustellen, ob die Apps unaufgefordert Kontaktdaten übermitteln, wurden vor Durchführung des Tests in den Adressbüchern der Smartphones drei Kontakte abgespeichert. Von diesen Kontakten wurden innerhalb der Einladungsfunktion der App jeweils zwei Kontakte eingeladen und einer explizit nicht eingeladen, sodass die Übermittlung dieses Kontaktes an den Anbieter einen unaufgeforderten Zugriff darstellen würde.

Um den Internetverkehr der Fitness-App aufzuzeichnen, wurde ein Man-in-the-middle-Angriff durchgeführt: Hierbei wurde der Datenverkehr zunächst über das Mobilfunknetz deaktiviert und der gesamte WLAN-Verkehr der Smartphones über einen eigenen Server geleitet (http-Proxy).[76] Um transportverschlüsselte Verbindun-

75 Bei iOS und unter Android ab Version 6 können App-Berechtigungen wie der Zugriff auf den internen Speicher, Kalender, Kontakte, Kamera oder Mikrophon entzogen werden, z. B. Barczok & Porteck, 2015.

76 Der eingesetzte Proxy-Server war Burp Suite (Version 1.7.03) der Firma

5 AUSWAHL ANGEFORDERTER ZUGRIFFSBERECHTIGUNGEN (GRUNDEINSTELLUNGEN)

App-Anbieter[a]	Standort	Kontakte	Kamera	Kalender	Fotos	Telefon	SMS	Speicher
Apple (iOS)	✓	✓	✓	×	×	✓	✓	✓
A-Rival	×	✓	×	×	×	×	✓	✓
Fitbit	✓	✓	✓	×	×	✓	✓	✓
Garmin	✓	✓	✓	✓	×	✓	×	✓
Jawbone	✓	✓	✓	×	×	✓	×	✓
MyFitn.Pal	✓	✓	✓	×	×	×	×	✓
Polar	✓	✓	×	✓	×	✓	×	✓
Runtastic	✓	✓	×	×	×	✓	×	✓
Samsung	✓	✓	✓	×	×	✓	✓	×
Striiv	✓	✓	×	✓	×	✓	✓	✓
Technaxx	×	×	×	×	×	×	×	✓
Withings	✓	✓	✓	×	×	×	×	✓
Xiaomi	✓	✓	✓	×	×	✓	✓	✓

a Am Beispiel von Android (Ausnahme: *Apple*, hier werden die Ergebnisse für iOS berichtet).

gen einsehen zu können, wurde der Smartphone-App ein anderes, nicht vom Server stammendes Zertifikat präsentiert, das zuvor von der Proxysoftware erstellt wurde. Der so aufgezeichnete Datenverkehr wurde anschließend analysiert, um die Übertragung von Daten innerhalb verschiedener Datenkategorien zu prüfen (Tabelle 6). Geprüft wurde auch, ob zusätzliche Maßnahmen zur Absicherung des Datenverkehrs der App getroffen wurden.[77]

Ergebnisse Übertragungssicherheit. Mit Ausnahme der Fitness-Apps von *A-Rival* und *Technaxx*, für deren jeweils zwei getesteten Apps zum Zeitpunkt der Prüfung kein ausgehender Datenverkehr beobachtet wurde, zeichnen sich alle Apps durch ein ausgeprägtes Datensendungsverhalten aus (zwanzig von 24 getesteten Apps). Die Übertragung personenbezogener Daten in den verbleibenden zwanzig Apps erfolgte ausnahmslos unter Einsatz von Transportverschlüsselung (https). Zusätzliche Sicherungsmechanismen konnten nur bei der Datenübertragung der Fitness-App *Apple Health/Activities* an den Anbieter-Server in Form von Certificate Pinning festgestellt werden. Hierbei wird die Datenübertragung vor ungewolltem Zugriff durch Dritte – zum Beispiel bei Man-in-the-middle-Angriffen – geschützt, indem die App Anfragen von potentiellen Empfänger-Servern nur unter sehr strengen Bedingungen als vertrauenswürdig einstuft und auch nur dann Daten dorthin sendet.[78] Daher konnte für diese App auch nicht analysiert werden, welche Daten an den Anbieterserver kommuniziert werden.

Ergebnisse Datenübermittlung an Anbieter. Zwanzig der 24 getesteten Apps übertragen Daten an die Server des Anbieters (Tabelle 7). Dies kann beispielsweise notwendig sein, um Funktionen der App zu gewährleisten oder einen eingebundenen Online-Dienst wie bei-

PortSwigger; zur genaueren Beschreibung der Methodik z. B. Eikenberg, 2012.

77 Auf unbekannte Weise komprimierte, kodierte oder verschlüsselte Daten konnten im Rahmen der technischen Prüfung nicht eingesehen werden. Zum Beispiel übermittelten einige Apps den kompletten binären Inhalt des Wearable-Speichers zur Auswertung an den Server, anstatt die Auswertung in der App auf dem Smartphone vorzunehmen. Ohne eine im Rahmen dieses Projekts nicht mögliche, aufwändige Nachkonstruktions-Untersuchung (sog. reverse engineering) der eingesetzten Hardware und Speicherformate ließen sich diese Daten nicht analysieren. Dies, sowie die Tatsache, dass die Wearables und Apps nur über einen begrenzten Zeitraum getestet wurden, schließt nicht aus, dass bei regelmäßiger Nutzung auch Daten von der App übermittelt werden, die innerhalb der vorliegenden Testung nicht abgefangen werden konnten.

78 Hilts et al., 2016, S. 35.

6 DATENKATEGORIEN UND BESCHREIBUNGEN

Datenkategorie	Beschreibung
Profildaten	Vom Nutzer im Rahmen der Nutzung oder des Registrierungsprozesses eingegebene Daten, wie Benutzername, Klarname, Passwort, E-Mail-Adresse, Geschlecht, Geburtsdatum, Größe, Gewicht oder Land.
Trainingsdaten[a]	Mittels Durchführung eines Trainingsprogramms oder manuelles Hinzufügen im Training erzeugte Daten, wie Schrittzahl oder gelaufene Strecke.
Gesundheitsdaten[a]	Vom Wearable gemessene Daten, wie die Herzfrequenz oder das Schlafverhalten.
Lokalisationsdaten	Beim Training oder auf andere Weise erhobene Lokalisationsdaten in Koordinatenform.
Ernährungsdaten[a]	Vom Nutzer eingegebene Daten zur Ernährung, z. B. konsumierte Nahrungsmittel.
Kontaktdaten	Im Rahmen der Einladungsfunktion der Fitness-App versendete Kontaktinformationen, z. B. E-Mail-Adressen.
Nutzungsverhalten	Daten zum Nutzungsverhalten, bspw. Übermittlung der App-Bedienung, Zeitpunkte der Synchronisation mit dem Wearable oder Batteriestatus.
Technische Daten	App-Version, Produktname und (Firmware-) Version des verwendeten Wearables, Produktname und Betriebssystemversion des verwendeten Smartphones.

a Zu Darstellungszwecken wird zwischen Gesundheitsdaten, Trainingsdaten und Ernährungsdaten differenziert. Trainingsdaten und Ernährungsdaten können jedoch ebenfalls mittelbaren Aufschluss über den Gesundheitszustand einer Person geben.

spielsweise Updates des eigenen Online-Profils zu realisieren. Allerdings übermitteln 15 dieser zwanzig Apps auch Daten zum Nutzungsverhalten an den Anbieter, die für die Inanspruchnahme der angebotenen Dienstleistung vermutlich nicht erforderlich sind.[79] Ausnahmen sind hier die Apps von *Xiaomi* und *Polar*, jeweils für iOS und Android (nicht analysierbar für *Apple*). Bei neun der Apps werden diese Daten schon vor Registrierung eines neuen Benutzerkontos und der damit verbundenen Zustimmung zu den Nutzungsbedingungen und gegebenenfalls den Datenschutzbestimmungen gesendet (unter iOS und Android: *Garmin*, *Runtastic* und *Striiv*; nur unter Android: *Withings* und *MyFitnessPal*; nur unter iOS: *Jawbone*). Zu diesem Zeitpunkt werden außerdem bei 17 Apps schon technische Daten an den Anbieter übermittelt (Ausnahmen: *Polar* unter iOS und Android, nicht analysierbar für *Apple*). Für *Apple* konnte aufgrund der zusätzlichen Sicherung der Datenübertragung nicht analysiert werden, welche Daten an den Anbieterserver übertragen werden.

Fitbit und *Runtastic* senden bei Verwendung der Einladungsfunktion die E-Mail-Adressen aller auf dem Smartphone gespeicherten Kontakte an den Anbieterserver. Durch eine Einstellung am mobilen Endgerät kann dieses Verhalten auf beiden getesteten Betriebssystemen durch Entzug der App-Berechtigung „Kontakte“ unterbunden werden. Allerdings kann die Einladungsfunktion dann überhaupt nicht mehr verwendet werden, sodass der Nutzer nur die Wahl zwischen der Übermittlung aller oder keiner seiner Kontakte hat.

Garmin übermittelt auch bei ausgeschalteter Standortberechtigung Laufstrecken an den *Garmin*-Anbieter-Server, da für die Messung die GPS-Funktion des Wearables (und nicht des Smartphones) benutzt wird. Bei Synchronisation des Wearables mit dem *Garmin-Connect-Server* wird der Speicher des Wearables (und somit die erfassten Strecken) hochgeladen und ausgewertet.

79 Die Beurteilung, ob eine Information erforderlich für die gewünschte Dienstleistung ist, wurde durch die *datenschutz nord GmbH* vorgenommen.

7 DATENSENDUNGSVERHALTEN: ERHEBUNG VON DATEN DURCH DEN ANBIETER

App-Anbieter[a]	Profil	Training	Gesundheit	Lokalisation	Ernährung	Nutzung	Kontakte	Technisch
Apple[b]	–	–	–	✓	–	–	–	–
A-Rival	×	×	×	×	×	×	×	×
Fitbit	✓	✓	✓	✓	✓	✓	✓	✓
Garmin	✓	✓	✓	✓	✓	✓	×	✓
Jawbone	✓	✓	✓	✓	✓	✓	✓	✓
MyFitn.Pal	✓	✓	✓	×	✓	✓	×	✓
Polar	✓	✓	✓	✓	×	×	×	✓
Runtastic	✓	✓	✓	×	×	✓	✓	✓
Samsung	✓	✓	✓	✓	✓	✓	×	✓
Striiv	✓	✓	✓	×	✓	✓	×	✓
Technaxx	×	×	×	×	×	×	×	×
Withings	✓	✓	✓	×	×	✓	×	✓
Xiaomi	✓	✓	✓	×	×	×	×	✓

a Es wurden hierbei keine Unterschiede zwischen iOS und Android festgestellt.
b Das Datensendungsverhalten an den Anbieter konnte in diesem Fall nicht analysiert werden, da *Apple* die Übertragung über zusätzliche Mechanismen vor ungewolltem Zugriff sichert; der Abruf von Kartenmaterial für *Apple Maps* erfolgte unverschlüsselt.

Welche Daten genau an den Anbieter gesendet werden, kann bei sechs Anbietern zumindest teilweise über die Deaktivierung von App-Berechtigungen kontrolliert werden (*Fitbit, Jawbone, Runtastic, Samsung, Striiv* und *Xiaomi*). So lässt sich beispielsweise bei *Fitbit* unter iOS, bei *Runtastic* unter Android und bei *Samsung* verhindern, dass Gesundheitsdaten an den Anbieter gesendet werden. Bei *Samsung* lässt sich zudem unterbinden, dass Daten zum Nutzungsverhalten oder technische Details wie App-/Trackerdaten übermittelt werden. Bei *Garmin, MyFitnessPal, Polar* und *Withings* gibt es für den Nutzer über den Entzug von Berechtigungen hingegen weniger Möglichkeiten, Datenflüsse zu kontrollieren und somit zu reduzieren. Keine der Apps mit Online-Verbindung erlaubte die gänzliche Offline-Verwendung oder Einschränkung des Datenverkehrs.

Ergebnisse Datenübermittlung an Drittanbieter. Zusätzlich zur Übermittlung an den Anbieter können – wiederum durch den Anbieter gesteuert – weitere Server in die Datenverarbeitung mit eingebunden werden, die direkt von der App kontaktiert werden können (sog. Drittanbieter).[80] Drittanbieter-Server können in manchen Fällen für die Funktionen der Apps notwendig sein oder um Daten extern (zwischen) zu speichern. Zusätzlich können Daten auch zu Drittanbietern übermittelt werden, um Nutzungsverhalten zu analysieren und statistisch zu verarbeiten. Die somit gewonnenen Erkenntnisse über das Nutzungsverhalten können der Verbesserung von Dienstleistungen dienen, jedoch auch ein Tracking des Nutzers ermöglichen (sog. Analytics-Dienste). Außerdem können Server zum Einsatz kommen, die steuern, welche Werbung Nutzer auf Basis der analysierten Nutzungsdaten sehen. Derlei Ad-Server erfassen und analysieren außerdem auch das anschließende Surf-Verhalten des Nutzers, um den Erfolg der geschalteten Werbung zu messen. Für die reine unmittelbare Funktionalität und Nutzung der App sind Werbe- und Analytics-Drittanbieter oft nicht erkennbar erforderlich.

Die Prüfung der Datenübermittlung an Drittanbieter zeigte, dass 19 von 24 Fitness-Apps Daten an eine variierende Anzahl und Art von Drittanbietern versenden

80 Z. B. Schneider, Enzmann, & Stopczynski, 2014.

8 ANZAHL UND ART EINGEBUNDENER DRITTANBIETER

App-Anbieter[a]	Drittanbieter gesamt	Werbung	Analyse, Tracking	Andere
Apple (iOS)	0	0	0	0
A-Rival	0	0	0	0
Fitbit	2	0	1	1
Garmin	4	0	1	3
Jawbone	4	0	2	2
MyFitnessPal	10	5	4	1
Polar	2	0	1	1
Runtastic	4	1	1	2
Samsung	4	0	1	3
Striiv	6	0	3	3
Technaxx	0	0	0	0
Withings	3	0	3	0
Xiaomi	1	1	0	0

a Am Beispiel von Android (Ausnahme: *Apple*, hier werden die Ergebnisse für iOS berichtet). Nur bei den Apps von *Xiaomi*, *Garmin* und *Striiv* wurden geringfügige Unterschiede bezüglich der Anzahl eingebundener Drittanbieter zwischen der jeweiligen iOS- und Android-Version festgestellt.

(Tabelle 8, Tabelle 9). Dieses Verhalten ist durch den Nutzer kaum kontrollierbar. *MyFitnessPal* sendet Daten an zehn Drittanbieter, darunter befinden sich vor allem Werbe- und Analytics-Anbieter. Neun dieser zehn eingebundenen Server sind für die angebotene Dienstleistung nicht erkennbar erforderlich (Tabelle 8).[81]

Der überwiegende Anteil dieser Apps sendet schon vor einer Möglichkeit zur Zustimmung Daten an Drittanbieter-Server (16 von 19 Apps). Dies sind im Wesentlichen Daten zum Nutzungsverhalten oder Informationen zu technischen Details, die beispielsweise ein Tracking des Nutzers ermöglichen. Ausnahmen hiervon sind die beiden Apps von *Polar* und die Android-App von *Xiaomi*, die erst nach einer Möglichkeit zur Zustimmung Daten an Drittanbieter weitergeben. Die *Apple Health/ Activities*-App scheint keine Drittanbieter in den Datensendungsprozess mit einzubauen; die Apps von *A-Rival* und *Technaxx* bauen keine Online-Verbindung auf und übertragen entsprechend auch keine Daten an Drittanbieter.

2.4 DATENSPEICHERVERHALTEN DER APP

Methode. Nach Aufzeichnung des Datensendungsverhaltens wurde der App-interne Speicher der Apps ausgelesen. Die gespeicherten Daten wurden unter beiden Betriebssystemen in XML- oder Datenbank-Dateien (sog. SQLite-Datenbanken) abgelegt und konnten somit systematisch durchsucht werden.[82] Für Android-Fitness-Apps wurde zusätzlich geprüft, ob auch Daten auf dem externen Speicher des Telefons (SD-Karte) abgelegt werden.[83] Diese externe Speicherung stellt ein Si-

81 Die Beurteilung, ob eine Information erforderlich für die gewünschte Dienstleistung ist, wurde durch die *datenschutz nord GmbH* vorgenommen. *MyFitnessPal* hat als einzige App in der Untersuchung mit einbezogenem App-Anbieter keine Einnahmen aus dem Hardware-Vertrieb. Der Einbezug zahlreicher Drittanbieter legt den Schluss nahe, dass das Hauptfinanzierungsmodell auf Werbeeinnahmen basiert. Zugrunde liegende Geschäftsmodelle wurden in der vorliegenden Untersuchung nicht tiefergehend beleuchtet.

82 SQLite-Datenbanken wurden hierzu mit Hilfe des sqlite3-Tools über die „dump"-Funktion in Textdateien umgewandelt; XML-Dateien lagen bereits als Textdateien vor.

83 Dies wurde nur für Android-Geräte geprüft, da Apple-Geräte über keinen externen Speicher verfügen.

9 DATEN, DIE AN MINDESTENS EINEN DRITTANBIETER GESENDET WERDEN

Datenkategorien	Apple (iOS)	A-Rival	Fitbit	Garmin	Jawbone	MyFitness Pal	Polar	Runtastic	Samsung	Striiv	Technaxx	Withings	Xiaomi
Benutzername	×	×	×	×	×	×	×	×	×	×	×	×	×
E-Mail	×	×	×	×	✓[a]	×	×	×	×	×	×	×	×
Passwort	×	×	×	×	×	×	×	×	×	×	×	×	×
Name	×	×	×	×	✓[a]	×	×	×	×	×	×	×	×
Telefonnummer	×	×	×	×	×	×	×	×	×	×	×	×	×
Land	×	×	×	×	×	×	×	×	×	×	×	×	×
Geschlecht	×	×	×	×	×	×	×	×	×	×	×	×	×
Geburtsdatum	×	×	×	×	×	×	×	✓	×	×	×	×	×
Größe	×	×	×	×	×	×	×	×	×	×	×	×	×
Gewicht	×	×	×	×	×	×	×	×	×	×	×	×	×
Trainingsdaten	×	×	×	×	×	×	×	×	×	×	×	×	×
Gesundheitsdaten	×	×	×	×	×	×	×	×	×	×	×	×	×
Lokalisationsdaten	×	×	✓	✓	×	✓	✓	×	✓	×	×	×	×
Ernährungsdaten	×	×	×	×	×	×	×	×	✓	×	×	×	×
Kontaktdaten	×	×	×	×	×	×	×	×	×	×	×	×	×
Nutzungsverhalten	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×
Technische Daten	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓

a Datum wurde nur in der iOS-Version der App gesendet.

cherheitsrisiko dar, da andere Apps auf dem Smartphone mit Zugriffsberechtigung auf denselben Speicherort Dateien auslesen oder bearbeiten können – und somit ein Datenaustausch zwischen verschiedenen Apps stattfinden kann.

Ergebnisse. Das Datenspeicherverhalten konnte mit Ausnahme von *Apple Health/Activities* und der iOS-Version der *A-Rival*-App analysiert werden (22 von 24 Apps). Die gespeicherten Daten werden bei allen 22 Apps im App-internen Speicher abgelegt. Dieser ist unverschlüsselt, jedoch nicht ohne weiteres vom Nutzer oder anderen Smartphone-Apps auslesbar. Neben den Anmeldedaten speichern die Apps auch Gesundheitsdaten (zwanzig von 22 Apps, Ausnahme: *Samsung S Health* und *Runtastic* unter Android). Mit Ausnahme der *A-Rival*-App für Android hinterlegen alle Apps darüber hinaus auch Daten zum Nutzungsverhalten im internen App-Speicher. Die *Mi*-App von *Xiaomi* speichert diese unter Android auf dem externen Speicher (SD-Karte) des Smartphones ab. Für keine der 22 Apps ist eindeutig erkennbar, was die maximale Speicherdauer der Daten auf dem lokalen Speicher ist, noch, inwieweit die Speicherdauer der Daten durch den Nutzer einschränkbar ist. Eine Ausnahme stellt *Polar* dar. Hier kann der Nutzer entscheiden, ob die Daten unbegrenzt, für ein Jahr, oder für zwei Jahre gespeichert werden sollen – per Default ist die Option „immer“ eingestellt.

2.5 ZWISCHENFAZIT: TECHNISCHE PRÜFUNG

Die technische Prüfung von zwölf Wearables und insgesamt 24 Fitness-Apps sollte Einblicke in datenschutzrelevante Aspekte bei der Nutzung von Wearables und Fitness-Apps geben.

Forschungsfrage 1: Welche Daten werden im Zuge der Wearable-Nutzung erhoben, gespeichert und genutzt?

Alle getesteten Fitness-Apps mit Online-Verbindung zeichnen sich durch ein ausgeprägtes Datensendungsverhalten aus. Hierbei werden zum Teil sensible personenbezogene Daten an die Anbieter-Server übertragen.

Neunzehn der zwanzig Apps mit Online-Verbindung senden darüber hinaus Daten an Drittanbieter-Server. Dies geschieht, für den Nutzer nicht erkennbar, in 16 Fällen bereits vor Registrierung eines neuen Benutzerkontos und der damit verbundenen Zustimmung zu den Nutzungsbedingungen und gegebenenfalls den Datenschutzbestimmungen. Es ist in keiner Weise erkennbar, inwieweit Werbedienstleister und in einigen Fällen auch Analytics-Dienste erforderlich für die Nutzung der jeweiligen Fitness-App sind. Eine abschließende Beurteilung der Frage, welche Datenflüsse hier erforderlich sind, wird jedoch erschwert durch die Tatsache, dass nicht immer nachvollziehbar ist, welche Daten und Drittanbieter für die zur Verfügung gestellte Dienstleistung wirklich benötigt werden.

Forschungsfrage 2: Inwieweit sind die im Rahmen der Wearable-Nutzung generierten Daten vor dem Zugriff durch Unbefugte geschützt?

Sicherheitslücken wurden insbesondere in Bezug auf die Bluetooth-Verbindung festgestellt. So lassen zehn der zwölf getesteten Geräte eine eindeutige Identifizierung des Wearables durch Dritte zu, wenn die Kopplung zwischen Wearable und Smartphone inaktiv ist. Ein physisches Tracking durch Dritte kann somit unter Umständen nicht verhindert werden. Möglich wäre hierdurch beispielsweise, dass Betreiber von Einkaufszentren die Laufwege ihrer Kunden ohne deren Wissen oder Einwilligung tracken.[84]

Positiv in Bezug auf die Datensicherheit ist hervorzuheben, dass alle von den jeweiligen Apps ausgehenden Daten über Transportverschlüsselung vor unbefugtem Zugriff durch Dritte gesichert werden. Die Güte der Transportverschlüsselung konnte im Rahmen der vorliegenden Untersuchung zwar nicht vertieft geprüft, wohl jedoch über einen Man-in-the-middle-Angriff bei 19 der zwanzig Apps mit Online-Verbindung umgangen werden. In einer Untersuchung der TU Darmstadt wurde darüber hinaus gezeigt, dass die von Fitness-Apps eingesetzte Transportverschlüsselung nicht immer ausreichenden Schutz vor ungewolltem Zugriff bietet.[85] Insofern sind weitere Mechanismen zur Sicherung des Datenverkehrs wünschenswert und denkbar. So verwendet die App von *Apple* zur Sicherung der Datenübertragung Certificate Pinning, bei dem die App nur unter sehr strengen Voraussetzungen Daten an einen externen Server sendet.[86]

Forschungsfrage 3: Inwieweit räumen Wearable-Anbieter ihren Nutzern Möglichkeiten zur Einflussnahme und Kontrolle ihrer Daten ein?

Der Nutzer hat kaum Möglichkeiten, den Fluss seiner Daten zu kontrollieren. Selbst die Speicherdauer der Daten auf dem eigenen Smartphone lässt sich nur bei einem der insgesamt 13 untersuchten Anbieter einstellen, die Mindestspeicherdauer beträgt hierbei ein Jahr. Über den Entzug von App-Berechtigungen kann die Übermittlung sensibler Daten an den Anbieter lediglich teilweise eingeschränkt werden. Keine der Apps mit Online-Verbindung erlaubte die gänzliche Offline-Verwendung oder Einschränkung des Datenverkehrs.

Hinzu kommt, dass Verbraucher die Grundeinstellungen ihrer Apps nicht unbedingt ändern: Default-Werte werden kontextübergreifend eher akzeptiert (sog. Status Quo Bias)[87] und für den Einzelnen ist darüber hinaus nur schwer ersichtlich, welche Berechtigungen eine App tatsächlich braucht, ohne dass ihre Funktionsweise eingeschränkt ist.[88]

84 Hilts et al., 2016, S. 26.

85 https://www.tu-darmstadt.de/vorbeischauen/aktuell/news_details_157888.en.jsp [Stand: 06.02.2017].

86 Hilts et al., S. 17.

87 Samuelson & Zeckhauser, 1988.

88 Surfer haben Rechte, 2014.

3. INFORMATION UND EINWILLIGUNG

Damit Nutzer ihr Recht auf informationelle Selbstbestimmung ausüben können, müssen Anbieter ihre Nutzer zu Beginn des ersten Nutzungsvorgangs darüber informieren, auf welche Weise, in welchem Umfang und zu welchem Zweck sie personenbezogene Daten erheben[89] (§§ 4 Abs. 3, § 13 Abs. 1 TMG; Tabelle 7). Dies tun Anbieter in ihren Datenschutzerklärungen.[90] Diese Hinweise auf die Datenschutzpraxis können als Allgemeine Geschäftsbedingungen (AGB) auch durch das deutsche AGB-Recht der §§ 305 ff. BGB kontrolliert werden, soweit es im Rahmen des Wearable-Angebotes zu einem Vertragsverhältnis mit Verbrauchern kommt, das hierdurch näher geregelt wird. Bei der Nutzung der Anbieter-Produkte kommt es stets zu einem Vertragsverhältnis mit Verbrauchern.

Die Datenschutzerklärungen wurden für die in der Untersuchung berücksichtigten Apps abgerufen und rechtlich eingeordnet (Abschnitt 3.1).[91] Im Zuge dessen wurde in Kombination mit dem Installations- und Registrierungsprozess der Apps auch überprüft, ob Einwilligungen separat eingeholt werden.[92] In einem zweiten Schritt wurden Aspekte der Lesbarkeit der Datenschutzhinweise auf sprachlicher Ebene untersucht (Abschnitt 3.2).

Material. Vorab wurde bei der Auswahl des zu prüfenden Textmaterials berücksichtigt, ob eine Unterrichtung des Verbrauchers überhaupt erforderlich ist. So fand bei den Apps von *Technaxx* und *A-Rival* zum Zeitpunkt der technischen Prüfung keine Erhebung von Daten statt, da keine Daten an Anbieter- oder Drittanbieter-Server übertragen wurden. Die Datenschutzerklärungen dieser beiden Anbieter wurden nicht weiter analysiert, da nach Auffassung der Artikel-29-Datenschutzgruppe die Schutzvorschriften nicht anwendbar sind, wenn die Daten nicht außerhalb des Endgeräts des Nutzers verarbeitet werden.[93]

Für die Überprüfung wurden darüber hinaus ausschließlich Datenschutzerklärungen berücksichtigt, die in deutscher Sprache verfügbar waren: Da Kenntnisse der englischen Sprache – insbesondere vertragssprachliches, juristisches oder kommerzielles Englisch – bei deutschen Verbrauchern nicht vorausgesetzt werden können, sind entsprechende Angaben innerhalb eines solchen Regelwerks ungeachtet ihres eigentlichen Inhaltes als intransparent zu beurteilen und wurden daher nicht weitergehend analysiert. Sie können der Anforderung aus § 12, § 13 Abs. 1 TMG, den Betroffenen auf eine verständliche Art zu informieren nicht gerecht werden. Soweit der jeweiligen Bestimmung auch Regelungscharakter zukommt, stellt diese zudem eine Allgemeine Geschäftsbedingung dar. Intransparente Geschäftsbedingungen können jedoch nicht wirksam in einen Vertrag mit einem Verbraucher eingebunden werden und entfalten folglich keine Rechtswirkung.[94] Nicht berücksichtigt werden konnten dadurch die Datenschutzerklärungen der Anbieter *Xiaomi, Striiv* und *Withings*, da diese nur in englischer Sprache verfügbar waren.

Die *Fitbit*-Apps stellten in der Android- und iOS-Version unterschiedliche Datenschutzerklärungen bereit, sodass hier zwei Versionen geprüft wurden. Insgesamt wurden somit neun Datenschutzerklärungen von acht Anbietern geprüft: *Apple, Fitbit Android, Fitbit iOS, Garmin, Jawbone, MyFitnessPal*[95]*, Polar, Runtastic* und *Samsung* (Tabelle 10). Die Datenschutzerklärungen wurden am 05. September 2016 zuletzt abgerufen. Aktualisierungen, die nach diesem Datum durch Anbieter vorgenommen wurden, sind daher nicht Bestandteil der inhaltlichen Prüfung.

3.1 RECHTLICHE ASPEKTE

Die rechtliche Einordnung der Datenschutzerklärungen erfolgte anhand der gesetzlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG), des Telemediengesetzes (TMG) sowie der entsprechenden aktuellen Rechtsprechung.

89 Nach § 3 Abs. 3 BDSG ist „Erheben" das Beschaffen von Daten über den Betroffenen.

90 Für derlei Informationen werden oft unterschiedliche Bezeichnungen verwendet, z. B.: Datenschutzrichtlinien, -bestimmungen oder -hinweise.

91 Die rechtliche Prüfung wurde von Juristen der Verbraucherzentrale NRW vorgenommen.

92 Dokumentiert im Rahmen der technischen Prüfung durch die *datenschutz nord GmbH* für die zum Zeitpunkt der Erhebung aktuelle App-Version (Tabelle 2).

93 S. auch Artikel-29-Datenschutzgruppe, 2015; EU-Datenschutzrichtlinie 95/46/EGEC.6.

94 KG Berlin, Urteil vom 08.04.2016, 15 O 44/13, rechtskräftig.

95 Die Datenschutzerklärung von *MyFitnessPal* stellte ergänzende Informationen in aufklappbaren Texten bereit.

10 ABGERUFENE DATENSCHUTZERKLÄRUNGEN (DSE)

	DSE erforderlich wegen Datenübertragung	DSE ist generell verfügbar/ verlinkt	In deutscher Sprache verfügbar	Unterschied iOS- und Android	Stand der abgerufenen DSE[a]
Apple	ja	ja	ja	nein	31.05.16
A-Rival	nein	–	–	–	–
Fitbit	ja	ja	ja	ja	09.12.14 (iOS) 06.01.12 (andr)
Garmin	ja	ja	ja	nein	11.01.16
Jawbone	ja	ja	ja	nein	16.12.14
MyFitnessPal	ja	ja	ja	nein	22.01.16
Polar	ja	ja	ja	nein	01.10.13
Runtastic	ja	ja	ja	nein	16.09.15
Samsung	ja	ja	ja	nein	k. A.
Striiv	ja	ja	nein	nein	29.08.11
Technaxx	nein	–	–	–	–
Withings	ja	ja	nein	nein	26.04.15
Xiaomi	ja	ja	nein	nein	06.05.16

a Abgerufen am 05. September 2016

Anwendbarkeit deutschen Datenschutzrechts. Bezüglich der rechtlichen Einordnung stellt sich zunächst die Frage, inwieweit das BDSG bei der Überprüfung von Datenschutzerklärungen anwendbar ist. Das BDSG findet nicht ausschließlich Anwendung auf Unternehmen mit Sitz in Deutschland. Auch ausländische Unternehmen, insbesondere mit Sitz im Nicht-EU-Ausland, die auf dem deutschen Markt tätig sind, können dem deutschen Datenschutzrecht unterliegen.

Entscheidend ist nach § 1 Abs. 5 BDSG, ob die Daten im Inland, also in Deutschland *erhoben* werden. Wann jedoch die Datenerhebung im Inland erfolgt, ist in Bezug auf die *Datenerhebung per Distanz*, wie sie auch bei einer App-Nutzung vorliegt, umstritten. Alleine das Bereitstellen von Angeboten zum Abruf oder zur Anmeldung im Ausland begründet laut herrschender Meinung[96] keinen hinreichenden Inlandsbezug.[97] Allerdings kann ein Inlandsbezug entstehen, wenn der ausländische Anbieter sich auf den PC des inländischen Nutzers Zugriff verschafft, etwa mit Hilfe von Cookies, Viren oder Trojanern.[98] Erst recht liegt nach in dieser Untersuchung vertretener Auffassung dann ein Inlandsbezug vor, wenn durch die App auf das Smartphone zugegriffen wird: Wenn bereits der Zugriff auf den Computer des Nutzers durch das Setzen von Cookies eine Datenerhebung in Deutschland darstellt, so gilt dies erst recht für eine auf dem Smartphone des Nutzers installierte App, die darüber hinaus umfangreiche Zugriffsrechte fordern kann. Ein Smartphone ist funktional und technisch gesehen ein Computer, die darauf installierte App erhebt im Inland Nutzerdaten und überträgt diese in vollautomatisierter Weise in Länder außerhalb der EU. Entsprechend ist deutsches Recht nach Auffassung der Verbraucherzentrale Nordrhein-Westfalen anwendbar, sofern eine Software wie eine App installiert wird,

96 Gusy, 2016, BDSG § 1 Rn. 112-116.

97 Nach anderer Ansicht reicht bereits eine Ausrichtung auf den deutschen Markt bzw. die Nutzung durch deutsche Verbraucher; Weichert, 2009, S. 323.

98 Gusy, 2016, BDSG § 1 Rn. 113; Jandt, 2008, S. 664; siehe auch KG Berlin, Urteil vom 24.01.2014, 5 U 42/12, S. 26.

die eigenständig Daten erfasst und in Länder außerhalb der EU übermittelt.

Eine Ausnahme ist jedoch für Unternehmen vorgesehen, die ihre Niederlassung in Europa haben, für die das BDSG eine Privilegierung vorsieht: Nach § 1 Abs. 5, S. 1 BDSG findet das BDSG keine Anwendung, wenn die letztendlich entscheidungsbefugte datenverarbeitende Stelle des Unternehmens ihre Niederlassung innerhalb der EU hat. Unternehmen, die in einem Mitgliedsstaat der EU tätig sind, sollen nicht mit allen nationalen Regelungen der Mitgliedsländer konfrontiert werden, sondern im Sinne eines einheitlichen Rechts- und Wirtschaftsraums nur mit den Gesetzen des Mitgliedsstaates. Somit ist das BDSG bei zwei der geprüften Anbieter, *Polar* und *Runtastic*, nicht anwendbar, da deren Sitz in Finnland beziehungsweise Österreich liegt. Dennoch wurden für eine bessere Vergleichbarkeit der Anbieter im Rahmen der vorliegenden Prüfung die Wertungen des BDSG zu Grunde gelegt, auch wenn sich hieraus ergebende Rechtsverstöße für diese Anbieter unter Umständen nicht verfolgbar sind.

Zentrale Vorgaben des BDSG/TMG. Die Datenschutzerklärungen müssen gemäß § 4 Abs. 3 BDSG, § 13 Abs. 1 TMG Informationen dazu beinhalten, welche Art von Daten, zu welchem Zweck erhoben werden und wie sie verarbeitet oder genutzt werden (z. B. auch, an wen sie weitergeleitet werden). Neben der Prüfung der Datenschutzerklärungen wurde auch begutachtet, ob eine explizite Einwilligung in die Datenerhebung, -speicherung und -verarbeitung notwendig ist und ob diese eingeholt wird.

Das Erheben oder Verwenden personenbezogener Daten ist gemäß § 4 Abs. 1 BDSG nämlich nur zulässig, wenn das Gesetz dies gestattet oder der Betroffene eingewilligt hat (vgl. auch § 12 Abs. 1 TMG für Bestands- und Nutzungsdaten). Besondere Bedeutung hat hierbei § 28 Abs. 1 Nr. 1 BDSG. Hiernach ist das Erheben und Verwenden von persönlichen Daten gesetzlich gestattet, sofern es für die Dienstleistung *erforderlich* ist.

Je nach Funktionalität der App liegt beispielsweise die Erforderlichkeit der Erhebung und Verwendung von (personenbezogenen) Daten wie Größe, Gewicht, Alter oder Geschlecht bei der Wearable-Nutzung nahe, um die Messergebnisse des Wearables mit diesen individuellen Parametern in Relation setzen zu können. Auch das Speichern von Standortdaten kann erforderlich sein, wenn der Nutzer beispielsweise seine Laufroute mit Hilfe der App nachverfolgen will.

Hinsichtlich zweier Aspekte lässt sich die Datenverarbeitung allerdings nicht alleine mit der gesetzlichen Gestattung aus § 28 Abs. 1 Nr.1 BDSG begründen.[99]

Erstens betrifft dies die *Erhebung und Verarbeitung von Gesundheitsdaten*. Hierfür stellt § 28 Abs. 6 BDSG eine Spezialnorm gegenüber § 28 Abs. 1 Nr. 1 BDSG dar, die wesentlich höhere Anforderungen an die Datenerhebung und -nutzung stellt (Abschnitt 3.1.1). Zweitens gilt dies für die *Datenübertragung ins Nicht-EU-Ausland* mit den in §§ 4b ff. BDSG definierten Spezialnormen, das heißt Länder, die keine Mitglieder der Europäischen Union sind (Abschnitt 3.1.2).

Auf diese Aspekte wurde im Rahmen der rechtlichen Prüfung daher ein besonderer Fokus gelegt. Darüber hinaus wurden weitere sich häufende rechtswidrige Bestimmungen dokumentiert (Abschnitt 3.1.3). Dies betrifft insbesondere Regelungen zur Datenweitergabe bei Fusion oder Übernahme sowie die Informationspflicht bei einer Aktualisierung der Datenschutzerklärung.

3.1.1 Erhebung und Verarbeitung von Gesundheitsdaten

Das BDSG, ebenso wie die EG-Datenschutzrichtlinie (Art. 8),[100] verschärft bei bestimmten Daten die Verarbeitungsvoraussetzungen. Dies ist ihrer besonderen Art und der damit verbundenen erhöhten Gefährdung der Betroffenen geschuldet.

Gesundheitsdaten sind nach § 3 Abs. 9 BDSG besondere Arten personenbezogener Daten. Sie werden auch als sensible Daten bezeichnet. „Sensibel“ sind alle Angaben, die direkt oder indirekt Informationen zu den in § 3 Abs. 9 BDSG angegebenen Datenkategorien vermitteln, hierzu zählen auch Gesundheitsdaten.[101]

99 Eine gesetzliche Gestattung nach § 28 Abs.1 Nr.2 BDSG ist vorliegend nicht einschlägig, da aufgrund der Verwendung sensibler Daten das Interesse des Betroffenen überwiegt.

100 RL 95/46/ EG.

101 Gola & Schomerus, 2015 BDSG § 3 Rn. 56-57c 12.

Gesundheitsdaten beinhalten zum einen unmittelbare Informationen zur Gesundheit einer Person, wie beispielsweise Krankheitsdiagnosen, Behinderungen oder Alkohol- beziehungsweise Drogenmissbrauch. Für einen möglichst wirksamen Schutz der Betroffenen reicht es zum anderen jedoch nicht, lediglich Daten einzubeziehen, die beispielsweise unmittelbar eine Krankheit betreffen.[102] Entsprechend lassen auch Daten, die den körperlichen Zustand im Allgemeinen betreffen, Rückschlüsse auf den Gesundheitszustand zu (sog. mittelbare Gesundheitsdaten). Um einen effektiven Schutz zu gewährleisten, resultiert hieraus, dass auch mittelbare Gesundheitsdaten von § 3 Abs. 9 BDSG umfasst sind.[103]

Aus mittelbaren Gesundheitsdaten können vor allem Rückschlüsse auf den Gesundheitszustand der betroffenen Person gezogen werden, wenn diese über eine bloße Momentaufnahme hinausgehen. Dies schließt Daten über vitale Funktionen wie Herzfrequenz und Daten zum Schlafverhalten des Betroffenen ein, wie sie mit nur einer Ausnahme (*Apple*[104]) von allen Anbietern verarbeitet werden (vgl. Technische Prüfung, Tabelle 7).

Werden derlei Daten über einen längeren Zeitraum hinweg gespeichert und/oder mit weiteren Daten kombiniert, sind Rückschlüsse auf den Gesundheitszustand des Betroffenen möglich. So könnte ein als Schlafstörung interpretierbares Schlafverhalten zu einer (Wahrscheinlichkeits-) Aussage über aktuelle oder zukünftige Herz-Kreislauferkrankungen führen, da diese aus medizinischer Sicht mit Schlafstörungen zusammenhängen können.[105]

Aus der Voraussetzung nach § 4 Abs. 3 BDSG, eine genaue Zweckbestimmung vorzunehmen, ergibt sich: Speichert der Anbieter auch gesundheitsbezogene Daten, so muss dies auch aus der Datenschutzerklärung hervorgehen.[106] Hierbei muss der Anbieter konkret diejenigen Daten benennen, die er erhebt. Diese Unterrichtungspflicht über die Art der Daten ergibt sich für Nutzungs- und Bestanddaten auch aus § 13 Abs. 1 TMG.

Die rechtliche Prüfung der Datenschutzerklärungen ergab, dass alle relevanten Datenschutzerklärungen (*Fitbit*: *iOS* und *Android, Garmin, Jawbone, MyFitnessPal*[107], *Polar, Runtastic, Samsung*) zumindest (nicht abschließende) Beispiele für diejenigen Gesundheitsdaten angeben, die sie auch verarbeiten. So deklariert *Garmin* beispielsweise:

> *„Auf einigen Garmin-Websites und in einigen mobilen Apps […] können Sie […] Aktivitätsdaten (beispielsweise Schrittanzahl, Position, Distanz, Pace, Aktivitätszeit, Kalorienverbrauch, Herzfrequenz und Schlafdaten) vom Garmin-Gerät hochladen."*

Mit *Samsung* und *Jawbone* geben nur zwei Anbieter über die bloße Nennung der erhobenen Daten hinaus auch Hinweise auf deren potenziell weitreichende Bedeutung. So fügt *Samsung* der Benennung konkreter erhobener Gesundheitsdaten hinzu:

> *„Bitte beachten Sie, dass sich aus derartigen gesundheitsbezogenen Daten Rückschlüsse über Ihren Gesundheitszustand gewinnen lassen und dass es sich daher um sensible persönliche Daten handeln kann."*

Unabhängig von der Informationspflicht, denen der Anbieter in seiner Datenschutzerklärung nachkommt, gelten für besondere Arten personenbezogener Daten wie Gesundheitsdaten nach § 3 Abs. 9 BDSG besondere Anforderungen hinsichtlich der *Zulässigkeit der Verarbeitung:* Die Erhebung, Verarbeitung oder Nutzung von sensiblen Daten ist nur zulässig, wenn der Betroffene darin eingewilligt hat oder das Gesetz dies gestattet.

Eine gesetzliche Gestattung liegt jedoch im Falle der Smartwatches und Fitnesstracker in der Regel nicht vor. Maßgeblich ist nach unserer Auffassung § 28 Abs. 6 BDSG.[108] Wird das Wearable mit der dazugehörigen App nicht aus medizinischen Gründen genutzt, ist eine Gesundheitsdatenerhebung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten nicht erforderlich (Nr. 1).[109] Ebenso wenig handelt es sich um

102 Simitis, 2014, BDSG § 3 Rn. 263.
103 Simitis, 2014, BDSG § 3 Rn. 263 f.
104 Ob Gesundheitsdaten an Apple übertragen werden, konnte technisch nicht analysiert werden, daher wurde hier auf eine rechtliche Einordnung verzichtet; *A-Rival* und *Technaxx* entfallen (Tabelle 7).
105 Laugsand, Strand, Platou, Vatten, & Janszky, 2014.
106 BeckOK DatenSR/Bäcker, BDSG, 2017, § 4 Rn. 58.
107 Ausführungen im aufklappbaren Text.
108 Teilweise wird vertreten, dass die Verwendung von patientenbezogenen Gesundheitsdaten unter § 28 Abs. 1 BDSG fällt, da Ärzte vollumfängliche Berechtigungen zur Erfüllung Ihrer Behandlungspflicht benötigen. Abgestellt wird auf die Wertung des § 28 Abs. 7 BDSG, da der Arzt Geheimnisträger ist. (vgl. Simitis § 28 Rn. 81).
109 Die Nummerierungen beziehen sich auf die Ausnahmetatbestände des § 28 Abs. 6 Nr. 1-4 BDSG.

Daten, die der Betroffene offenkundig öffentlich gemacht hat (Nr. 2). Auch die weiteren Ausnahmen sind in der Regel nicht einschlägig: Die Daten sind weder erforderlich zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche (Nr. 3)[110] noch für die wissenschaftliche Forschung (Nr. 4). Letztlich handelt es sich auch nicht um eine ärztlich betriebene Gesundheitsvorsorge im Sinne des § 28 Abs. 7 BDSG.

Demnach müssen Wearable-Anbieter eine Einwilligung für die Erhebung und Nutzung von Gesundheitsdaten einholen. Unabhängig von der Frage, ob eine Zustimmung zur Datenschutzerklärung eine solche Einwilligung darstellen kann, muss die Einwilligung den Anforderungen von § 4a BDSG genügen. Sie muss auf der freien Entscheidung des Betroffenen beruhen und sich ausdrücklich auf die besonderen Arten der erhobenen und genutzten personenbezogenen Daten beziehen (§ 4 a Abs. 3 BDSG). Werden also beispielsweise Pulsdaten des Betroffenen erhoben, so muss sich die Einwilligung explizit auf diese beziehen und es muss erklärt werden, wie und warum die Daten über den Pulsschlag gespeichert werden müssen. Der Betroffene muss zweifelsfrei erkennen können, welche sensiblen Daten, für welchen genau umschriebenen Verwendungszweck, in welchem Verwendungskontext erhoben, verarbeitet und genutzt werden sollen.[111]

Die rechtliche Prüfung zeigt jedoch: Kaum einer der Anbieter, die Gesundheitsdaten verarbeiten, holt für die Verarbeitung dieser sensiblen personenbezogenen Daten eine separate Einwilligung innerhalb des Installationsprozesses der App ein (Tabelle 11). Nur bei dem Anbieter *MyFitnessPal* werden im Rahmen der Zustimmung zur Datenschutzerklärung und den Nutzungsbedingungen die Gesundheitsdaten ausdrücklich genannt.

3.1.2 Datenübertragung ins Nicht-EU-Ausland

Zur Informationspflicht des Anbieters im Rahmen der Datenschutzerklärungen zählt, den Nutzer darüber aufzuklären, *wo* seine personenbezogenen Daten verarbeitet werden.

So wird von den Anbietern auf die Datenübertragung nach Südkorea (*Samsung*) und die Vereinigten Staaten (*Apple, Fitbit iOS, Fitbit Android, Garmin, Jawbone, MyFitnessPal*) hingewiesen.[112] Eine Datenübermittlung ins Nicht-EU-Ausland ist jedoch nur dann zulässig, wenn eine Ausnahmeregelung für die Datenübermittlung einschlägig ist oder wenn das Datenschutzniveau im Zielland angemessen im Sinne des § 4 b Abs. 2 S. 2 BDSG ist, also europäischen Standards gerecht wird.

Eine der gesetzlichen Ausnahmeregelungen des § 4 c Abs. 1 S. 1 Nr. 4 bis 6 BDSG liegt nicht vor: Die Datenübermittlung ist weder erforderlich zur Wahrung eines wichtigen öffentlichen Interesses, noch ist die Datenübermittlung erforderlich für die Wahrung lebenswichtiger Interessen des Betroffenen. Auch erfolgt die Datenübermittlung nicht aus einem Register, das zur Information der Öffentlichkeit bestimmt ist.

Dementsprechend muss das Datenschutzniveau in dem Empfängerland angemessen sein im Sinne des § 4 b Abs. 2 S. 2 BDSG, also europäischen Standards entsprechen. Dies kann durch zusätzlich ergriffene Maßnahmen gesichert werden, die dem Nutzer entsprechend zu erläutern sind.[113] Beispielhaft genannt seien hier die EU-Standard Vertragsklauseln, die sogenannten „Binding Corporate Rules“, sowie der neue Privacy Shield, der seit Juli 2016 implementiert werden kann.[114] Der Privacy Shield ist ein Ersatz für die zwischen der Europäischen Union und den Vereinigten Staaten von Amerika im Jahre 2000 getroffene Safe-Harbor-Vereinbarung (dt.: sicherer Hafen). Diese gewährleistete, dass personenbezogene Daten legal in die USA übermittelt werden können. Der EuGH hat jedoch die Safe-Harbor-Entscheidung der Europäischen Kommission durch sein Urteil vom 6. Oktober 2015 aufgehoben.[115] Seitdem ist jegliche weitere auf dieser Regelung beruhende Datenübertragung rechtswidrig.

Die rechtliche Prüfung der Datenschutzerklärungen zeigt, dass nur einer (*MyFitnessPal*) der sechs hier relevanten Anbieter (*Apple, Fitbit, Garmin, Jawbone, MyFitnessPal, Samsung*) eine korrekte Bestimmung bezüg-

110 Teilweise wird angenommen, dass nach sensiblen Daten gefragt werden darf, wenn es für das Vertragsverhältnis zwingend geboten ist, so zum Beispiel im Arbeitgeber-Arbeitnehmer-Verhältnis, vgl. Simitis § 28 Rn. 306.

111 Roßnagel, 2013, Kap. 4.8, Rn. 56; Simitis, BDSG § 4a, 2014, Rn. 87.

112 Polar macht hierbei die Angabe, Daten nach Finnland oder in nicht weiter spezifizierte Länder zu übertragen.

113 Gola & Schomerus, 2015, BDSG § 4b, Rn. 17.

114 LDI Nordrhein-Westfalen, 2016.

115 EuGH Urteil vom 06.10.2015, C-263-14.

11 INFORMATION UND EINWILLIGUNG

Anbieter	Stand der abgerufenen DSE	Erhebung und Verarbeitung von Gesundheitsdaten		Datenübertragung ins Nicht-EU-Ausland		Weitere Auffälligkeiten	
		Unterrichtung	Separate Einwilligung während Installation[c]	Unterrichtung	Separate Einwilligung während Installation[c]	Vorbehalt bei Über-nahme/ Fusion	Benachrichtigen aktiv über Aktualisierung der DSE
Apple	31.05.16	–	–	ja[e]	nein	ja	nein
Fitbit iOS	09.12.14	ja[d]	nein	ja[e]	ja	ja	nein[f]
Fitbit andr.	06.01.12	ja[d]	nein	ja[e]	ja	ja	nein
Garmin	11.01.16	ja[d]	nein	ja[e]	nein	ja	nein[f]
Jawbone	16.12.14	ja	nein	ja[e]	nein	ja	nein
MyFitnessPal	22.01.16	ja[d]	ja	ja	ja	ja	ja
Polar[a]	01.10.13	ja[d]	nein	k. A.	entfällt	nein	nein
Runtastic[a]	16.09.15	ja[d]	nein	k. A.	entfällt	nein	nein
Samsung	k. A.	ja	nein	ja[e]	nein	nein	ja
Striiv[b]	29.08.11	–	nein	–	nein	–	–
Xiaomi[b]	06.05.16	–	nein	–	nein	–	–
Withings[b]	26.04.15	–	nein	–	nein	–	–

a Das BDSG wurde aus Gründen der Vergleichbarkeit der Prüfung zu Grunde gelegt, ist aber für diesen Anbieter nicht anwendbar (s. Abschnitt 3.1).
b Datenschutzerklärung nicht in deutscher Sprache verfügbar, daher keine inhaltliche Prüfung.
c Kein diesbezüglicher Unterschied im Installationsprozess zwischen iOS- und Android-Versionen der Anbieter-Apps.
d aber: lediglich beispielhafte Aufzählung und ohne Hinweis auf die Besonderheit der Daten.
e aber: keine Risikoaufklärung und/oder keine gültige Regelung, die ein angemessenes Datenschutzniveau gewährleistet; Stand 05.09.2016.
f Intransparente Voraussetzung: Nur bei „wesentlichen" Änderungen bzw. nur gültig für nach der Aktualisierung erhobene Daten.

lich einer Übertragung von Daten ins Nicht-EU-Ausland formuliert (Tabelle 11).

Die Anbieter *Fitbit* (iOS und Android), *Apple* und *MyFitnessPal* beziehen sich in ihren Datenschutzerklärungen auf die für unwirksam erklärte Safe-Harbor-Vereinbarung. *MyFitnessPal* stützt sich jedoch zusätzlich auf EU-Modell-Vertragsklauseln. Der seit Juli 2016 ersatzweise heranzuziehende Privacy Shield wurde in keiner der relevanten Datenschutzerklärungen erwähnt. Bis auf *MyFitnessPal* und *Fitbit* holt keiner der entsprechenden Anbieter eine separate Einwilligung für die Datenübertragung in das Nicht-EU-Ausland ein (Tabelle 11). Allerdings unterrichtet *Fitbit* in den Datenschutzhinweisen, auf die im Rahmen der Einwilligung Bezug genommen wird, nicht ausreichend über diese Datenübertragung.

3.1.3 Weitere Auffälligkeiten in den Datenschutzerklärungen

Im Zuge der rechtlichen Prüfung fielen über die vorab definierten Prüfpunkte hinaus außerdem zwei weitere unserer Ansicht nach rechtswidrige Bestimmungen seitens der Anbieter auf. Diese betreffen Regelungen bei Fusion und Übernahme sowie die Aktualisierung der Datenschutzerklärungen. Die §§ 305 ff. BGB sind auf die nachfolgenden Bestimmungen anwendbar, denn die Datenschutzerklärungen werden standardmäßig gegenüber einer Vielzahl von Verbrauchern verwendet, haben einen regelnden Charakter und sind mithin als vorformulierte Klauseln einzustufen. Die folgenden verwendeten Bestimmungen enthalten diverse Regelungen, da sie unter anderem festlegen, welche perso-

nenbezogenen Daten des jeweiligen Nutzers künftig in welcher Art, welchem Ausmaß und zu welchem Zweck erhoben und verwendet werden sollen und darüber hinaus auch, an wen diese Daten weitervermittelt werden. Insoweit handelt es sich auch nicht um Leistungsbeschreibungen, die der Inhaltskontrolle gem. § 307 Abs. 3 BGB entzogen wären.

Fusion und Übernahme. Behält sich ein Anbieter vor, dass Drittparteien in irgendeiner Form und zu einem unbestimmten Zeitpunkt in die Rechte und Pflichten des Verwenders eintreten, so stellt das Gesetz Anforderungen an die Zulässigkeit solcher Regelungen. Sollen hierbei Daten auf Basis der Datenschutzerklärung bei einer Fusion oder einem teilweisen Unternehmensverkauf an eine Drittpartei weitergereicht werden, so muss der Drittanbieter namentlich benannt sein oder für den Nutzer eine Widerspruchsmöglichkeit gegeben sein. Denn der Verbraucher soll nur an den Vertragspartner gebunden sein, den er sich selbst ausgesucht hat. Ein Dritter weist unter Umständen nicht die Seriosität des ursprünglich gewählten Vertragspartners auf. Fünf Anbieter verwenden eine nach in dieser Untersuchung vertretener Auffassung unzulässige Bestimmung bezüglich etwaiger Fusionen (*Apple, Garmin, FitBit* unter *iOS* und *Android, Jawbone, MyFitnessPal*[116]; Tabelle 11). *Jawbone* deklariert beispielsweise:

> *„Wir können Ihre personenbezogenen Daten zum Zweck eines Geschäftsabschlusses (oder der Verhandlung eines Geschäftsabschlusses) weitergeben, der den Verkauf oder Transfer aller oder eines Teils unserer Geschäfte oder des Unternehmensvermögens beinhaltet. Dabei kann es sich zum Beispiel um eine Fusionierung, eine Kapitalbeschaffung, Übernahme oder ein Konkursverfahren handeln.“*

Die oben genannten Voraussetzungen werden hier nicht erfüllt: Weder ist im Sinne des § 309 Nr. 10a BGB der Dritte im Falle einer Fusion, Übernahme etc. genannt, noch wird dem Vertragspartner das Recht eingeräumt, sich vom Vertrag zu lösen (§ 309 Nr. 10b BGB). Darüber hinaus ist zumindest im Fall des Weiterverkaufs von Gesundheitsdaten eine entsprechende Einwilligung des Betroffenen erforderlich.

Aktualisierung der Datenschutzerklärung. Sinn und Zweck der Informationspflicht seitens des Anbieters ist es, den Betroffenen anhand der Datenschutzerklärung über den Umgang mit seinen Daten zu informieren. Sollten diese Informationen sich im Rahmen einer Aktualisierung ändern, muss sichergestellt sein, dass der Nutzer auch die aktualisierten Informationen erhält. Andernfalls könnten Anbieter ihre Informationspflicht umgehen, was Verbraucher in Unkenntnis über den tatsächlichen Umgang mit ihren Daten lassen würde. Entsprechend muss der Anbieter seine Nutzer in jedem Fall aktiv über Änderungen in der Datenschutzerklärung informieren (zum Beispiel per E-Mail).[117] Dies gebietet die Unterrichtungspflicht, die sich aus § 4 Abs. 3 BDSG beziehungsweise § 12, 13 TMG ergibt.

Darüber hinaus darf im Zuge der Aktualisierung der Vertragsgegenstand nicht ohne weiteres geändert werden. Dazu zählt beispielsweise der Zweck, zu dem Daten erhoben, gespeichert und genutzt werden. Handelt es sich um eine solche Zweckänderung, muss über die bloße Information zur Aktualisierung auch eine Einwilligung des Nutzers eingeholt werden.

Sechs Anbieter (*Apple, FitBit iOS* und *Android, Garmin, Jawbone, Polar, Runtastic*) binden eine Klausel mit ein, die dies nicht vorsieht und somit nicht sicherstellt, dass potentiell geänderte Bedingungen zur Kenntnis genommen werden (Tabelle 11). So deklariert *Fitbit* (*Android*) beispielsweise:

> *„Wir können diese Richtlinie gelegentlich aktualisieren. Das Datum der letzten Überarbeitung wird am Ende der Richtlinie angezeigt. Änderungen treten unmittelbar mit ihrer Veröffentlichung in Kraft.”*

Zunächst fällt an diesem Beispiel auf, dass diese Klausel für den Verbraucher intransparent ist. Weder wird die genaue Bedeutung von „gelegentlich“ erläutert, noch ergibt sich hieraus, in welchem Umfang Änderungen vorgenommen werden können.

Darüber hinaus ist eine schlichte Veröffentlichung der Aktualisierung auf der Homepage aus Sicht des Verbraucherschutzes nicht ausreichend, vor allem dann nicht, wenn hiermit inhaltliche Änderungen verbunden sind. Auch die Empfehlung, sich die Bedingungen von

116 Ausführungen im aufklappbaren Text.

117 S. auch § 308 Nr. 5 BGB.

Zeit zu Zeit erneut durchzulesen, wie etwa *Polar* sie gibt, entbindet den Wearable-Anbieter nicht von der Pflicht, dem Kunden in zumutbarer Weise die Möglichkeit einzuräumen, von dem Inhalt der neuen oder geänderten Bedingungen Kenntnis zu nehmen. Insoweit befindet sich der Verbraucher nicht in der „Holschuld".

Zwei Anbieter (*Garmin* und *Fitbit* unter iOS) geben an, Verbraucher zumindest bei erheblichen Änderungen informieren zu wollen. So schreibt *Garmin* beispielsweise:

> *„Sollte es sich um wesentliche Änderungen handeln, werden Sie von uns darüber informiert und, sofern dies nach anwendbarem Recht erforderlich ist, holen wir Ihre Zustimmung ein."*

Während hier außerdem vorgesehen ist, eine Zustimmung bei wesentlichen Änderungen einzuholen, wird der Verbraucher jedoch im Unklaren darüber gelassen, wann eine wesentliche Änderung vorliegt bzw. was eine solche ist. Dies wäre beispielsweise der Fall, wenn die Nutzerdaten zu einem anderen als dem vereinbarten Zweck verarbeitet würden.

Zwei Anbieter geben in Ihren Datenschutzerklärungen an, den Nutzer ordnungsgemäß über jegliche inhaltliche Änderung informieren zu wollen. Dies soll per Mail oder Bildschirmanzeige in der App geschehen. Verfahren wird so zum einen von der App von *MyFitnessPal* und zum anderen von *Samsung*. [118]

3.2 TEXTSCHWIERIGKEIT

Datenschutzerklärungen sollen in erster Linie Verbraucher über den Umgang mit ihren Daten informieren (s. Abschnitt 1.3.1), darin unterscheiden sie sich von reinen Vertragstexten. Nutzer können jedoch nur als tatsächlich informiert gelten, wenn sie die in den Datenschutzerklärungen bereitgestellten Hinweise lesen und auf Basis dessen auch verstehen können. Dies hängt mit Eigenschaften des Lesers einerseits und des gelesenen Texts andererseits zusammen.

In Bezug auf den Leser stellt sich beispielsweise die Frage, ob er die zeitlichen, kognitiven und motivationalen Ressourcen hat, um die zur Verfügung gestellten Informationen zu lesen, oder ob er geübt im Lesen langer und möglicherweise komplexer Texte ist.[119] Die Leserzielgruppe der geprüften Datenschutzerklärungen ist jedoch maximal heterogen, da prinzipiell jeder Verbraucher ein Wearable kaufen und mit der dazugehörigen App nutzen kann. Insofern können für das Erfassen der Datenschutzerklärungen keine spezifischen Eigenschaften in der Lesekompetenz des Verbrauchers angenommen werden. Der Text sollte insofern so verständlich wie möglich geschrieben sein.[120]

Ob ein Text verständlich ist, hängt von verschiedenen Faktoren ab. Beispielsweise spielen die inhaltliche Ordnung der Informationen, die Verwendung von Fachbegriffen und visuelle Elemente eine Rolle.[121] Entscheidend ist darüber hinaus, wie schwierig die im Text verwendete Sprache ist (Textschwierigkeit).[122] Dieser Aspekt wurde in der vorliegenden Untersuchung näher beleuchtet.

Methode. Wie bei der rechtlichen Einordnung wurden neun Datenschutzerklärungen von insgesamt acht Anbietern geprüft (Tabelle 10).[123] Um die Schwierigkeit der Texte unabhängig von gestalterischen Merkmalen zu untersuchen, wurden die Datenschutzerklärungen hinsichtlich verschiedener sprachlicher Eigenschaften analysiert.[124] Zur Durchführung der automatisierten Analyse[125] wurden vorab Formatierungen, Über- und Unterüberschriften, Sonderzeichen, mehrstellige Zahlen, Bindestriche und Hyperlinks aus den zu analysierenden Dokumenten entfernt.

Zunächst wurde die durchschnittliche Wort- und Satzlänge erfasst: Längere Texte, bestehend aus längeren Wörtern und Sätzen deuten hierbei auf größere Herausforderungen für den Leser hin als kürzere Texte mit weniger komplexen Wort- und Satzkonstruktionen. Um eine erste Einschätzung der Textschwierigkeit zu ermitteln, wurde der Flesch-Lesbarkeitsindex *(Flesch-Index)* für jede der Datenschutzerklärungen berechnet.

118 Soweit bei der Installation der Smartwatch/Fitnesstracker ein Konto eröffnet wurde.

119 Christmann, 2004.

120 Z. B. Sachverständigenrat für Verbraucherfragen, 2016 (Empfehlung Nr. 2); s. auch Art. 12 EU DS-GVO.

121 Christmann, 2004.

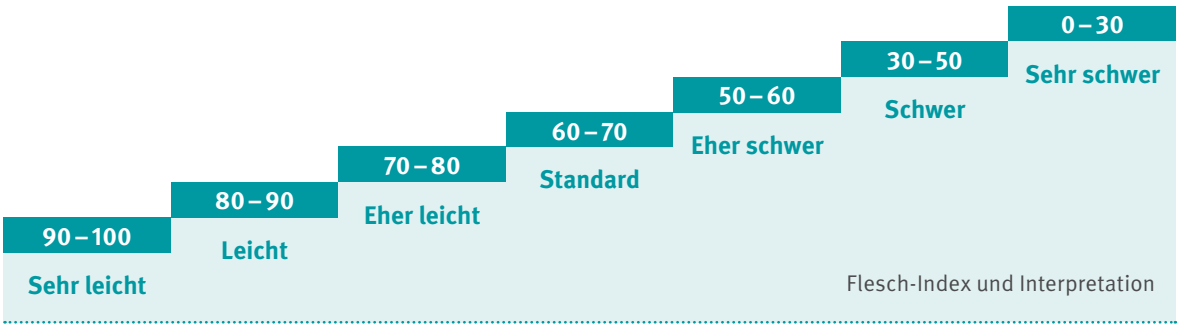
122 Hancke, Vajjala, & Meurers, 2012.

123 Die Datenschutzerklärung von *MyFitnessPal* stellte ergänzende Informationen in aufklappbaren Texten bereit. Diese waren nicht Bestandteil der vorliegenden Textanalyse.

124 Hancke, Vajjala, & Meurers, 2012.

125 Die Analyse wurde mit Hilfe des R-Pakets koRpus durchgeführt; Michalke, 2012.

12 INTERPRETATION VON FLESCH-INDICES[a]



a Angepasst übernommen von Lucassen, Dijkstra, & Schraagen, 2012, S. 2.

Der Flesch-Index berücksichtigt die durchschnittliche Anzahl an Wörtern pro Satz, sowie die durchschnittliche Anzahl an Silben pro Wort.[126] Das Resultat ist ein Wert zwischen eins und hundert, wobei höhere Werte auf eine einfachere Sprache hindeuten (Tabelle 12). Lesbarkeitsindices dieser Art können keine endgültige Aussage über die Schwierigkeit eines Textes geben. Allerdings werden sie in vielen wissenschaftlichen Studien als Indikator für die Einfachheit von Texten hinzugezogen,[127] insbesondere wenn diese Texte in erster Linie Laien beziehungsweise Fachfremde informieren und aufklären sollen.[128] Die Schwierigkeit des konkret verwendeten Vokabulars kann mit dieser Methode nicht erfasst werden.

Ergebnisse. Die analysierten Angaben zum Datenschutz unterscheiden sich deutlich in ihrer Länge (Minimum: 842, Maximum: 3408 Wörter). Die längste Datenschutzerklärung (*Fitbit* unter iOS) erstreckt sich über etwa fünf Din A4 Seiten reinen Text.[129] Entsprechend unterschiedlich ist auch die Dauer, die Verbraucher theoretisch aufbringen müssten, um die Texte zu lesen (Tabelle 13). Über alle neun Datenschutzerklärungen hinweg bräuchte ein durchschnittlich geübter Leser im Mittel acht Minuten (SD[130] = 4.02), um eine der Datenschutzerklärungen zu lesen.[131]

Unabhängig von der Länge der Texte gibt es verschiedene Indikatoren für eine relativ hohe Textschwierigkeit der Datenschutzerklärungen. Neben den oft langen Satzkonstruktionen (Maximum: 84 Wörter bei *Jawbone*) drückt sich dies in den ermittelten Lesbarkeitsindices aus: Alle Flesch-Indices befinden sich in einem Bereich, der als „schwer“ oder „sehr schwer“ zu bewerten ist (Tabelle 13).

3.3 ZWISCHENFAZIT: INFORMATION UND EINWILLIGUNG

Durch die Analyse der Datenschutzerklärungen wurde geprüft, ob Anbieter, soweit erforderlich, eine Einwilligung für den Umgang mit personenbezogenen Nutzerdaten einholen, inwieweit sie ihre Nutzer hinreichend über diesen Umgang informieren und ob die Datenschutzerklärungen darüber hinaus auch für Laien verständlich geschrieben sind.

126 Angepasste Formel für die deutsche Sprache: 180 - ASL - (58.5*ASW), ASL = durchschnittliche Anzahl an Wörtern pro Satz und ASW = durchschnittliche Anzahl an Silben pro Wort. Amstad, 1978.
127 Für einen Überblick: DuBay, 2004.
128 Howes, Julian, Kelty, Kemp, & Kirkbride, 2014a; Luers, Gostian, Roth, & Beutner, 2013; Tian, Champlin, Mackert, Lazard, & Agrawal, 2016; Wilson, 2009.
129 Schrift: Arial 10, einfacher Zeilenabstand.
130 Abkürzung für Standardabweichung. Die Standardabweichung ist ein statistisches Maß zur Kennzeichnung der Variabilität einer Verteilung; Bortz, 2005, S. 41.
131 Angenommen wurde eine Lesegeschwindigkeit von ca. 250 Wörtern pro Minute, s. z. B. Musch & Rösler, 2011; McDonald & Cranor, 2008, S. 10.

13 ÜBERSICHT AUSGEWÄHLTER EIGENSCHAFTEN DER ANALYSIERTEN TEXTE

Datenschutz-erklärung von	Wort-anzahl	Satz-anzahl	Wort-länge[a]	Satz-länge[b]	Längster Satz	Flesch-Index[c]	Schwie-rigkeit (Flesch)	Lese-dauer in min
Apple	3101	132	6,5	23,5	55	25,5	Sehr schwer	12,4
Fitbit (andr.)	2309	121	6,7	19,1	49	29,6	Sehr schwer	9,2
Fitbit (iOS)	3408	199	6,2	17,1	61	39,5	Schwer	13,6
Garmin	3008	112	6,5	26,2	80	22,4	Sehr schwer	12,0
Jawbone	1308	60	6,0	21,8	84	35,1	Schwer	5,2
MyFitnessPal[d]	2051	135	6,5	15,2	64	35,0	Schwer	8,2
Polar	2217	83	6,6	26,7	99	21,4	Sehr schwer	8,9
Runtastic	1324	75	6,6	17,7	53	32,4	Schwer	5,3
Samsung	842	43	6,9	19,6	52	24,4	Sehr schwer	3,4

a Durchschnittliche Buchstabenanzahl pro Wort.
b Durchschnittliche Wortanzahl pro Satz.
c Angepasste Formel nach Amstad (1978).
d Ohne ausklappbare Texte.

? Forschungsfrage 4: Wird eine wirksame Einwilligung für die Erhebung, Speicherung und Übertragung personenbezogener Daten eingeholt?

Überprüft wurde, ob im Zuge der App-Installation eine separate Einwilligung für die Verarbeitung personenbezogener Daten eingeholt wird. Der Fokus lag hierbei auf der Verarbeitung von Gesundheitsdaten und der Übertragung von Daten ins Nicht-EU-Ausland (s. Abschnitt 3.1.1 und 3.1.2). Im Ergebnis werden nur bei dem Anbieter *MyFitnessPal* im Rahmen der Zustimmung zu den Nutzungsbedingungen und der Datenschutzerklärung die Gesundheitsdaten ausdrücklich genannt. Zwei Anbieter (*Fitbit* und *MyFitnessPal*) erwähnen im Rahmen dieser Zustimmung außerdem die Übertragung von Daten ins Nicht-EU-Ausland.

? Forschungsfrage 5: Wird der Nutzer hinreichend über den Umgang mit seinen personenbezogenen Daten unterrichtet?

Die rechtliche Prüfung der Datenschutzerklärungen zeigt, dass diese in allen geprüften Fällen Mängel aufweisen: Drei von dreizehn Anbietern stellen keine Datenschutzerklärung in deutscher Sprache bereit. Die Aufklärung über den Umgang mit Gesundheitsdaten durch die Anbieter ist nicht zufriedenstellend: Sieben der neun geprüften Datenschutzerklärungen zählen erhobene Gesundheitsdaten lediglich auf, ohne jedoch auf die Besonderheit dieser Daten einzugehen. Darüber hinaus informiert nur einer der relevanten Anbieter ausreichend über die Übertragung von Daten ins Nicht-EU-Ausland. Kritisch ist auch, dass mehreren Datenschutzerklärungen zufolge Änderungen jederzeit ohne aktive Information des Nutzers implementiert werden können.

? Forschungsfrage 6: Ist die Datenschutzerklärung für Laien verständlich?

Die Analyse ausgewählter sprachlicher Eigenschaften der neun Datenschutzerklärungen weist auf deren ausgeprägte Textschwierigkeit hin. Entsprechend stellt das Verstehen einer Datenschutzerklärung hohe Anforderungen an die Lesekompetenz des Nutzers.[132]

132 Diese Einordnung deckt sich beispielsweise mit Untersuchungsergeb-

Einerseits entspricht dieses Ergebnis beobachtbaren Konventionen der Gestaltung von Nutzungsbedingungen und Datenschutzerklärungen.[133] Hierbei muss berücksichtigt werden, dass Datenschutzerklärungen einen komplexen Sachverhalt einfach darstellen sollen, sodass ihre Gestaltung notwendigerweise ein Kompromiss aus inhaltlicher Genauigkeit und Lesbarkeit ist.[134] Gleichzeitig sind die Daten, die im Zuge der Nutzung von Wearables und Fitness-Apps verarbeitet werden, teilweise besonders sensibel. Insofern ist es von noch größerer Relevanz, dass Nutzer auch verstehen, wie mit ihren Daten umgegangen wird. Aus Verbraucherschutzperspektive sind Anbieter daher insbesondere in diesem Kontext in der Pflicht, sich um eine einfache Sprache zu bemühen.

nissen norwegischer Verbraucherschützer, s. Myrstad, 2016, S. 8.

133 Z. B. Stiftung-Warentest, 2016a; McDonald & Cranor, 2008; s. auch Dachwitz, 2016.

134 BMJV, 2008, Teil B.

4. VERBRAUCHERBEFRAGUNG

Die Verbraucherbefragung erfasst die Perspektive von Verbrauchern auf ausgewählte datenschutzrelevante Aspekte bei der Nutzung von Wearables und Fitness-Apps. Untersucht wurde insbesondere wie sie mögliche Folgen der Nutzung von Wearables und Fitness-Apps bewerten (Forschungsfrage 7) und ob Wearable-Nutzer sich von Nicht-Nutzern hinsichtlich ihrer allgemeinen Datenschutzbedenken unterscheiden (Forschungsfrage 8).

4.1 METHODE

Befragt wurde eine repräsentative Stichprobe (n = 1055)[135] deutschsprachiger Internetnutzer (Mindestalter 14 Jahre). Die Teilnehmer wurden über das Telefonstichproben-System des Arbeitskreises Deutscher Markt- und Sozialforschungsinstitute (ADM e.V.) zufällig ausgewählt (mehrfach geschichtete Stichprobe).[136] Die Befragung wurde zwischen dem 25. August und 29. September 2016 von *mindline media GmbH*[137] durchgeführt.

Die Teilnehmer wurden mittels computergestützter Telefoninterviews (CATI) anhand eines strukturierten Fragebogens befragt:[138] Nach einer kurzen Einführung wurden den Teilnehmern Fragen zu ihrer Wearable-Nutzung gestellt. Anschließend beantworteten sie Fragen zu ihren generellen Datenschutzbedenken im Kontext von Online-Anwendungen.[139] Daraufhin wurden die Teilnehmer gebeten, die Eintrittswahrscheinlichkeit von insgesamt sieben Situationen einzuschätzen, die mögliche Folgen der Nutzung von Wearables und Fitness-Apps beschrieben.[140] Die Situationen wurden entweder auf Basis bekannt gewordener Präzedenzfälle formuliert, bei denen Wearable- und Fitness-App-Daten von Dritten genutzt wurden (z. B.: Nutzung der Daten zu Beweiszwecken in Gerichtsverfahren)[141] oder in Anlehnung an gesellschaftliche Szenarien beschrieben, die sich aus Sicht des Verbraucherschutzes kurz- oder langfristig ergeben können (z. B.: Nutzung von Fitness-Daten durch Krankenkassen und Arbeitgeber; s. Abschnitt 1.2).

Dieselben Situationen wurden den Teilnehmern erneut präsentiert: Gefragt wurde nun jeweils, ob sie es *in Ordnung* fänden, wenn ihre Daten auf diese Art und Weise verwendet würden.[142]

4.2 NUTZUNG VON WEARABLES

Die Befragungsergebnisse zeigen, dass aktuell fünf Prozent der deutschen Internetnutzer ein Wearable nutzen (Abbildung 14), wobei es eine Präferenz für Fitness-Armbänder (58 % der Wearable-Nutzer) und Smartwatches (37 %) gibt. Weitere 15 Prozent der Befragten halten es für wahrscheinlich, künftig ein Wearable zu nutzen.

Wearables und Fitness-Apps werden verstärkt von jüngeren Verbrauchern genutzt (Abbildung 15). So nutzen doppelt so viele Verbraucher im Alter zwischen 14 und 29 Jahren ein Wearable (6 %) als in der Gruppe der über 50-Jährigen (3 %). Dieser Alterseffekt zeigt sich auch in Bezug auf die Nutzer von Fitness-Apps (insgesamt 12 % aller Befragten), die, ohne dazugehöriges Wearable, von 19 Prozent der 14 bis 29-Jährigen, aber nur von sechs Prozent der über 50-Jährigen genutzt werden.

Wearables werden insbesondere zur Überwachung sportlicher Aktivitäten (86 %) und zur Kontrolle von Blutdruck oder Puls (51 %) genutzt. Außerdem verwen-

135 Inkl. Boost (n =100) für Wearable-Nutzer; für die Auswertung wurde die Anzahl der Wearable-Nutzer rückgewichtet, sodass die Repräsentativität der Stichprobe erhalten bleibt; Fehlertoleranz (Gesamtstichprobe): Maximal +/- 3,0 Prozentpunkte (bei einem Anteilswert von 50 Prozent).

136 S. auch https://www.adm-ev.de/telefonbefragungen; Auswahl per Dual Frame-Ansatz (Kombination von Festnetz- und Mobilfunkstichprobe im Verhältnis von 70 Prozent Festnetz-Nummern zu 30 Prozent Mobilnetz-Nummern). Die Ergebnisse der Untersuchung wurden nach Alter, Geschlecht, Bildungsgrad und Wearable-Nutzung gewichtet, sodass sie repräsentativ für Internetnutzer (ab 14 Jahren) in Deutschland sind; zusätzliche Designgewichtung (Transformation) zur Korrektur unterschiedlicher Auswahlchancen in den Sampling Frames.

137 www.mindline-media.de

138 Der Fragebogen ist abrufbar unter http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps

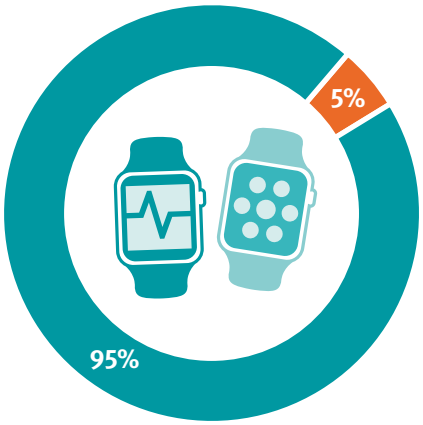
139 Hierzu wurden zehn Items der Fragebogenbatterie von Hong & Thong (2013) aus dem Englischen übersetzt und auf verständliche Formulierungen hin angepasst. Die Fragebogenbatterie erfasst Online-Privatheitssorgen als mehrdimensionales Konstrukt und bezieht einen großen Teil der in diesem Kontext existierenden Literatur für die Itemkonstruktion mit ein. Antwortformat: 4-Likert-Skala; stimme gar nicht zu – stimme weniger zu – stimme weitgehend zu – stimme voll und ganz zu.

140 Antwortformat: 4-Likert-Skala; sehr unwahrscheinlich – eher unwahrscheinlich – eher wahrscheinlich – sehr wahrscheinlich.

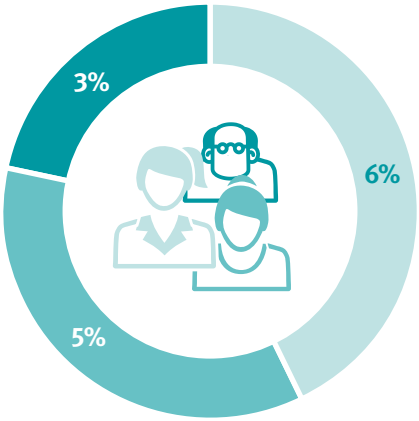
141 Olson, 2014.

142 Antwortformat: 4-Likert-Skala; überhaupt nicht in Ordnung – eher nicht in Ordnung – eher in Ordnung – völlig in Ordnung.

14 NUTZUNGSHÄUFIGKEIT VON WEARABLES IM FITNESS-KONTEXT

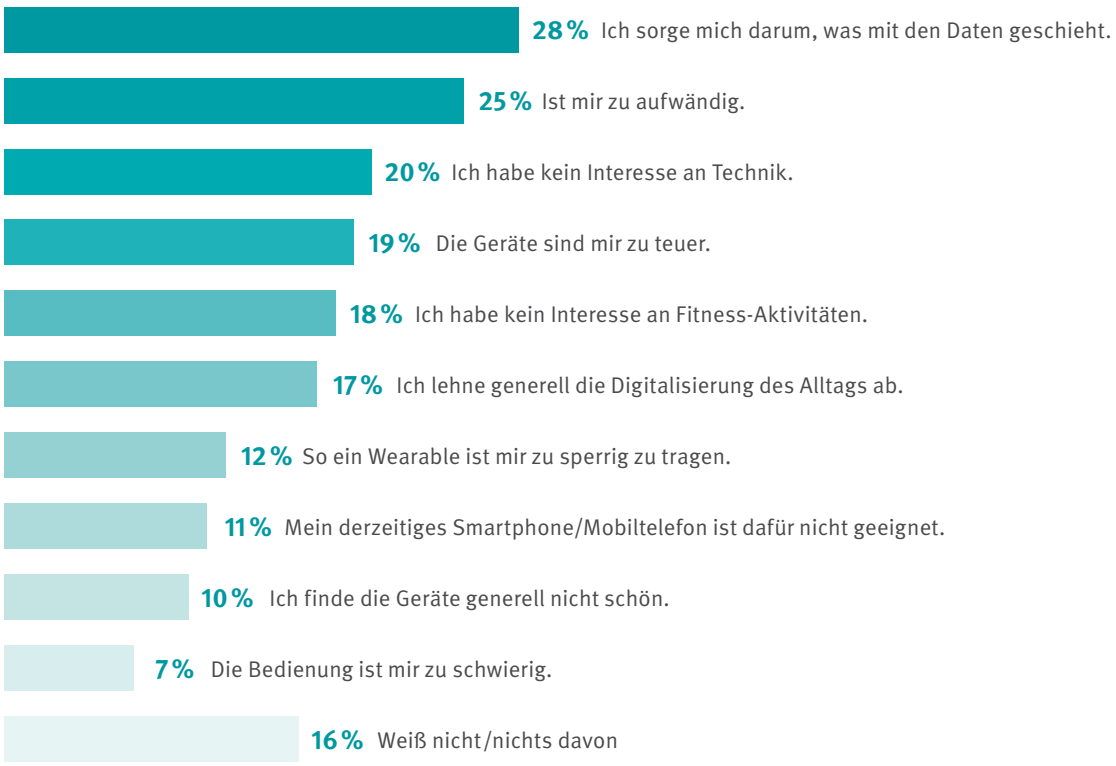


15 NUTZUNGSHÄUFIGKEIT NACH ALTERSGRUPPEN



Basis: Alle Befragten (n = 1.055), Angaben in Prozent **Frage:** Nutzen Sie ein Wearable mit Fitness-App?

16 GRÜNDE GEGEN DIE NUTZUNG VON WEARABLES



Basis: Künftige Nutzung eher/sehr unwahrscheinlich unter Nicht-Nutzern, die schon einmal von Wearables gehört haben (n = 392) | Angaben in Prozent: Anzahl der Nennungen. **Frage:** Welche der folgenden Gründe sind dafür ausschlaggebend, dass Sie Wearables nicht nutzen würden? Bitte nennen Sie mir alle Gründe, die auf Sie zutreffen (offene Frage mit vorkodierten Antworten, Mehrfachnennungen möglich).

den 28 Prozent der Nutzer ihr Wearable für Aktivitäten, für die ansonsten das Smartphone eingesetzt wird, wie beispielsweise für Kalenderfunktionen und Erinnerungen, um E-Mails abzurufen und Anrufe entgegenzunehmen.

Personen, die kein Wearable nutzen (Nicht-Nutzer), und darüber hinaus auch nicht planen, sich ein Wearable anzuschaffen, nennen hierfür eine Reihe unterschiedlicher Gründe (Abbildung 16). Neben dem zu hohen Nutzungs-Aufwand, nennen die Teilnehmer als häufigsten Grund die Sorge darum, was mit den hierdurch generierten Daten geschieht.

4.3 DATENSCHUTZBEDENKEN VON WEARABLE-NUTZERN UND NICHT-NUTZERN

Der überwiegende Anteil der Teilnehmer zeigt deutliche Datenschutzbedenken im Kontext von Online-Anwendungen (Abbildung 17). Wearable-Nutzer zeigen sich hierbei tendenziell weniger besorgt als Nicht-Nutzer, dass zu viele (65 vs. 74 %) oder unzutreffende Daten über sie gesammelt werden (48 vs. 62 %). Ebenso stören sie sich weniger häufig (66 %) – wenn auch mehrheitlich – daran, keine Kontrolle über ihre Daten zu haben als Nicht-Nutzer (78 %). Wearable-Nutzer finden es weniger riskant (62 vs. 75 %), persönliche Informationen preiszugeben und geben eher an, Vertrauen in Online-Dienste und deren Umgang mit persönlichen Informationen zu haben (50 vs. 39 %). Gleichzeitig zeigen sich sowohl Nutzer (75 %) als auch Nicht-Nutzer (78 %) in hohem Maße besorgt, wenn es um die Weitergabe ihrer Daten an andere Unternehmen geht.

4.4 FOLGENBEWERTUNG

Ein zentrales Problem bei der Nutzung von Wearables und Fitness-Apps ist die Möglichkeit, dass die zur Selbstvermessung generierten Daten auf eine vom Verbraucher ursprünglich nicht beabsichtigte Art und Weise genutzt werden könnten. Verbraucher können damit zusammenhängende Folgen jedoch nur subjektiv einschätzen. Hierbei können sie das Eintreten einer bestimmten Situation für mehr oder weniger wahrscheinlich halten und das eintretende Ergebnis in unterschiedlichem Ausmaß für akzeptabel halten.

Insgesamt hält es die Mehrheit der Teilnehmer für wahrscheinlich, dass Wearable-Daten im Zuge von Gerichtsverfahren verwendet werden (62 %) und findet dies darüber hinaus auch überwiegend in Ordnung (61 %, Abbildung 18). Fast drei Viertel (71 %) der Teilnehmer sind darüber im Bilde, dass ihre Daten für personalisierte Werbung verwendet werden – sie halten dies also für wahrscheinlich. Auffällig ist hierbei die große Diskrepanz zur diesbezüglichen Akzeptanz der Verbraucher: Nur 29 Prozent der Teilnehmer hält diese gängige Praktik für akzeptabel.

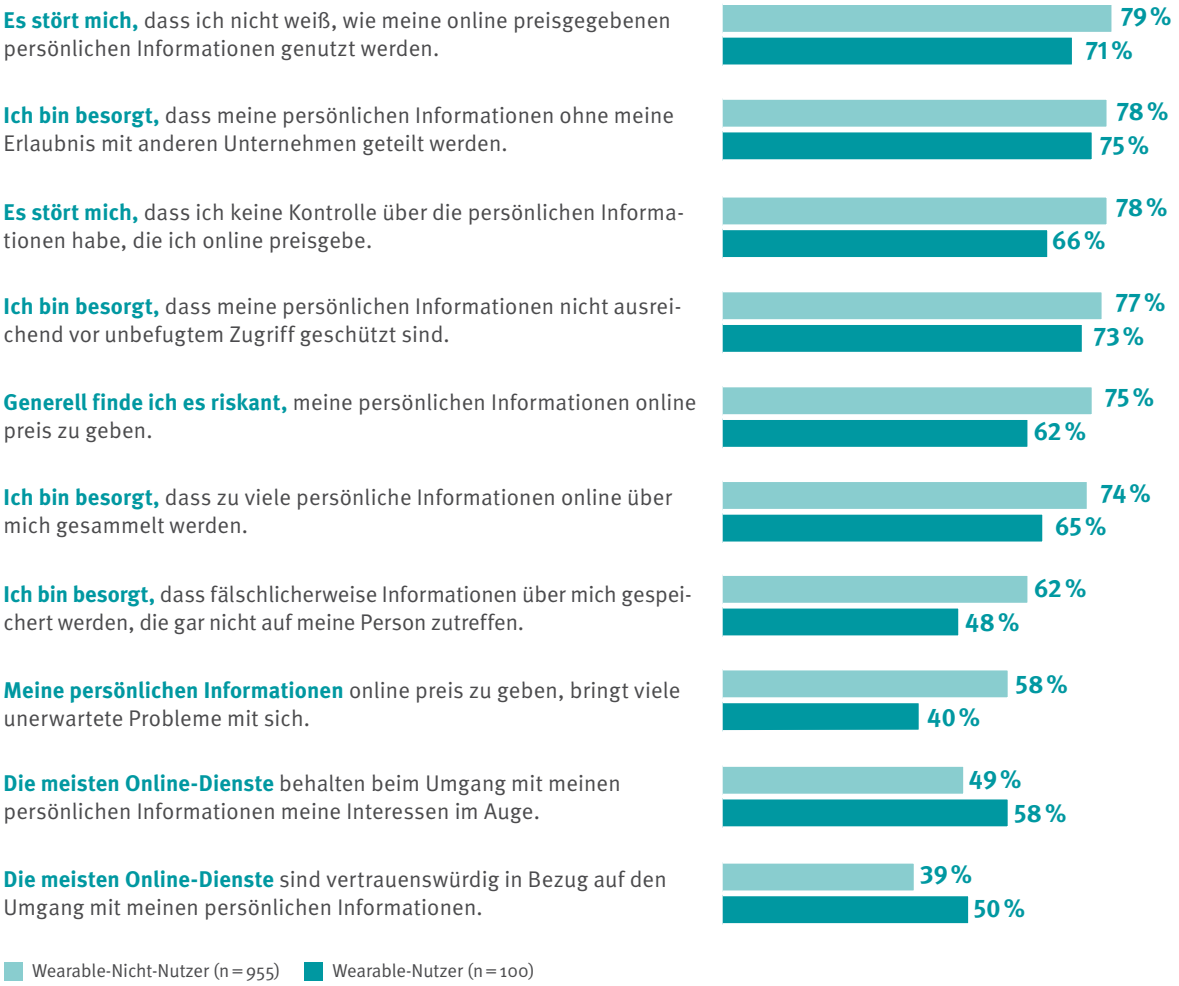
Ebenso zeigt sich eine große Diskrepanz für Situationen, in der Daten durch eine unbekannte Einzelperson ausgelesen werden – das Eintreten eines solchen Szenarios hält ungefähr die Hälfte (48 %) der Befragten für wahrscheinlich, die wenigsten fänden dies jedoch in Ordnung (7 %). Nur wenige Verbraucher fänden es akzeptabel, wenn ihr eigener Krankenkassenbeitrag auf Basis ihrer Fitness-Daten steigen würde (13 %), 34 Prozent fänden es jedoch in Ordnung, wenn ein Bekannter aufgrund seines ungesunden Lebensstils einen höheren Beitrag zahlen müsste. Nur bei einem Szenario übersteigen die Akzeptanzwerte die Schätzungen zur Eintrittswahrscheinlichkeit: 44 Prozent der Befragten fänden es in Ordnung, wenn Arbeitgeber Bonus-Prämien auf Basis von Fitness-Daten zahlen würden, nur 34 Prozent halten dies jedoch für wahrscheinlich.

4.5 ZWISCHENFAZIT: VERBRAUCHERBEFRAGUNG

Nutzungshäufigkeit. Die Ergebnisse der für Internetnutzer repräsentativen Verbraucherbefragung zeigen, dass ca. fünf Prozent der deutschen Internetnutzer ein Wearable in Zusammenhang mit Fitness nutzen. Im Vergleich zu anderen Untersuchungen ist dies eine relativ geringe Nutzungshäufigkeit. So gaben in einer YouGov-Befragung[143] 14 Prozent der Teilnehmer an, ein Wearable zu nutzen. Der Grund für diese Abweichung könnte in den unterschiedlichen methodischen Herangehensweisen liegen: Die Ergebnisse der YouGov-Untersuchung basieren auf Online-Interviews, wodurch eine Verzerrung der Stichprobe zugunsten Internet-affiner Personen – die möglicherweise auch eher ein Wearable nutzen – nicht auszuschließen ist. Dementgegen konnten die telefonisch befragten Teilnehmer der vorliegenden

143 YouGov, 2016, S.3.

17 ALLGEMEINE DATENSCHUTZBEDENKEN DER BEFRAGTEN



Basis: Alle Befragten (n = 1.055) | zusammengefasste Werte: stimme weitgehend/stimme voll und ganz zu. **Frage:** Ich lese Ihnen jetzt einige Aussagen zum Thema Umgang mit persönlichen Informationen vor. Bitte sagen Sie mir zu jeder Aussage, ob Sie ihr voll und ganz zustimmen, weitgehend zustimmen, weniger zustimmen oder gar nicht zustimmen.

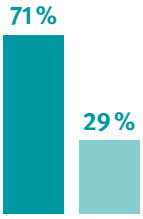
Untersuchung das Internet auch lediglich selten nutzen (mindestens einmal innerhalb der letzten drei Monate), ohne dass dies die Wahrscheinlichkeit minderte, in die Untersuchung mit aufgenommen zu werden.

Weiterhin bezieht die vorliegende Untersuchung auch Personen ab 14 Jahren mit ein. Eine detailliertere Analyse der Stichprobe zeigt hier, dass nur drei Prozent der unter 18-Jährigen ein Wearable nutzen (im Vergleich zu jeweils sechs Prozent bei den 19 bis 24-Jährigen und 25 bis 29-Jährigen). Somit setzt das Einbeziehen dieser Altersgruppe die Gesamt-Nutzungshäufigkeit notwendigerweise herab im Vergleich zur YouGov-Stichprobe, die Personen ab einem Alter von 18 Jahre befragt hat.

? Forschungsfrage 7: Wie bewerten Verbraucher mögliche Konsequenzen der Nutzung von Wearables und Fitness-Apps?

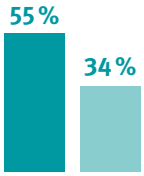
Wie potenzielle Folgen der Nutzung der Fitness-Daten durch Dritte eingeschätzt werden, hängt von der jeweiligen Situation ab. Besonders kritisch sehen Verbraucher offensichtlich Situationen, in denen Einzelpersonen ungefragt Fitness-Daten auslesen oder in denen derlei Daten automatisch über soziale Medien geteilt

18 BEWERTUNG MÖGLICHER FOLGEN DER WEARABLE-NUTZUNG: EINGESCHÄTZTE WAHRSCHEINLICHKEIT UND AKZEPTANZ

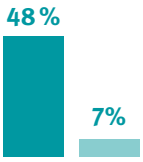


Auf Basis Ihrer Fitnessdaten erhalten Sie auf Sie persönlich zugeschnittene Werbung.

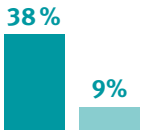
Sie beobachten einen Überfall, für den Sie als Zeuge vor Gericht aussagen sollen. Um zu überprüfen, ob Sie wirklich zur relevanten Uhrzeit am Tatort waren, werden Daten Ihres Wearables ausgelesen.



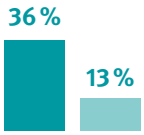
Ein Bekannter zahlt wegen seines ungesunden Lebensstils einen höheren Krankenkassentarif als Sie, denn er hat ein größeres Risiko krank zu werden.



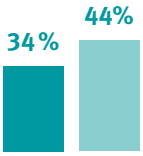
Eine unbekannte Person verbindet sich mit Ihrem Wearable, um Ihre Fitness-Daten auszulesen.



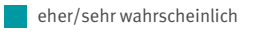
Ihre Fitness-Daten der letzten Woche werden automatisch auf Ihrem Facebook-Profil gepostet, darunter Ihre zurückgelegten Schritte und verbrannten Kalorien.



Sie haben längere Zeit keinen Sport gemacht, und ihre Aktivitätsdaten werden an ihre Krankenkasse übermittelt. Daraufhin erhöht sich Ihr Krankenkassenbeitrag.



Ihr Arbeitgeber zahlt zukünftig solchen Mitarbeitern eine Bonus-Prämie, die sich in ihrer Freizeit viel bewegen und das mit ihren Wearable-Daten nachweisen.



Basis: Alle Befragten (n = 1.055), zusammengefasste Werte: eher/völlig unwahrscheinlich bzw. eher/völlig in Ordnung. **Frage:** Im Folgenden werden einige Situationen beschrieben, die bei der Nutzung von Wearables und Fitness-Apps kurz- oder langfristig auftreten könnten. Bitte versetzen Sie sich in die jeweilige Situation und

a) schätzen Sie ein, für wie wahrscheinlich Sie es halten, dass Daten auf diese Art und Weise verwendet werden: sehr wahrscheinlich, eher wahrscheinlich, eher unwahrscheinlich oder sehr unwahrscheinlich?

b) beurteilen Sie, wie Sie es persönlich finden würden, wenn Daten auf diese Art und Weise verwendet würden: völlig in Ordnung, eher in Ordnung, eher nicht in Ordnung oder überhaupt nicht in Ordnung?

werden. Ebenso würde nur ein geringer Anteil der Verbraucher akzeptieren, wenn ihre Fitness-Daten zur Erhöhung ihres Krankenkassenbeitrags führen würden. Gleichzeitig zeigt eine aktuelle *Bitkom*-Studie,[144] dass dreißig Prozent der Befragten sich vorstellen können, Daten im Tausch gegen Rabatte an ihre Krankenkasse zu übermitteln. Ob Verbraucher die Verwendung ihrer Fitness-Daten durch Krankenkassen befürworten oder nicht, scheint insofern davon abzuhängen, ob sie sich einen (finanziellen) Vorteil davon erhoffen. So bewirkte das Skizzieren einer negativen Konsequenz – nämlich der Erhöhung des Beitrags anstatt einer Rabattierung – in der vorliegenden Befragung, dass nur wenige Teilnehmer eine solche Nutzung ihrer Daten akzeptie-

144 Maas & Rohleder, 2016, S.7.

ren würden. Anders sieht es aus, wenn es um Andere geht: Über die Hälfte der Befragten (55 %) hält es für wahrscheinlich, dass eine ungesund lebende Person zukünftig mit höheren Krankenkassentarifen rechnen muss.

Überraschend in der vorliegenden Untersuchung ist auch, dass die Mehrheit der Befragten ein Auslesen ihrer Daten im Rahmen eines gerichtlichen Verfahrens für wahrscheinlich hält und dies akzeptabel fände. Verbraucher scheinen also gewissermaßen damit zu rechnen, dass staatliche Stellen bei Bedarf auf ihre Daten zugreifen.

? Forschungsfrage 8: Unterscheiden sich Nutzer von Wearables und Fitness-Apps von Nicht-Nutzern in ihren generellen Datenschutzbedenken?

Knapp ein Viertel der Verbraucher, die die Nutzung von Wearables und Fitness-Apps eher ablehnen, nennen hierfür die Sorge um ihre Daten als wichtigen Grund. Im Vergleich zu Wearable-Nutzern äußern Nicht-Nutzer hierbei tendenziell häufiger allgemeine Datenschutzbedenken, während Wearable-Nutzer häufiger angeben, den Unternehmen im Umgang mit ihren Daten zu vertrauen.

Unabhängig davon sorgt sich jedoch auch die Mehrheit der Wearable-Nutzer um die Sicherheit und eine potentielle Weitergabe ihrer Daten und lehnt letztere deutlich ab. Mit anderen Worten: Wearable-Nutzern ist die Sicherheit ihrer Daten keineswegs egal.

Ein häufig hervorgebrachtes Argument in diesem Kontext ist, dass der Nutzen für Verbraucher größer sein muss als der empfundene Nachteil, wenn Verbraucher sich trotz ihrer Bedenken für die Nutzung der Dienstleistung entscheiden.[145] Dies muss vor dem Hintergrund einer aktuellen US-amerikanischen Studie in Frage gestellt werden.[146] Die Autoren zeigten, dass viele Menschen nur bereit sind, ihre Daten gegen Dienstleistungen und Rabatte „einzutauschen“, weil sie in einer Art grundlegenden Resignation davon ausgehen, die Kontrolle über ihre Daten ohnehin schon verloren zu haben.

145 Dinev & Hart, 2006.
146 Turow, Hennessy, Michael, & Draper, 2015.

5. ZUSAMMENFASSUNG

Die vorliegende Untersuchung beleuchtet drei datenschutzrelevante Aspekte der Nutzung von Wearables und Fitness-Apps. Untersucht wurden technische Eigenschaften von Wearables und Fitness-Apps, der Umgang der Anbieter mit geltenden Datenschutzbestimmungen sowie Einstellungen seitens der Verbraucher im Kontext der Nutzung von Wearables und Fitness-Apps.

Die technische Prüfung von zwölf Wearables und 24 Fitness-Apps zeigte, dass Datenschutzstandards auf technischer Ebene nicht immer eingehalten werden. So integrieren nur wenige Wearable-Anbieter Schutzmaßnahmen gegen ungewolltes Tracking. Möglich wäre hierdurch beispielsweise, dass Betreiber von Einkaufszentren die Laufwege ihrer Kunden ohne deren Wissen oder Einwilligung tracken.[147] Die Mehrzahl der Apps sendet – wenig datensparsam – eine Vielzahl mitunter sensibler Informationen an Anbieter-Server und bindet auch Drittanbieter in ihre Dienste mit ein. Technische Daten und Daten zum Nutzungsverhalten werden von 16 der 24 geprüften Apps schon an Drittanbieter gesendet, bevor der Verbraucher die Möglichkeit hat, den Nutzungsbedingungen und gegebenenfalls der Datenschutzerklärung zuzustimmen. Positiv hervorzuheben ist, dass alle Informationen https-transportverschlüsselt versendet werden, wenngleich zusätzliche Sicherungsmaßnahmen wie Certificate Pinning aus Verbraucherschutzperspektive wünschenswert wären.

Die getesteten Wearables bieten kaum Schutz vor ungewolltem Tracking. Fitness-Apps senden in vielen Fällen schon Daten an Anbieter und Drittanbieter, bevor der Verbraucher die Möglichkeit hat, den Nutzungsbedingungen und gegebenenfalls der Datenschutzerklärung zuzustimmen.

Anbieter müssen ihre Kunden über den Umgang mit den nutzergenerierten Inhalten aufklären – in der Regel tun sie dies in ihren Datenschutzhinweisen. Eine Analyse der zur Verfügung gestellten Informationen zeigt jedoch, dass Anbieter dieser Informationspflicht nach in dieser Untersuchung vertretener Auffassung in mehreren Fällen nicht ausreichend nachkommen: Drei Anbieter stellen ihre Datenschutzhinweise nur in englischer Sprache bereit, nur zwei Anbieter informieren über die Besonderheit der erhobenen Gesundheitsdaten. Nur bei einem Anbieter werden im Rahmen der separaten Zustimmung zur Datenschutzerklärung und den Nutzungsbedingungen Gesundheitsdaten ausdrücklich genannt. Darüber hinaus erschwert oft die bloße Textschwierigkeit der Datenschutzerklärungen, dass Nutzer sich tatsächlich über den Umgang mit ihren Daten informieren können.

Anbieter informieren kaum über die besondere Sensibilität der erhobenen Gesundheitsdaten. Nur ein Anbieter erwähnt im Rahmen des Installationsprozesses ausdrücklich, dass Gesundheitsdaten verarbeitet werden.

Die Ergebnisse der repräsentativen Befragung weisen darauf hin, dass Datenschutz ein wichtiges Thema für Verbraucher im Kontext von Wearables und Fitness-Apps ist. Sowohl Wearable-Nutzer als auch Nicht-Nutzer zeigen sich hierbei mehrheitlich besorgt in Bezug auf den Umgang mit ihren online generierten Daten und stören sich daran, die Kontrolle über ihre eigenen Daten abzugeben. Wearable-Nutzer scheinen jedoch tendenziell größeres Vertrauen zu haben, dass Dienste-Anbieter verantwortungsvoll mit den über sie erhobenen Daten umgehen. Potentielle Folgen, die eine Verwendung der von Wearables generierten Daten nach sich ziehen können, werden unterschiedlich bewertet: Viele Verbraucher fänden es akzeptabel, wenn Wearable-Daten zur Validierung von Zeugenaussagen (61 %) oder im Rahmen von Arbeitgeber-Bonusprogrammen (44 %) verwendet würden. Andere Szenarien wie die Anpassung von Krankenkassentarifen auf Basis von Fitness-Daten oder auch das Auslesen von Fitness-Daten durch fremde Personen werden nur von einem kleineren Teil der Befragten akzeptiert.

Wearable-Nutzer und Nicht-Nutzer haben ausgeprägte Datenschutzbedenken. Die Verwendung von Fitness-Daten zur Anpassung von Krankenkassentarifen und auch das Auslesen von Fitness-Daten durch fremde Personen werden mehrheitlich abgelehnt.

147 Hilts et al., 2016, S. 26.

Damit Verbraucher langfristig von der fortschreitenden Digitalisierung tatsächlich profitieren, muss der Umgang mit den sensiblen nutzergenerierten Inhalten verbraucherfreundlich reguliert werden. Denn während die Nutzung von Wearables und Fitness-Apps ein Mehr an Autonomie über die eigene Gesundheit bedeuten kann, ist der Preis hierfür ein Autonomieverlust[148] über die eigenen sensiblen Daten: Lückenhafte Schutzmechanismen gegen unbefugtes Tracking, ein ausgeprägtes Datensendungsverhalten der Fitness-Apps und diesbezügliche mangelnde Kontrollmöglichkeiten seitens des Nutzers machen Nachbesserungen in Sachen Datenschutz und Datensicherheit notwendig.

148 Dockweiler & Razum, 2015.

QUELLENVERZEICHNIS

Literatur

Abril, E. P. (2016). Tracking myself: Assessing the contribution of mobile technologies for self-trackers of weight, diet, or exercise. Journal of Health Communication, 21(6), 1–9. http://doi.org/10.1080/10810730.2016.1153756

Ackerman, L. (2013). Mobile health and fitness applications and information privacy: Report to California Consumer Protection Foundation. Privacy Rights Clearinghouse. Abgerufen von https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks [Stand: 12.01.2017].

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM conference on Electronic commerce (pp. 21-29). New York, USA. Abgerufen von http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf [Stand: 11.01.2017].

Amstad, T. (1978). Wie verständlich sind unsere Zeitungen? Dissertation Universität Zürich. http://doi.org/10.1017/CBO9781107415324.004. Artikel-29-Datenschutzgruppe (2015). ANNEX - health data in apps and devices. Abgerufen von http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [Stand: 11.01.2017].

Ballhaus, W., Song, B., Meyer, F.-A., Ohrtmann, D. J.-P., & Dressel, D. C. (2015). Media Trend Outlook Wearables: Die tragbare Zukunft kommt näher. PricewaterhouseCoopers Aktiengesellschaft Wirtschaftsprüfungsgesellschaft (Hrsg.). Abgerufen von http://www.pwc.de/de/technologie-medien-und-telekommunikation/whitepaper_wearables.html [Stand: 11.01.2017].

Barczok, A. & Porteck, S. (2015). Frisst weniger, weiß mehr - Android 6.0 Marshmallow mit Assistent, Berechtigungssystem und Stromsparmodus. C't, 23, 20-21. Abgerufen von http://epaper.heise.de/download/archiv/a5ac98c5ad28/ct.15.23.020-021.pdf [Stand: 16.02.2017].

Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11 (9). Abgerufen von http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/867 [Stand: 11.01.2017].

BMJV (2016). Am Puls der Zeit? Wearables und Gesundheits-Apps aus verbraucherpolitischer Sicht. Positionspapier zum Safer Internet Day. Abgerufen von http://www.bmjv.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/Positionspapier.pdf?__blob=publicationFile&v=2 [Stand: 11.01.2017].

Bortz, J. (2005). Statistik für Human- und Sozialwissenschaftler (6. Auflage). Heidelberg: Springer Medizin Verlag.

Bundestags-Drucksache 18/0958. Kleine Anfrage - Verhaltensbasierte Versicherungstarife – Apps und Wearables in der gesetzlichen Krankenversicherung (04.07.2016). Abgerufen von http://dip21.bundestag.de/dip21/btd/18/090/1809058.pdf [Stand: 11.01.2017].

Bundestags-Drucksache 18/9243. Antwort der Bundesregierung – Verhaltensbasierte Versicherungstarife – Apps und Wearables in der gesetzlichen Krankenversicherung (21.07.2016). Abgerufen von http://dip21.bundestag.de/dip21/btd/18/092/1809243.pdf [Stand: 11.01.2017].

Burkhardt, W. (2013). Einer für alle, alle für einen – Das Solidarprinzip in der gesetzlichen Krankenversicherung. Bundeszentrale für politische Aufklärung. Abgerufen von http://www.bpb.de/politik/innenpolitik/gesundheitspolitik/72358/solidarprinzip?p=all [Stand 09.02.2017].

Christl, W. (2014). Kommerzielle digitale Überwachung im Alltag. Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data. Wien: Studie im Auftrag der Bundesarbeitskammer. Abgerufen von http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf [Stand: 11.01.2017].

Christmann, U. (2004). Verstehens- und Verständlichkeitsmessung. Methodische Ansätze in der Anwendungsforschung. In K. D. Lerch (Hrsg.), Recht verstehen. Verständlichkeit, Missverständlichkeit und Unverständlichkeit von Recht (S. 33–62). Berlin: de Gruyter.

Clausing, E., Schiefer, M., Lösche, U., & Morgenstern, M. (2015). Internet of Things: Security evaluation of nine Fitness Trackers. Magdeburg. Abgerufen von https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf [Stand: 12.01.2017].

Dachwitz, I. (2016). Norwegische Verbraucherschützer decken Datenschutzleck bei Fitness-App auf – morgen AGB-Vorlese-Marathon. Netzpolitik.org e. V. Abgerufen von https://netzpolitik.org/2016/norwegische-verbraucherschuetzer-decken-datenschutzleck-bei-fitness-app-auf-morgen-agb-vorlese-marathon/ [12.01.2017].

Damm, K., Kuhlmann, A., & von der Schulenburg, J.-M. (2010). Der Gesundheitsmarkt 2015 – Trends und Entwicklungen. Göttingen: Cuvillier Verlag. Abgerufen von https://www.ivbl.uni-hannover.de/fileadmin/versicherung/Publikationen/Publikationen/Graf_von_der_Schulenburg_2010_Der_Gesundheitsmarkt_2015.pdf [12.01.2017].

Delisle, M. (2016). Step Into "The Circle" – Wearables und Selbstvermessung im Fokus. Abgerufen von http://www.abida.de/sites/default/files/09%20Wearables.pdf [12.01.2017].

Di Luzio, A., Mei, A., & Stefa, J. (2016). Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests. Proceedings of the 35th Annual IEEE International Conference on Computer Communications (10. – 14. April), San Francisco, CA, USA. http://doi.org/10.1109/INFOCOM.2016.7524459

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80. http://doi.org/10.1287/isre.1060.0080

Dockweiler, C., Boketta, R., Schnecke, J. H., & Hornberg, C. (2016). Nutzungsverhalten und Akzeptanz von mHealth-Applikationen bei jungen Erwachsenen in Deutschland. Tagungsband TELEMED 2015 - 20. Nationales Forum für Gesundheitstelematik und Telemedizin (im Druck).

Dockweiler, C., & Razum, O. (2015). Digitalisierte Gesundheit: Neue Herausforderungen für Public Health. *Gesundheitswesen* (Editorial). 78(01), 5-7. doi:10.1055/s-0041-110679

DuBay, W. H. (2004). The principles of readability. Costa Mesa, CA: Impact Information. http://doi.org/10.1.1.91.4042

Ehlert, P., Flischikowski, C., Gerloch, T., Hammerl, A., Kasper, B., Klaiber, M., Klose, M., Schleifer, T., Staiger, L., Urbanczyk, M., Wurst, M. (2015). Das vermessene Selbst – Praktiken und Diskurse digitaler Selbstvermessung. Eberhard Karls Universität Tübingen, Wirtschafts- und Sozialwissenschaftliche Fakultät. Abgerufen von http://dx.doi.org/10.15496/publikation-1200 [Stand: 11.01.2017].

Eikenberg, R. (2012). Gut App-geschaut - Netzwerkverkehr von Smartphones kontrollieren. C't, 7, 120–124.

En, B., & Pöll, M. (2016). Are you (self-)tracking? Risks, norms and optimisation in self-quantifying practices. Graduate Journal of Social Science, 12(2), 37–57. Abgerufen von http://gjss.org/sites/default/files/issues/chapters/papers/GJSS Vol 12-2 2 En and Pöll_0.pdf [Stand: 11.01.2017].

Gigerenzer, G., Schlegel-Matthies, K., & Wagner, G. G. (2016). Digitale Welt und Gesundheit. eHealth und mHealth – Chancen und Risiken der Digitalisierung im Gesundheitsbereich. Sachverständigenrat für Verbraucherfragen beim Bundesministerium für Justiz und den Verbraucherschutz (Hrsg.), Berlin. Abgerufen von www.svr-verbraucherfragen.de/wp-content/uploads/2016/01/Digitale-Welt-und-Gesundheit.pdf [Stand: 11.01.2017].

Goldhammer, K. (2016). Die Zukunft des Computers liegt in seinem Verschwinden: Die Wearables kommen! In Digitaltrends – LfM. Wearables. Landesanstalt für Medien Nordrhein Westfalen (Hrsg.), Düsseldorf. Abgerufen von www.lfm-nrw.de/fileadmin/user_upload/lfm-nrw/Foerderung/Digitalisierung/Digitaltrends/Digitaltrends_Wearables.pdf [Stand: 11.01.2017].

Hancke, J., Vajjala, S., & Meurers, D. (2012). Readability classification for German using lexical, syntactic, and morphological features. Proceedings of the 24th International Conference on Computational Linguistics (COLING 2012), 1063–1080. Abgerufen von http://www.aclweb.org/anthology/C12-1065 [Stand: 11.01.2017].

Hartge, D. (2012). Erlaubnisse und Verbote im Datenschutzrecht. In J.-H. Schmidt & T. Weichert (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen (S. 280–288). Bonn: Bundeszentrale für politische Bildung.

Herrmann, D., & Lindemann, J. (2016). Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights? CoRR, abs/1602.0. Abgerufen von http://arxiv.org/abs/1602.01804 [Stand: 11.01.2017].

Hilts, A., Parsons, C., & Knockel, J. (2016). Every step you fake: A comparative analysis of Fitness Tracker privacy and security. Open Effect Report (2016). Abgerufen von https://openeffect.ca/reports/Every_Step_You_Fake.pdf [Stand: 11.01.2017].

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. MIS Quarterly, 37(1), 275–298. Abgerufen von https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229627 [Stand: 11.01.2017].

Howes, L. M., Julian, R., Kelty, S. F., Kemp, N., & Kirkbride, K. P. (2014). The readability of expert reports for non-scientist report-users: Reports of DNA analysis. Forensic Science International, 237, 7–18. http://doi.org/10.1016/j.forsciint.2014.01.007

Jahberg, H., Mortsiefer, H., Neuhaus, C., Haselberger, S., Müller-Lissner, A., & Bosch, R. (2015, 08.08.). Datenschützer warnen vor Fitness-Apps. Der Tagesspiegel. Abgerufen von http://www.tagesspiegel.de/weltspiegel/software-und-wearables-datenschuetzer-warnen-vor-fitness-apps/12162152.html [Stand: 11.01.2017].

Jandt, S. (2008). Grenzenloser Mobile Commerce. Schutzwirkung und Durchsetzbarkeit datenschutzrechtlicher Ansprüche gegenüber ausländischen Dienstanbietern. In Datenschutz und Datensicherheit (DuD), 32 (10), 664–669.

Klofta, J. & Rest, J. (2015, 23.04.). Der überwachte Mitarbeiter macht nicht blau. Panorama (Das Erste). Abgerufen von http://daserste.ndr.de/panorama/Der-ueberwachte-Mitarbeiter-macht-nicht-blau,gesundheitsapp104.html [Stand: 31.01.2017].

Laugsand, L. E., Strand, L. B., Platou, C., Vatten, L. J., & Janszky, I. (2014). Insomnia and the risk of incident heart failure: A population study. European Heart Journal, 35(21), 1382–1393. http://doi.org/10.1093/eurheartj/eht019

LDI Nordrhein-Westfalen (2016). Datenübermittlungen in die USA – Fragen und Antworten zum EU-US Privacy Shield. https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt/Eingangsseite/EU_US_Privacy_Shield_Text_komplett.pdf [Stand: 15.02.2017]

Lester, S. & Stone, P. (2016, 05.05.). Bluetooth LE - Increasingly popular, but still not very private.Contextis.com. Abgerufen von https://www.contextis.com/resources/blog/bluetooth-le-increasingly-popular-still-not-very-private/ [Stand: 16.01.2017].

Lucassen, T., Dijkstra, R., & Schraagen, J. M. (2012). Readability of Wikipedia. First Monday, 17(9). http://doi.org/10.5210/fm.v0i0.3916

Luers, J. C., Gostian, A. O., Roth, K. S., & Beutner, D. (2013). Lesbarkeit von medizinischen Texten im Internetangebot deutscher HNO-Universitätskliniken. HNO, 61(8), 648–654. http://doi.org/10.1007/s00106-013-2674-7

Lupton, D. (2014). Self-tracking modes: Reflexive self-monitoring and data practices. Abgerufen von http://ssrn.com/abstract=2483549 [Stand: 11.01.2017].

Lupton, D. (2015). Digital health technologies and digital data: New ways of monitoring, measuring and commodifying human embodiment, health and illness. In F. X. Olleros & M. Zhegu (Hrsg.), Research Handbook on Digital Transformations (pp. 1–16). Northampton, MA: Edward Elgar.

Lutter, T., Pentsi, A., Poguntke, M., Böhm, K., & Esser, R. (2015). Zukunft der Consumer Electronics – 2015. Marktentwicklung, Schlüsseltrends, Mediennutzung Konsumentenverhalten, Neue Technologien. Bitkom e.V. (Hrsg.), Berlin. Abgerufen von https://www.bitkom.org/Publikationen/2015/Studien/CE-Studie-2015/150901-CE-Studie-2015-online.pdf [Stand: 11.01.2017].

Maas, H. & Rohleder, B. (2016). Fitnesstracker und Datenschutz. Bundesministerium der Justiz und für Verbraucherschutz in Kooperation mit Bitkom e.V. Abgerufen von https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/Bitkom-Charts-PK-Safer-Internet-Day-E-Tracker-und-Datenschutz-09-02-2016-final.pdf [Stand 12.01.2017].

McDonald, A. M., & Cranor, L. F. (2009). The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4(3), 543–568.

Meißner, S. (2016). Selbstoptimierung durch Quantified Self? Selbstvermessung als Möglichkeit von Selbststeigerung, Selbsteffektivierung und Selbstbegrenzung. In S. Selke (Hrsg.), Lifelogging – Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel (S. 217–236). Wiesbaden: Springer VS. http://doi.org/DOI 10.1007/978-3-658-104160

Michalke, M. (2012). Using the koRpus package for text analysis. Abgerufen von https://reaktanz.de/R/pckg/koRpus/koRpus_vignette.pdf [Stand: 11.01.2016].

Musch, J., & Rösler, P. (2011). Schnell-Lesen: Was ist die Grenze der menschlichen Lesegeschwindigkeit? In M. Dresler (Hrsg.), Kognitive Leistungen. Intelligenz und mentale Fähigkeiten im Spiegel der Neurowissenschaften (S. 89–106). Berlin/ Heidelberg: Springer Verlag. http://doi.org/10.1007/978-3-8274-2809-7

Myrstad, F. (2016). Consumer protection in fitness wearables. Forbrukerrådet. Abgerufen von http://fbrno.climg.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf [Stand: 11.01.2017].

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. The Journal of Consumer Affairs, 41(1), 100–126. http://doi.org/10.1111/j.1083-6101.2009.01494.x

Olson, P. (2014, 16.11.). Fitbit data now being used in the courtroom. *Forbes*. Abgerufen von http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#182387b209f8 [Stand: 02.02.2017].

Plattform Verbraucherschutz in einer digitalisierten Welt (2015). One Pager: Muster für transparente Datenschutzhinweise. Abgerufen von http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Verbraucherportal/OnePager/11192915_OnePager-Datenschutzhinweise.html [Stand: 30.01.2017].

Raether, T. (2013). Rührt euch! Sueddeutsche Zeitung Magazin, Heft 39. Abgerufen von http://sz-magazin.sueddeutsche.de/texte/anzeigen/40717/Ruehrt-Euch [Stand: 08.02.2017].

Renn, O. (2008). Concepts of Risk: An Interdisciplinary Review Part 1: Disciplinary Risk Concepts. GAIA – Ecological Perspectives for Science and Society, 17(2), 196–204.

Sachverständigenrat für Verbraucherfragen (2016). Verbraucher in der Digitalen Welt - Verbraucherpolitische Empfehlungen. Berlin: Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision-making. Journal of Risk and Uncertainty, 1, 7–59. http://doi.org/10.1007/bf00055564

Schneider, M., Enzmann, M., & Stopczynski, M. (2014). Web Tracking Report 2014. Waidner, M. (Hrsg.), Darmstadt: Fraunhofer-Institut für Sichere Informationstechnologie (SIT). Abgerufen von https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf [Stand: 11.01.2017].

Schumacher, F. (2016). Quantified Self – eine nachhaltige Bewegung? In T. Andelfinger & V. Hänisch (Hrsg.), eHealth. Wie Smartphones, Apps und Wearables die Gesundheitsversorgung verändern wollen (S. 39–53). Wiesbaden: Springer Gabler.

Schwan, B. (2017, 09.01.). Samsung macht Gear S2, S3 und Gear Fit2 iOS-kompatibel. Abgerufen von https://www.heise.de/newsticker/meldung/Samsung-macht-Gear-S2-S3-und-Gear-Fit2-iOS-kompatibel-3591298.html [Stand: 18.01.2017].

Selke, S. (2015). Lifelogging oder: Der fehlerhafte Mensch. Blätter Für deutsche und internationale Politik. Abgerufen von https://www.blaetter.de/archiv/jahrgaenge/2015/mai/lifelogging-oder-der-fehlerhafte-mensch [Stand: 11.01.2017].

Selke, S. (2016). Lifelogging zwischen disruptiver Technologie und kulturellem Wandel. In S. Selke (Hrsg.), Lifelogging – Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel (S. 1–21). Wiesbaden: Springer VS.

Sjögren, P., Fisher, R., Kallings, L., Svenson, U., Roos, G., & Hellénius, M.-L. (2014). Stand up for health—avoiding sedentary behaviour might lengthen your telomeres: Secondary outcomes from a physical activity RCT in older people. British Journal of Sports Medicine, 48(19), 1–3. http://doi.org/1136/bjsports-2013-093342

Slovic, P. (2000). The perception of risk. London: Earthscan Publications.

IDC (2016). Worldwide Quarterly Wearable Device Tracker. Abgerufen von http://www.idc.com/getdoc.jsp?containerId=prUS41037416 [Stand 02.02.2017].

Steinbrunn, L., Dominsky, S., & Goods, L. (2016). Der Uhrenmarkt in Deutschland. Trends und Entwicklungen. GfK Retail and Technology GmbH. Nürnberg. Abgerufen von http://fs-media.nmm.de/ftp/INH/Website/Files/PDF/Watch-Innovation-Forum-2016/Laura-Steinbrunn-Sabine-Dominski.pdf [12.01.2017].

Stiftung Warentest (2013). Ich weiß, wieviel du wiegst – Gesundheits-Apps. Test, 11/2013, 84 – 97.

Stiftung Warentest (2015). Smartwatches - Handlanger für's Handy. Test, 10/2015, 30–35.

Stiftung Warentest (2016a). Fitness-Armbänder - Noch nicht in Topform. Test, 1/2016, 82–87.

Stiftung-Warentest (2016b). Datenschutzerklärungen: Lange Texte, wenig Inhalt. Test, 3/2016, 57–61.

Surfer haben Rechte (2014). Untersuchung von Apps - Zugriffsberechtigung, Kontaktmöglichkeiten, Verbraucherinformationen und In-App-Käufe. Eine Untersuchung des Projekts „Verbraucherrechte in der digitalen Welt". Verbraucherzentrale Bundesverband (Hrsg.). Abgerufen von http://www.surfer-haben-rechte.de/content/untersuchungsbericht-appberechtigungen [Stand: 03.02.2017].

Tian, C., Champlin, S., Mackert, M., Lazard, A., & Agrawal, D. (2016). Readability, suitability, and health content assessment of web-based patient education materials on colorectal cancer screening. Gastrointestinal Endoscopy, 80(2), 284–290.e2. http://doi.org/10.1016/j.gie.2014.01.034

Tomlinson, M., Rotheram-Borus, M. J., Swartz, L., & Tsai, A. C. (2013). Scaling up mHealth: Where is the evidence? PLoS Medicine, 10(2), 1–5. http://doi.org/10.1371/journal.pmed.1001382

Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy. How marketers are misrepresenting American consumers and opening them up to exploitation. A report from the Annenberg School for Communication, University of Pennsylvania. Abgerufen von:
https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [Stand: 06.02.2017].

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131.

Umann, M., Tuscher, H., Buchmann, T., Bosch, J. (2016). eHealth in der Arbeitswelt – Prävention von stress- und bewegungsbedingten Berufskrankheiten. In T. Andelfinger & V. Hänisch (Hrsg.), eHealth. Wie Smartphones, Apps und Wearables die Gesundheitsversorgung verändern wollen (S. 209–216). Wiesbaden: Springer Gabler. http://doi.org/10.1017/CBO9781107415324.004

Verbraucherzentrale NRW (2015). Bonusprogramme der gesetzlichen Krankenkassen. Untersuchung der Verbraucherzentrale NRW. Abgerufen von http://www.verbraucherzentrale.nrw/media236794A.pdf [Stand: 11.01.2017].

Wang, P. (2014). Bluetooth Low Energy – privacy enhancement for advertisement. Norwegian University of Science and Technology. Abgerufen von http://www.diva-portal.org/smash/get/diva2:750267/FULLTEXT01.pdf [Stand: 11.01.2017].

Weichert, T. (2009). Datenschutz bei Internetveröffentlichungen. In Verbraucher und Recht. Zeitschrift für Wirtschafts- und Verbraucherrecht (VuR), 24 (9), 323-330.

Wiggers, K. (2016). Jiobit aims to make Wearables so discreet they´re practically invisible. Digital Trends. Abgerufen von http://www.digitaltrends.com/wearables/jiobit-childrens-wearable-could-last-weeks-on-one-charge/ [Stand: 11.01.2017].

Wilson, M. (2009). Readability and patient education materials used for low-income populations. Clinical Nurse Specialist: The Journal for Advanced Nursing Practice, 23(1), 33–40. http://doi.org/10.1097/01.NUR.0000343082.95955.e3

YouGov (2016). Wearables und Gesundheits-Apps. Verbraucherbefragung im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz. BMJV (Hrsg.) Abgerufen von http://www.bmjv.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/YouGov.pdf?__blob=publicationFile&v=3 [Stand: 11.01.2017].

Kommentare und Handbücher

Gusy, C. (2016). BeckOK BDSG. In: H. A. Wolff & S. Brink (Hrsg.), BeckOK Datenschutzrecht (16. Ed, § 1 Rn. 112-116). München: C. H. Beck. Abgerufen von http://www.beck-online.de [Stand: 26.01.2017].

BeckOK Datenschutzrecht (16. Auflage). München: C. H. Beck. Abgerufen von http://www.beck-online.de [Stand: 26.01.2017].

Gola, P., & Schomerus, R. (2015). BDSG Kommentar. In: P. Gola & R. Schomerus (Hrsg.), Bundesdatenschutzgesetz Kommentar (12. Auflage). München: C. H. Beck.

Bäcker, M. (2016). BeckOK BDSG. In: H. A. Wolff & S. Brink (Hrsg.), BeckOK Datenschutzrecht (17. Auflage). München: C. H. Beck. Abgerufen von http://www.beck-online.de [Stand: 26.01.2017].

BMJV (2008). Handbuch Rechtsförmlichkeit (3. Auflage). Berlin. Abgerufen von http://hdr.bmj.de/vorwort.html [Stand: 11.01.2017].

Simitis, S. (2014). BDSG Kommentar. In: S. Simitis (Hrsg.), Bundesdatenschutzgesetz (8. Auflage). Baden-Baden: Nomos.

Roßnagel, A. (2003). Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung. München: Verlag C. H. Beck.

Bitte zitieren Sie die vorliegende Studie wie folgt:

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C., & Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e. V. (Hrsg.). Online verfügbar unter http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps

IMPRESSUM

Herausgeber
Verbraucherzentrale NRW e. V.
Mintropstr. 27
40215 Düsseldorf
Tel. (0211) 3809 0
Fax. (0211) 3809 172
marktwaechter@verbraucherzentrale.nrw

Text: Dr. Ricarda Moll, Dr. Anne Schulze, Miriam Rusch-Rodosthenous, Christopher Kunke, Lisa Scheibel

Titelbild: iStockphoto/venimo
Gestaltung: Birgit Hirschmann
Druck: Königsdruck – Printmedien und digitale Dienste GmbH

Stand: April 2017
Gedruckt auf 100 Prozent Recyclingpapier

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

verbraucherzentrale