International Working Group
on Data Protection
in Telecommunications

675.50.25

Arbeitspapier zum Datenschutz bei tragbaren Endgeräten („Wearables“)[1]

57. Sitzung, 27./28. April 2015, Seoul (Republik Korea)

- Übersetzung -

Allgemeiner Hintergrund und Anwendungsbereich

Die Nutzung von tragbaren Endgeräten (im folgenden „wearables“) beschreibt den Einsatz von Rechentechnik, die klein genug ist, um am Körper des Nutzers getragen werden zu können[2]. Diese Geräte weisen verschiedene Arten von Sensoren mit unterschiedlichen Fähigkeiten auf. So haben Sensoren z.B. die Fähigkeit, laufend Informationen über den Körper des Nutzers (Stimmung, Gewohnheiten, körperliche Aktivitäten, Gesundheitszustand, Geschwindigkeit, Mobilität), die Umgebung des Nutzers (Bilder, Geräusche, Temperatur, Feuchtigkeit, Aufenthaltsort, soziale Umgebung) wie auch computer-generierte Daten zur Vermittlung der Nutzererfahrung mit seiner Umwelt zu sammeln.

Viele Wearables enthalten in irgendeiner Form eine Kamera. Auch wenn eine Kamera nur einige der oben genannten Informationen erfassen würde, ist die Kamera-Funktion der Gegenstand vieler aktueller Datenschutz-Bedenken[3]. Es ist die Fähigkeit dieser Geräte, möglicherweise permanent und heimlich Bilder aufzuzeichnen, die zu vielen datenschutzbezogenen Bedenken führt, insbesondere, wenn Dritte derartigen Gegenstand solcher Aufnahmen werden.

Gegenwärtig gibt es vier Hauptbereiche auf dem Markt für Wearables[4]:

---

[1] Dieses Arbeitspapier fusst wesentlich auf dem Bericht der Research Branch of the Office of the Privacy Commissioner of Canada “Wearable Computing: Challenges and Opportunities for Privacy Protection”, January 2014, mit weiteren Nachweisen; https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.asp

[2] Es gibt mehrere unterschiedliche Definitionen des Begriffs “wearable computing”. S. z.B. Steve Mann, (1996a): Smart Clothing: The Shift to Wearable Computing. In Communications of the ACM, 39 (8) pp. 23-24. Siehe Mann, Steve (2014): Wearable Computing. In: Soegaard, Mads and Dam, Rikke Friis (eds.). *The Encyclopedia of Human-Computer Interaction*, 2nd Ed., Aarhus, Denmark: The Interaction Design Foundation. Online verfügbar unter https://www.interaction-design.org/encyclopedia/wearable_computing.html, gesehen am 11. März 2015. S. auch Webopedia, “wearable computing”, http://www.webopedia.com/TERM/W/wearable_computing.html) oder dictionary.com, “wearable computer”, http://dictionary.reference.com/browse/wearable+computer).

[3] Donald Melanson and Michael Gorman, “Our augmented selves: The promise of wearable computing.” Engadget. December 12, 2012. Gesehen am 8. Juli 2013.

[4] “Wearable Technology Market - Global Scenario, Trends, Industry Analysis, Size, Share And Forecast, 2012 – 2018.” *Market Research Reports Biz*. January 2013. Gesehen am 13. Juni 2013.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

a) Geräte zur Beobachtung der Fitness, des Wohlbefindens und des Lebens (z.B. smarte Kleidung oder Sportbrillen, Aktivitätsmonitore, Schlafsensoren), die immer beliebter für diejenigen werden, die viele Aspekte ihres Lebens aufzeichnen möchten;[5]

b) Infotainment (z.B. smarte Armbanduhren, Headsets zur „Erweiterung" der Realität (augmented reality), smarte Brillen;[6]

c) Gesundheitsversorgung und medizinische Anwendungen (z.B. dauerhafte Kontrolle des Blutzuckerspiegels, Biosensoren als Pflaster);[7]
und

d) Industrie, Polizei und Militär (z.B. Handterminals, am Körper angebrachte Kameras, Headsets für „erweiterte" Realität).[8]

Die Bereiche c) und d) werden in diesem Arbeitspapier nicht behandelt. Auch wenn dieses Arbeitspapier den Bereich c) – Gesundheitsversorgung und medizinische Anwendungen – nicht behandelt, ist anerkannt, dass Daten im Bereich a) – Fitness, Wohlbefinden und Beobachtung des Lebens – als Gesundheitsdaten angesehen werden können[9].

Das Zeitalter der Wearables schafft neue oder vergrößert bestehende Risiken für die Privatsphäre in der mobilen Umgebung, indem zusätzliche und möglicherweise sensitive personenbezogene Informationen in unauffälliger oder verdeckter Weise gesammelt werden. Informationen in Echtzeit über jemandes Stimmung, körperliche Fitness und Gesundheitszustand unterfallen wahrscheinlich dem Begriff der personenbezogenen Daten. Auch Informationen über eine gesunde Person (z.B. Herzschlag) können als sensitiv angesehen werden. Die Unterschiede zwischen einem Smartphone und vielen anderen tragbaren Geräten (Wearables) sind eher graduell als substanziell, aber es handelt sich um wichtige Unterschiede aus der Sicht des Datenschutzes.

Bei tragbaren Endgeräten scheint die Rechentechnik in der Kleidung, in Brillen und Uhren und schließlich unter der Haut zu verschwinden, wobei viele herkömmliche Hinweise entfallen, die den

---

[5] Emily Waltz, "How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives?" IEEE Spectrum, August 30, 2012. Nachweis bei Steve Mann. "Steve Mann: My "Augmediated" Life." *IEEE Spectrum*. March 1, 2013. Gesehen am 14. Juni 2013.

[6] Zu den Beispielen von Wearables in dieser Kategorie gehören Google Glass (www.google.com/glass/start), Oculus Rift (www.oculus.com, gekauft von Facebook, Google Cardboard (https://developers.google.com/cardboard/), und Samsung's Gear VR (http://www.samsung.com/global/microsite/gearvr/gearvr_specs.html).

[7] Siehe Vital Connect's HealthPatch. Gesehen am 6. Januar 2014.

[8] Kopin's Golden-i-Gerät wird entwickelt, um Live-Video-Streaming, mobilen Internet-Zugang, GPS-Navigation und freihändige Bedienung für Kundendienstmitarbeiter, Polizisten, Notärzte und Feuerwehrleute zu ermöglichen. Weitere Informationen unter www.mygoldeni.com/home/.

[9] Die Art.- 29 Arbeitsgruppe hat festgestellt, dass es bei manchen Datenverarbeitungen bei Gesundheits- und Lifestyle-Apps und –Geräten schwierig sein kann, festzustellen, ob Gesundheitsdaten verwendet werden oder nicht – der sog. Graubereich – vgl. Brief mit Anhang der Art. 29 Arbeitsgruppe an die Europäische Kommission, DG CNECT, zu mHealth vom 5.2.2015; http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf (Brief) und 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(Anhang).

Einzelnen darauf hinweisen, dass solche Endgeräte vorhanden sind und verwendet werden. Dies führt zu einem zunehmenden Transparenzdefizit und erhöht in der Konsequenz die Schwierigkeit für Nutzer und andere Betroffene, informierte Auswahlentscheidungen zu treffen. Außerdem sind viele Wearables mit der Verpflichtung verbunden, mit dem Hersteller der Hardware, des mobilen Betriebssystems oder mit Anbietern von Cloud-Diensten Verbindung aufzunehmen. Dies kann dazu führen, dass der Betroffene die Kontrolle über die gesammelten personenbezogenen Daten verliert.

Es bleibt schwierig, in der Mobilkommunikation mit kleinen Displays und unregelmäßiger Aufmerksamkeit des Nutzers aussagekräftige Informationen über Datenschutz-Einstellungen zu vermitteln. Diese Design-Eigenschaften erhöhen die Schwierigkeit, Nutzern Informationen über ihre Datenschutzrechte, in verständlicher Form und so rechtzeitig zu geben, dass sie informierte Entscheidungen treffen können. Der Einsatz von Wearables verstärkt diese Herausforderungen.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

- Die Verarbeitung personenbezogener Daten in und durch Wearables sollte so transparent wie möglich für den Nutzer und andere Betroffene erfolgen; bei versteckten oder miniaturisierten Geräten sollte Transparenz durch andere als visuelle Mittel sichergestellt werden. Dazu zählt auch die Transparenz der Verbindungen zu Zusatzgeräten wie Smartphones.

- Als Grundeinstellung sollten personenbezogene Daten unter der Kontrolle der Person verarbeitet werden, die das Gerät trägt. Es sollte keine Pflicht zur Herstellung einer Verbindung mit den Servern der Hard- oder Software-Hersteller, zu Plattformen oder Cloud-Diensteanbietern geben.

- Die Übermittlung oder Offenbarung von Daten setzt die klare Signalisierung gegenüber dem Nutzer des Geräts und seine informierte und ausdrückliche Einwilligung voraus.

- Die Rechte des Betroffenen, namentlich die auf Auskunft, Berichtigung und Löschung, sind zu respektieren. Insbesondere sollten Betroffene eine Möglichkeit haben, die Richtigkeit der von dem Wearable erzeugten Daten oder die auf ihrer Grundlage vorgenommene Analyse wirksam überprüfen zu lassen.

- Alle Produkte und/oder Dienste sollten vom Grundsatz der Nutzerkontrolle ausgehen. Dies sollte unter anderem einschließen:

    - Die Möglichkeit, die Funktionalität des Gerätes zu verändern (z.B. indem die Unterhaltung von Audio auf Text umgestellt wird, um den Datenschutz zu erhöhen (dynamische Nutzerkontrolle)).
    - Die Möglichkeit, die Erhebung ihrer personenbezogenen Daten vorübergehend von Fall zu Fall zu stoppen (z.B. für bestimmte Zeiträume und/oder Aktivitäten, in oder bei denen sie nicht beobachtet werden wollen).
    - Die Möglichkeit, die Granularität der Daten auszuwählen oder zu kontrollieren, die verarbeitet oder Dritten übermittelt werden.

- Einzelne sollte die Möglichkeit haben, ihre Zustimmung zur Datenoffenbarung jederzeit zu widerrufen. Sie sollten auch die Wahl haben, zur lokalen Speicherung zu wechseln (z.B. auf einem Smartphone oder einem anderen Gerät unter der Kontrolle des Nutzers) und ihre Daten zu sichern.

- Mittel zur Gewährleistung der Portabilität der Daten sollten bereitgestellt werden.

- Die Nutzung von Wearables am Arbeitsplatz wirft zusätzliche Fragen bezüglich der Wahlfreiheit der Beschäftigten auf. Beschäftigte, die sich gegen die Teilnahme an Programmen unter Einsatz von Wearables entscheiden, sollten deshalb keine Nachteile haben.

- Wenn Daten, die durch oder auf Wearables verarbeitet werden, als Gesundheitsdaten anzusehen sind, sollte ihre Weiterverarbeitung nur mit ausdrücklicher Einwilligung der Betroffenen zugelassen werden.

Zusätzlich zu diesen Empfehlungen unterstützt die Arbeitsgruppe die entsprechende Berücksichtigung der Empfehlungen in der Stellungnahme 8/2014 der Art.29 – Arbeitsgruppe zu neuen Entwicklungen beim Internet der Dinge (WP 223).[10]

Hintergrund zu den Empfehlungen[11]

Eigenschaften des Einsatzes von Wearables

Viele Wearable-Technologien, die gegenwärtig entwickelt werden oder schon auf dem Markt sind, haben verlockende Eigenschaften, die zu breiter Akzeptanz bei den Verbrauchern beitragen könnten. Beispielsweise:

a) sind sie äußerlich ansprechend gestaltet;
b) können sie nahtlos in die Kleidung integriert oder in den Körper des Nutzers implantiert werden;
c) können sie personalisiert und den Bedürfnissen des Nutzers angepasst werden und können Rückmeldungen geben;
d) können dem Nutzer nützliches Feedback geben, entweder in Echtzeit oder nicht, und direkt oder durch ein anderes intelligentes Endgerät (typischerweise ein Smartphone);
e) können die körperlichen oder geistigen Fähigkeiten des Nutzers ergänzen;
f) sind verhältnismäßig preisgünstig für den durch sie erzielten Nutzen;
g) sind handlich und bieten eine große Breite von Einsatzmöglichkeiten im persönlichen Bereich oder am Arbeitsplatz; und
h) sind verhältnismäßig einfach vom Verbraucher einzurichten und zu verwenden.

Ständige Interaktion zwischen dem Nutzer und dem Endgerät, wobei dieses „lernt“, was der Nutzer erlebt, während er es erlebt, und das Darüberlegen zusätzlicher Informationen zu dieser Erfahrung sind ein Ziel der gegenwärtigen Gestaltung von Wearables.

---

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_de.pdf; S. 21 ff.

[11] Dieser Teil beruht weitgehend auf dem in FN 1 genannten Forschungsbericht.

Konsequenzen für den Datenschutz

In einer kürzlich von der Industrie finanzierten Meinungsumfrage zu den Implikationen von Wearables in Großbritannien und den USA nannten 51% der Befragten den Datenschutz als Hindernis für den Einsatz, und 62% waren der Auffassung, dass Google Glass und andere Wearables in irgendeiner Form reguliert werden sollten, während 20% für ein vollständiges Verbot dieser Geräte eintraten. Forrester Research ist zu dem Schluss gekommen, dass das Potenzial der Wearables nur ausgeschöpft werden kann, wenn die Nutzer die Kontrolle über ihre eigenen Daten erhalten, wie beispielsweise entscheiden zu können, ob sie die Daten weitergeben wollen oder nicht.

Herausforderungen für das bestehende Einwilligungsmodell

Informationen, die von Sensoren in miteinander verbundenen Objekten gesammelt werden, sei es, dass diese Objekte von einzelnen Personen getragen oder einfach mitgeführt werden, können eine gewaltige Menge an Daten erzeugen, die verknüpft, analysiert und zur Entscheidungsgrundlage gemacht werden können, ohne dass eine angemessene Transparenz, Verantwortlichkeit oder eine echte Einwilligung gegeben sind.

Diese Entwicklungen stellen grundlegende Herausforderungen für bestehende Datenschutzregeln weltweit dar. So ist es z.B. zunehmend schwierig, den Grundsatz der Zweckbindung, der die Erhebung von personenbezogenen Daten begrenzen soll, soweit nicht die Einwilligung für die Verwendung für bestimmte andere Zwecke vorliegt, in einer Welt von allgegenwärtiger Rechentechnik und mobilen Endgeräten anzuwenden. Darüber bleibt es schwierig, eine wirksame Einwilligung durch mobile Endgeräte einzuholen. Es muss mehr getan werden, um Nutzern in kreativer und aussagekräftiger Weise zu zeigen, was tatsächlich mit ihren personenbezogenen Informationen geschieht.

Neue Überwachungsmöglichkeiten

Einige Wearables sammeln Fotos, Videos, Geräusche, Orte und nehmen die allgemeine Umgebung des Gerätes auf, einschließlich der umstehenden Menschen und benachbarten Geräte. Die in mehreren dieser Wearables enthaltene Kamera wirft zahlreiche Datenschutzfragen auf. Preisgünstige, vielfältige Alltagsgegenstände wie Baseball-Mützen, MP3-Spieler und Hemdknöpfe sind mit versteckten Kameras erhältlich. Viele dieser Gegenstände können permanent und verdeckt aufzeichnen.

Über die Kamera hinaus jedoch ist eine neue Generation von Fitness-Trackertechnologie gerade dabei, Krankenversicherungen und Arbeitgebern neue Einblicke in unseren Gesundheitszustand und unser Verhalten zu geben. Eine Reihe von Versicherungen und Arbeitgebern in Nordamerika nutzen Tracking-Technologie, um ihre Versicherten und Arbeitnehmer zu überwachen und bieten ihnen finanzielle Vergünstigungen als Gegenleistung für Daten über körperliche Aktivitäten an. In Europa beginnen Versicherungen, ähnliche Verträge anzubieten.

Weitere derartige Entwicklungen sind zu erwarten. Der entstehende Bereich der „Physiolytics“[12] wird Wearables mit Big Data-Analysen verknüpfen, um Rückmeldungen und ein Empfehlungssystem für Verhaltensänderungen anzubieten.

Die Aggregierung von durch Wearables erhobenen Daten

Wir werden Zeugen einer neuen Generation von Herausforderungen für den Datenschutz, die aus der Verknüpfung von scheinbar belanglosen und nicht-sensitiven Splittern von personenbezogenen Informationen zur Ableitung von Einsichten in persönliches Verhalten entstehen. Wir wissen auch,

[12] H. James Wilson, Wearables in the Workplace, Harvard Business Review, September 2013, https://hbr.org/2013/09/wearables-in-the-workplace/ar/1

dass die Verknüpfung von unzusammenhängenden Informationspartikeln, die aus verschiedenartigen Quellen gewonnen werden, zur Bildung detaillierter Profile führen kann, die einzelnen Personen zuzuordnen sind. Es ist bereits schwierig für Einzelne, informierte Entscheidungen darüber zu treffen, ob sie personenbezogene Informationen offenbaren wollen, weil sie nicht völlig absehen können, wie ihre Informationen zukünftig verknüpft und verwendet werden können. Wearables, die ständig Daten sammeln, verarbeiten und versenden, werden dieses Problem wahrscheinlich noch verschärfen.

Beschleunigung des Kontextverlusts

Menschen versuchen möglicherweise, die verschiedenen Bereiche ihres Lebens, seien es verschiedene soziale Zusammenhänge, in denen sie sich befinden, oder einfach Beruf und Privatleben, voneinander getrennt zu halten. Soziale Medien und die Online-Umgebung haben allgemein unsere Fähigkeit beeinträchtigt, diese Unterscheidung aufrechtzuerhalten. Diese Auflösung, die Sozialwissenschaftler als „Kontextverlust" bezeichnen, könnte beschleunigt werden durch Sensoren, die immer eingeschaltet sind und ständig mit dem Körper des Nutzers und anderen Geräten in der Umgebung des Nutzers interagieren.

Neue Methoden der Authentisierung, neue personenbezogene Informationen

Der Einsatz von Wearables kann so gestaltet werden, dass personenbezogene Informationen datenschutzgerecht und sicher verarbeitet werden. So wird gegenwärtig in Forschungsprojekten untersucht, wie Daten, die von Sensoren in gegenwärtig verfügbaren Smartphones erzeugt wurden, zur Identifikation und Authentisierung von Personen genutzt werden können, die ihr Smartphone bei ihren täglichen Aktivitäten bei sich führen.

Das bedeutet, dass bereits das Gehen, Joggen, Klettern und das Hinabgehen von Treppen mit einem Smartphone in der Tasche biometrische Signaturen des Nutzers erzeugen können. Obwohl dies die Sicherheit durch Authentisierung des Nutzers verbessern kann, führt es gleichzeitig zu neuen Risiken für die Privatsphäre.

Design-Überlegungen

Dynamische Nutzer-Kontrolle

Gegenwärtige Überlegungen zum Begriff der Privatheit legen es nahe, sie als einen dynamischen Zustand zu begreifen, weil die soziale und kulturelle Umgebung des Einzelnen sich ständig ändert. Eine Konstellation kreativer Auswahlmöglichkeiten sollte untersucht werden, um der Einwilligung abhängig von den jeweiligen Umständen und Vorlieben mehr Bedeutung zukommen zu lassen und um ein Übermaß an Auswahlentscheidungen bei der Nutzung von Wearables zu begrenzen. So sollten beispielweise Vorarbeiten geleistet werden, um

a) dynamisch kalibrierte Datenschutzregeln zu entwickeln, um den Bedürfnissen und Erwartungen Betroffener bezüglich des Datenschutzes zu entsprechen;

b) einfache Gestaltungselemente zu integrieren, so dass das tragbare Gerät (Wearable) die Datenschutzpräferenzen des Einzelnen widerspiegeln kann;

c) um verantwortliche Stellen dazu aufzufordern, ihre Datenschutzerklärungen um dynamische und interaktive Datenkarten und Infografiken zu erweitern, um die Beziehungen im Ökosystem der Wearables zu verdeutlichen.

Die Gestaltungsanforderungen für die Interaktion mit dem tragbaren Gerät werden Einfluß auf den Datenschutz des Nutzers haben. So führt die Nutzung eines Wearable mittels Sprachsteuerung zu ähnlichen Datenschutzproblemen wie ein in der Öffentlichkeit geführtes Telefonat. Die Möglichkeit des Nutzers zur Verhaltensänderung, vielleicht durch Umstellung der Unterhaltung von Sprach- auf Textkommunikation, wäre eine interessante Anpassung des Designs zur Verbesserung des Datenschutzes.

Entstehende Transparenz-Modelle

Es gibt beim Einsatz von Wearables Chancen und Herausforderungen für die Transparenz. So können Wearables, die die Sehkraft, das Gehör oder andere Sinne nutzen, enger mit dem Nutzer verbunden werden, so dass es in gewisser Weise leichter sein kann, die unmittelbare Aufmerksamkeit des Nutzers zu gewinnen. Auf diese Weise kann es leichter sein, Zustimmung und Information zum inneren Bestandteil des Designs eines Wearables zu machen als bei einem Smartphone. Die Gestaltung mancher Wearables setzt überhaupt keine Displays voraus, deshalb müssen neue Verfahren zur Aushandlung von Privatheit entwickelt werden.

Der Datenschutz der Nutzer ist eine Seite, aber der Datenschutz der Menschen in der Umgebung des Nutzers ist ein anderes und vielleicht schwierigeres Problem. Es ist bereits schwierig zu wissen, wann jemand ein Smartphone oder anderes Gerät zur Aufnahme von Ton oder Bild benutzt. Im Fall von Wearables, bei denen die Computer noch nahtloser in belanglose Gegenstände integriert werden, wie Gestelle für alltägliche Brillengläser, wird die Fähigkeit anderer, die Sammlung von Daten über sie zu bemerken oder zu kontrollieren stark reduziert.

Auskunft über Daten und Kontrolle der Richtigkeit bei automatisierten Entscheidungen

Die Frage der Auskunft über personenbezogene Daten ist direkt mit der Transparenz verbunden. Es ist nicht offensichtlich, wie Betroffene feststellen können, was durch ein Wearable erhoben wird, von wem es erhoben wird und wie es genutzt und weitergegeben wird. Nutzer müssen die Möglichkeit haben, die von Institutionen als Grundlage für deren Entscheidungen gesammelten Informationen zu überprüfen, da deren Richtigkeit nicht garantiert ist.

Eine neuere Untersuchung einiger fitness-bezogener Wearables bezweifelte die Zuverlässigkeit der Messung des Kalorienverbrauchs bei wenig intensiven Tätigkeiten wie Stehen oder Saubermachen. Ungenauigkeiten bei der Erhebung solcher Daten können reale Folgen für die Nutzer dieser Geräte haben. Beispielsweise können ungenaue Messergebnisse einer neuen Methode zur Früherkennung von Alzheimer, bei der die Bewegungen von Patienten mit einem Beschleunigungsmessgerät bewertet werden, die Diagnose und Versorgung des Patienten beeinflussen. Ungenaue Messergebnisse können auch Probleme am Arbeitsplatz auslösen, wenn ein Arbeitgeber sich auf solche Geräte bei der Messung der Produktivität des Arbeitnehmers verlässt. Es wäre ein wichtiges Element der Gestaltung von Wearables, wenn die Betroffenen die Möglichkeit haben, die Richtigkeit der mit solchen Geräten erhobenen Daten oder der darauf basierenden Analyse wirksam zu überprüfen.

Sicherheitslücken

Wearables ohne angemessene Sicherheits- und Authentisierungssysteme sind angreifbar. Kompromittierte Geräte können nicht nur die personenbezogenen Informationen und den Ruf eines Nutzers gefährden, sondern auch seine Gesundheit. So könnte etwa das Abhören oder das Simulieren einer Insulin-Pumpe gravierende Folgen für die Gesundheit des Einzelnen haben. Wie ein Kommentator formulierte, „ist die Sicherheit Deiner persönlichen Daten nur so stark wie das schwächste Glied im Öko-System Deiner Selbstvermessung.“