Preprint. Erscheint als: Langheinrich, M., Schaub, F., & Karjoth, G. (2016). Selbstvermessung oder Selbstüberwachung? *Digma – Zeitschrift Fuer Datenrecht Und Informationssicherheit*, *16*(2), 50–56.

Selbstvermessung oder Selbstüberwachung?

Sicherheits- und Datenschutzbedenken beim Quantified Self

Während für die Mehrheit der Nutzer von *Quantified Self*-Apps und -Geräten diese heutzutage noch eher spielerischen Charakter haben, birgt die "Vermessung des Ichs" das Potential für neuartige Datenschutz- und Sicherheitsbedenken: Wer vermisst wen? Wer wertet was wie aus? Und wie kann ich sicher sein, woher meine Daten stammen?

I. DAS VERMESSENE ICH

Beim Quantified Self (QS) Ansatz geht es darum, alltägliche Handlungen detailliert zu protokollieren um so, quasi als "Big Picture", mittels statistischer Analyse Zusammenhänge und Trends im eigenen Verhalten zu erkennen, getreu der alten Management-Weisheit "You can't manage what you can't measure." Ähnlich wie eine Zeitraffer Kamera lassen sich so Prozesse, die man selbst nur schwer beobachten kann, sichtbar machen. Wie so oft gilt auch hier meist die Devise "Viel hilft viel" des "Big Data"-Ansatzes: je mehr Puzzlestücke ich sammeln kann, desto detaillierter wird mein Bild, desto mehr Einblicke lassen sich (hoffentlich) generieren. Und auch falls bestimmte Daten heute noch nicht verwertbar sind, so ermöglicht deren Erfassung womöglich eine Auswertung zu einem späteren Zeitpunkt.

QS-Geräte und -Anwendungen sollten daher prinzipiell alles erfassen, was einmal für den Nutzer von Interesse sein könnte – und tatsächlich scheint es für so ziemlich alles bereits eine App bzw. ein Gerät (zumindest einen Prototyp) zu geben:[1] Von Schritte- und Aktivitäts-Trackern, wie etwa Fitbit, Apple Watch oder Schritteerfassung über das Smartphone; der bekannten Withings "Smart Body Analyzer" Waage, die das Gewicht protokolliert; über den *Brain Activity Tracker* "Insight" der Firma Emotiv, der einem dabei hilft seine "cognitive health" zu überwachen, um so die "fitness & performance" seines Gehirns zu verbessern; bis hin zum Autodietary Prototyp von Forschern der Northeastern University welcher beim Essen zuhört und so erfasst, was und wieviel gegessen wird. Software-Tracker wie ManicTime und RescueTime bieten eine detaillierte Erfassung der Zeit die am Bildschirm verbracht wird. Startups wie "Human API" und "Fitabase" bieten darüber hinaus "meta-tracking" Dienste an, d.h. die Integration mehrerer Datenströme von den unterschiedlichsten Geräten. Für viele ist bereits heute Facebook ein detailliertes digitales Tagebuch – Journal-Dienste wie Day One, Diaro, oder Momento erlauben darüber hinaus die Integration mehrer Datenquellen mit manuellen Annotationen, für eine noch detailliertere Protokollierung des Alltags.

QS-Daten liefern so die Grundlage für eine Vielzahl möglicher Anwendungen, allen voran Motivationsanwendungen zur Verhaltensänderung: gesünder Leben, effektiver Arbeiten oder sparsamer Haushalten. Aber auch "dienstliches" Tracking ist verbreitet, gerade bei Selbständigen, die so besser erfassen können für welchen Kunden wieviel Arbeit geleistet wurde. Grosse Firmen sollen damit die Gesundheit ihrer Mitarbeiter fördern können – und nebenbei auch deren Effizienz im Job steigern helfen.[2] Im Gesundheitsbereich kann QS gezielt für Behandlungen genutzt werden,

---

[1] Die QS-Community Website http://lifestreamblog.com/lifelogging/ listet 35 Geräte, 42 Apps, 12 Web Services, and 21 Integrationsplatformen auf

[2] http://www.fitbit.com/fitbit-wellness: "Nutze das Potenzial der marktführenden Fitness-Tracker, um ein attraktives Gesundheitsprogramm anzukurbeln. Fitbit Wellness bietet unabhängig von der Größe oder Kultur deines Unternehmens flexible und spannende Möglichkeiten, gesundheitsbewusstes Verhalten zu fördern, Mitarbeiter für Fitness zu begeistern und Kosten zu reduzieren…. Fitbit Wellness ermöglicht es dir, die

damit Ärzte fundiertere Grundlagen für die Diagnostik erhalten. Nicht zuletzt ist natürlich auch die soziale Interaktion eine starke Triebkraft, wie das stetige "self-tracking" durch Check-ins und Postings auf Sozialen Netzwerken zeigt. Aggregiert auf Länder und Kontinente können QS-Daten neue Einblicke in die öffentlichen Gesundheit ermöglichen. So war QS-Anbieter Jawbone in der Lage, bei einem mittelschweren Erdbeben im Jahr 2014 im kalifornischen Napa-Valley zu beobachten, wieviele Nutzer durch das Erdbeben aufwachten und dass über 50% aller Nutzer im Erdbebengebiet nach dem Beben für mehrere Stunden nicht zurück in den Schlaf fanden.[3]

Gerade letzteres Beispiel zeigt das Potenzial von QS-Applikationen und -Geräten, aus den aufgezeichneten Daten weiteres Wissen zu generieren – aus dem Schlafverhalten einzelner lassen sich (in nahezu Echtzeit) Rückschlüsse über die Volksgesundheit ziehen. Und laut QS-Aktivist und Arzt Mark Leavitt kann die Herzfrequenzvariabiliät Aussagen über die momentane Willenstärke einer Person treffen.[4] Eine einfache App mit der man das abendliche Jogging mitprotokolliert erlaubt es dem App-Anbieter, nicht nur die gelaufene Distanz und exakte Strecke zu sehen, sondern bei regelmässigem Einsatz auch die bevorzugten Zeiten in der Woche für den Workout, den exakten Wohnort, sowie Abwesenheiten (z.B. während eines Urlaubs). Dies mag beim Teilen solcher Daten mit einem QS-App-Anbieter nicht dieselben Konsequenzen haben wie die berühmte "pleaserobme.com" Webseite, bei der öffentliche Twitter Feeds und Posts in Sozialen Netzwerken wie Forsquare dazu genutzt wurden, die Abwesenheit von Nutzern auf einer Karte zu visualisieren, um so hypothetischen Einbrechern die Arbeit zu erleichtern. Doch wenn die Daten Rückschlüsse über den aktuellen oder zukünftigen Gesundheitszustand erlauben, oder Vorhersagen über Aktivitäten und/oder Verhalten ermöglichen, dann ist deren Implikationen für unser Privatleben womöglich noch weitaus grösser als ein einfacher Einbruch es jemals sein könnte.

II. QUANTIFIED-SELF TECHNOLOGIE

Wie oben geschildert ist die Bandbreite an QS-Geräten und -Applikationen enorm. Es gibt daher keine dominante Technologie, die in der Mehrheit der QS-Anwendungen zum Einsatz kommt. Grundsätzlich von Interesse für die Betrachtung von Sicherheit und Datenschutz sind allerdings drei grundlegende Komponenten: die Sensorik (Was wird wie gemessen?); die Datenübertragung (Wie und zu wem werden die gemessenen Daten übermittelt?); und die Datenspeicherung (Wo werden die Daten gespeichert und wer hat Zugriff darauf?).

Sensorik

Die vielleicht populärste (und womöglich auch problematischste) Gruppe von QS-Anwendungen sind solche, die körperbezogene Daten erfassen. Die dazu nötigen Geräte können als portabel (Smartphone), tragbar (Fitnessarmband) oder implantierbar unterschieden werden, wobei der Unterschied zwischen den ersten beiden Gruppen fliessend ist. Ein heute gebräuchliches Smartphone besitzt eine Reihe von mikroelektromechanischen Systemen (MEMS), die eine

---

Entwicklung einzelner Mitarbeiter, des Teams und des gesamten Unternehmens im Auge zu behalten. Dank persönlicher Dashboards können die Teilnehmer detaillierte Zusammenfassungen ihrer Statistiken, eine Liste persönlicher Erfolge und ein Diagramm einsehen, in dem ihre Leistung mit der ihrer Gruppe oder des gesamten Unternehmens verglichen wird."

[3] Jawbone tracking sleep at 2014 CA Earthquake: https://www.washingtonpost.com/news/the-intersect/wp/2014/08/25/what-personal-fitness-trackers-like-jawbone-tell-us-about-earthquakes-public-health-and-just-about-anything-else/

[4] http://quantifiedself.com/2016/04/mark-leavitt-daily-hrv-measure-health-willpower/

bestimmte Umweltbedingung messen, z.B. die Beschleunigung, Rotation, Luftdruck, Temperatur, Feuchtigkeit, Helligkeit oder das Magnetfeld. Ergänzt werden diese Funktionen durch Geräte zur Ortung per GPS, Mobilfunk und WLAN. Ferner können über Mikrofon und Kamera Signale erfasst werden, die eine weitere Auswertung erlauben. Beispielsweise lässt sich durch Auflegen eines Fingers auf die Smartphone-Kamera zuverlässig der Puls bestimmen; Fitnessarmbänder und Smartwatches bieten hingegen den Vorteil, dass sie den Puls kontinuierlich überwachen und aufzeichnen können.

Smartphone-Apps und direkt am Körper tragbare Geräte wie Armbänder oder Brustgurte (auch im Deutschen oft mit dem Englischen "Wearables" bezeichnet) können diese MEMS zum Messen der Aktivitäten und das Befinden des Körpers verwenden. Ein dreiachsiger Beschleunigungsmesser reicht bereits aus, um komplexe Ereignisse wie etwa die zurückgelegten Schritte, das Ersteigen von Stockwerken, sowie das Schlafverhalten zu erfassen. Wearables sind klein, besonders geschützt gegen Schweiss, Regen und Wasserspritzer, und müssen oft erst nach mehreren Tagen wieder aufgeladen werden. Eventuell sind auf einem kleinen Display die aktuellen Werte oder zumindest der Fortschritt ablesbar. Im Speicher können oft mehrere Tage voller detaillierter Bewegungsdaten im Minutentakt aufgezeichnet werden, dazu die Gesamtwerte vergangener Wochen. Die Präzision der erfassten Aktivitäten wird in wissenschaftlichen Untersuchungen als "moderat genau" (10 % oder mehr Abweichung) bezeichnet, wobei es weniger auf den Sensor und das Analyseverfahren als auf den Trageort (Arm oder Hüfte) anzukommen scheint. Sportartikelhersteller bieten T-Shirts und Trainingsschuhe an, die direkt mit solchen Sensoren ausgestattet sind. Bereits an der WM 2014 waren mehrere Teams, darunter auch die Deutsche Mannschaft, mit solchen "Smart Shirts" ausgestattet.

Datenübermittlung

Wearables werden typischerweise drahtlos (meistens Buetooth Low Energy) mit einem Smartphone gekoppelt, wo eine App die Daten entgegen nimmt. Ob diese App die Daten auf dem Smartphone speichert und dort auch auswertet oder sie "nur" in die Cloud schickt, hängt manchmal von technischen Rahmenbedingungen ab, oft aber auch einfach vom Geschäftsmodell des Anbieters. So speichert beispielsweise die Lifelogging-Kamera "Narrative Clip" zu jedem automatisch geschossenen Foto auch Ortsinformationen in Form von GPS-Signalen. Da die Gewinnung von Längen- und Breitengrad aus GPS-Rohdaten allerdings zusätzliche Rechenenergie benötigt, stellt die Kamera diese Funktionalität gar nicht erst zur Verfügung (zwecks Energieeinsparung) und überlässt es dem Cloud-Service der Firma, diese Ortsdaten aus den Rohdaten zu berechnen. Wer seine Bilder nicht in die Cloud laden will muss daher ohne Ortsdaten auskommen.

Die ausgewerteten Daten werden typischerweise in einfach zu lesenden Grafiken und Tabellen dargestellt. Die Anbieter von Fitness-Apps ermöglichen beispielsweise das Protokollieren des Trainings, sowie die Erstellung eines Trainingskalenders, um Trainingsfortschritt und Kartenrouten aufzuzeichnen. Zur Förderung der Motivation kann Freunden und Familie Einsicht in diese Daten gegeben werden, um in einer Bestenliste gegeneinander anzutreten oder zumindest den Fortschritt zu kommentieren. Es können Ziele festgelegt werden, die bei Fortschritten zur Erreichung durch Nachrichten und Abzeichen belohnt werden. Bei eher gesundheitsorientierten Anwendungen sind es Gesundheitsziele, die festgelegt und verfolgt werden können (z.B. ein Zielblutdruck, -gewicht oder -glucosewert); das Teilen erfolgt mit Ärzten bzw. Gesundheitszentren aber auch mit Familienmitgliedern.

Datenauswertung

Die direkt gemessenen Daten sind meist nur ein erster Schritt – erst die (oft komplexe) Analyse der Daten bzw. das Zusammenführen mehrerer Sensordatenströme bringt "Interessantes" zu Tage. Bei

Fitness-Apps ist dies z.B. das Auswerten von GPS und Beschleunigungssensor, welches die Erfassung unterschiedlicher Aktivitäten ermöglicht (Laufen oder nur Gehen; Fussball spielen; Sitzen und Sitzhaltung; etc.). Benutzer können die Datensammlung durch eigene Angaben, z.B. über ihr Gewicht, Nahrung und Getränkeeinnahme ergänzen. Auf der Webseite des Hersteller sind meist Zusatzfunktionen verfügbar, z.B. das Setzen von Zielen, das Formen von Freundeskreisen, oder manuelle Annotation von Sensordaten. Zugriff auf die Daten und Auswertungen ist (häufig) nur über die Website des Herstellers möglich, bzw. direkt in der Smartphone-App. Bei manchen Herstellern ist der Zugriff auch über eine dokumentierte Programmierschnittstelle (API) möglich, so dass individuelle Auswertungen entwickelt werden können. Die digitalen Rohdaten, die ein QS-Dienst gesammelt hat, können bei manchen Anbietern durch ein solches API zu anderen Diensten übertragen bzw. zur eigenen Speicherung heruntergeladen werden. Integrationsplatformen wie die oben erwähnten Day One nutzen solche APIs, um Datenströme verschiedener Anbieter zusammenzuführen. Zugriff wird zum Beispiel mit dem OAuth 2.0 Authorization Framework realisiert, welches der Anwendung einer dritten Partei kontrollierten Zugang zu einem HTTP-Dienst ermöglicht. Diese kann generell Erlaubnis bekommen oder es wird eine Interaktion ausgelöst, in der der Ressourcenbesitzer seine Zustimmung geben kann. Die im Web bereits beliebte Vereinfachung des Anmeldevorgangs bei einem Service über den bereits bestehenden Social Media Account (z.B. Facebook oder Google) birgt hier besondere Risiken, da so auch diese Anbieter über Zugriffe (wenn auch nicht aber über die übermittelten Daten) informiert werden.

III. RISIKEN FÜR SICHERHEIT UND DATENSCHUTZ

Für QS-Daten gibt es drei Risikobereiche [Symantec]: (i) ihre Speicherung auf dem Gerät bei der Datenerfassung, (ii) in der Übertragung dieser Daten und (iii) ihrer endgültigen Speicherung und Analyse in der Cloud.

Angriffe auf Datenübermittlung und -speicherung

Um Daten direkt von einem Wearable abgreifen zu können, müsste der Angreifer wegen der geringen Sendeweite in die Nähe des Gerätes kommen. Darüber hinaus bietet der oft eingesetzte Funkstandard Bluetooth eine Basisverschlüsselung, allerdings muss diese vom Entwickler explizit aktiviert werden. Bei der Speicherung auf einem Smartphone, Tablet oder PC sind die Daten in der Fitness-App allerdings – wie alle anderen Apps auch – einem potentiellen Zugriff durch Malware ausgesetzt. Dies betrifft aber nur die Daten einer Person und meistens nur über einen begrenzten Zeitraum. Schutzmassnahmen werden vom jeweiligen Betriebssystem übernommen (Sandboxing, Zugriffskontrolle und Verschlüsselung bei Verlust oder Diebsstahl). Bei der Übertragung der Daten in die Cloud können die üblichen Sicherheitstechniken wie Authentifikation und Verschlüsselung Angriffen entgegen wirken – ob der jeweilige Anbieter diese korrekt umsetzt bzw. überhaupt implementiert (unverschlüsselte Verbindungen sind leider immer noch keine Seltenheit) ist natürlich eine andere Sache. Sind die Daten in einer Datenbank in der Cloud angekommen, bestehen die üblichen Risiken durch SQL Injection, schlecht geschützte Passwörtern, Software- und Systemangriffen. Der Angreifer kann entweder das Konto eines Benutzers knacken oder sich Zugang zu der ganzen Datenbank verschaffen. Diese sind ein lukratives Ziel, insbesondere wenn die erfassten Daten noch mit anderen Daten wie Kreditkarten-Informationen verknüpft sind. Diese Art von Gefahren sind grundsätzlich nicht neu, dennoch ist abzusehen, dass umfangreiche QS-Datensammlungen, vor allem von Aggregationsdiensten die Daten von mehrere QS-Applikationen zusammenfassen, lohnende Angriffsziele darstellen.

Risiko Mehrwertdienste

Je nachdem wie die QS-Daten verwaltet werden, können andere Personen bzw. Firmen Zugang zu ihnen bekommen, z.B. indem sie in aufbereiteter Form verkauft werden – abhängig vom

Geschäftsmodell des QS-Anbieters. Sobald Benutzer ihre Daten zu einem Online-Cloud-Service zur Speicherung, Analyse und Social Sharing hochladen, haben sie meist nur noch wenig Einfluss auf die weitere Verwendung dieser Daten. Da Auswertung und Aufbereitung der Daten bei den meisten QS-Anbietern grundsätzlich nur über einen solchen Cloud-Account angeboten wird, ist eine lokale Analyse durch den Nutzer meist nicht oder nur eingeschränkt möglich – die "kostenlose" Nutzung solcher Online-Dienste ist somit oft der einzige Weg, das Potenzial einer QS-Anwendung bzw. eines QS-Geräts auszuschöpfen.

Sind sozialen Medien integriert und eine API ermöglicht Drittentwicklern, Anwendungen zu erstellen, die diese Daten verwenden, können schnell interessante Mehrwertdienste angeboten werden (z.B. das Anfeuern in Echtzeit durch den Freundeskreis während einer sportlichen Betätigung, die "live" geteilt wird). Solche Mehrwertdienste machen es allerdings für den Einzelnen auch zunehmend schwieriger abzuschätzen, welche Firmen und Personen schlussendlich Zugriff auf diese Daten haben. In jedem Fall schaffen solche Dienste Anreize, mehr und mehr seiner Daten mit anderen zu teilen. Auch bieten viele QS-Anbieter Benutzern die Möglichkeit, sich statt eines neuen Accounts einfach mit einem existierenden Facebook-, Google- oder Twitter-Account anzumelden. So werden Soziale Netzwerkdienste, die bereits heute eine Vielzahl persönlicher Daten sammeln und diese zu Marketingzwecke nutzen, ebenfalls Teil der "QS-Wertschöpfungskette". Wie bereits bei Webdiensten im Allgemeinen bekannt, helfen Datenschutzerklärungen Benutzern hier kaum, auch nur im Ansatz zu verstehen, welche Daten wie mit wem geteilt werden [Reidenberg]. Auch ist die datenschutzrechtliche Lage von QS-Anwendungen oft unklar – während z.B. in den USA Gesundheitsdienste stark reguliert sind (e.g., HIPAA) sind QS-Anwendungen nicht zwangsläufig als solche klassifiziert. Eine kürzlich in Deutschland vom Bundesministerium für Gesundheit in Auftrag gegebene Studie [CHARISMHA] kommt zum Schluss, dass Gesundheits-Apps (zu denen auch QS-Anwendungen zählen) zwar ein erhebliches Potenzial zur Steigerung der Volksgesundheit im Allgemeinen als auch zur individuellen Patientenversorgung im Speziellen besitzen, diese jedoch ohne zusätzliche (sanfte) Regulierung erhebliche Risiken bergen. Auch in der Schweiz ist der rechtliche Rahmen solcher Anwendungen noch ungeklärt (siehe auch Gordon et al. "Erkenntnisgewinn über Selbstvermessung" in dieser Ausgabe).

Gesellschaftliche Risiken

Die zunehmende Verbreitung und Akzeptanz von QS-Anwendungen, vor allem auch im Gesundheitsbereich, bietet zusätzliche gesellschaftliche Risiken. So bieten etwa Krankenkassen schon heute vermehrt Bonusprogramme an, die Versicherte zu einem gesünderen Lebensstil bewegen sollen. QS-Anwendungen können hier zusätzliche Motivation bieten – erste Krankenkassen in Deutschland subventionieren bereits den Kauf von Pulsmesser und Smartwatch, während Krankenkassen in den USA bereits Discounts für das Übermitteln von Schrittdaten und das Erreichen von täglichen Schritt-Zielen anbieten. In der Schweiz hat die CSS im letzten Jahr ein ähnliches Pilotprojekt lanciert, bei dem Versicherte einen Pulsmesser tragen und dessen Daten an die CSS übermitteln. Ähnlich wie Autoversicherer mittels prämienreduzierender Blackbox Kunden unterschwellig zu einer sichereren (sprich: kostengünstigeren) Fahrweise erziehen wollen, könnte das Nichttragen von QS-Geräten bald teurere Krankenkassenprämien nach sich ziehen. Solch eine Entwicklung würde auf technischer Ebene die Manipulation solcher Daten noch vor der Übermittlung zum Versicherer lukrativ machen.

IV. FAZIT

Quantified Self ist nicht nur das Sammeln von Daten über das eigene Verhalten oder den eigenen Körper, sondern vor allem auch das Auswerten und Aufbereiten dieser Daten um Erkenntnisse abzuleiten. Heute gibt es allerdings wenig Möglichkeiten für Individuen ohne weitreichende

Programmierkenntnisse, dies selbst zu tun – stattdessen gibt es einen grossen Markt für Dritte, und insbesondere auch für Gerätehersteller von Fitness- und Aktivitätstrackern, diese Auswertung für den Nutzer zu übernehmen und dabei von den Daten aller Kunden zu profitieren. Auch wenn QS-Technologien darauf abzielen das Verständnis des *eigenen* Körpers und Verhaltens zu verbessern, ziehen die gesammelten QS-Daten somit weite Kreise. Sie stehen eben nicht nur einem selbst zur Verfügung sondern auch einer ganzen Reihe von anderen Akteuren. Die Schattenseite dieses "QS-Ökosystems" ist, dass QS-Anbieter oft nachweiteren kommerziellen Verwertungsmöglichkeiten suchen um ihre kostenfreien Dienste zu monetarisieren.

Wo ist die Grenze zwischen Selbstvermessung und Überwachung?

Einmal gesammelte QS-Daten werden selten bis nie gelöscht. Die Langzeitfolgen dieser freiwilligen kontinuierlichen Sammlung von detaillierten Verhaltens- und Gesundheitsdaten und deren Speicherung bei Cloud-Anbietern – die oft aus den USA operieren – sind jedoch schwer abschätzbar. Es ist nicht ausgeschlossen, dass diese Daten später von Firmen (Krankenkassen, Versicherungen, Arbeitgeber)[5] oder Behörden (Strafverfolgungsbehörden, Gerichte)[6] eingefordert werden.

Die Grenzen zwischen Selbstvermessung und Überwachung sind bei QS-Daten daher nicht klar verortbar. Viele der heute bereits gesammelten QS-Daten ermöglichen Rückschlüsse über Bewegungsmuster, Gesundheitszustand, Reaktionszeit und Auftreten. Daten, die heute als unverfänglich betrachtet werden, können morgen als Grundlage zur Bestimmung psychischer Störungen herangezogen werden. Hier sind aber die Grenzwerte, was noch als "normal" betrachtet wird, noch ungenauer und stärker den Zeitströmungen unterworfen. Auch aus entwicklungspsychologischer Sicht ist es fraglich, ob Dauervermessung und damit einhergehende Vergleiche mit anderen bei Heranwachsenden zu Stress (Angst, nicht zu passen, nicht Normal zu sein) bzw. auch zu einer gesellschaftlichen Normierung führen.

Was ist zu tun?

QS-Anbieter soltlen ihren Kunden klarer verdeutlichen welche Akteure Zugriff auf gesammelte QS-Daten haben und mit wem diese Daten ggf. unter welchen Umständen wie geteilt werden. Weiterhin sollten Kunden Möglichkeiten eingeräumt werden bestimmten Nutzungen und Weitergaben gezielt zu widersprechen, bzw. potentiell unerwartete Praktiken sollten dem 'Opt-In'-Prinzip unterliegen. Statt derartige Praktiken nur in Allgemeinen Datenschutzbestimmungen darzulegen, sollte eine gezielte Einwilligung oder Widerspruch von Nutzern eingeholt werden – zu dem Zeitpunkt wenn die Nutzung oder Weitergabe stattfindet.

Auch eine Normierung von Datenschutzbedingungen und wie diese dem Nutzer kommuniziert werden ist erstrebenswert um einen Vergleich zwischen den Praktiken verschiedener Anbieter zu erleichtern. Nutzern sollte es außerdem möglich sein alle bei einem QS-Anbieter gesammelten Daten zu exportieren und komplett zu löschen, um so im Falle von Unzufriedenheiten einen Wechsel zwischen QS-Anbietern zu erleichtern – dies bedeutet auch, dass der Kauf eines QS-Gerätes nicht mit dem Zwang verbunden sein sollte die QS-Plattform des Geräteherstellers nutzen zu müssen.

Mögliche Gefahren von QS-Daten müssen auch klarer an Kunden und Verbraucher vermittelt werden. Es benötigt speziell auf QS-Daten zugeschnittene Visualisierungen und

---

[5] http://www.zdnet.de/88214397/gesundheitsdaten-per-fitness-tracker-die-deutschen-krankenversicherer-planen/

[6] http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/

Informationsmaterialien, die die Aussagekraft von QS-Daten für Dritte besser für Verbraucher demonstrieren und potentielle Risiken verdeutlichen.

Vielleicht sollten QS-Daten auch als sensible Gesundheitsdaten betrachtet und entsprechend durch Regulierung und Auflagen geschützt werden. Dies könnte den Schutz vor Missbrauch und erwünschter Zweitnutzung erhöhen, muss aber auch dem Einsatzzweck gerecht werden. In den USA sind mobile Gesundheits-Apps, jenachdem welche Daten sie sammeln und wie sie sie aufbereiten, an verschiedenste gesetzliche Vorgaben gebunden.[7] Beispielsweise werden Apps die weitreichende Auswertungen und medizinische Diagnose anhand von gesammelten Daten anstellen als medizinische Geräte ("medical devices") eingestuft und benötigen somit die Genehmigung der US-Gesundheitsbehörde FDA bevor sie veröffentlicht oder verkauft werden dürfen – ein Prozess der kosten- und zeitintensiv ist und somit kleinere Firmen potentiell benachteiligt. Zertifizierung bestimmter Teilaspekte könnte einen sinnvollen Kompromiss zwischen Verbraucherschutz und Firmenbedürfnissen darstellen. Denkbar wären beispielsweise Gütesiegel für Sicherheit und Datenschutz oder aber auch ein Gütesiegel für die Qualität und Verlässlichkeit von Auswertungen und Gesundheitstipps.

Gleichzeitig ist eine intensivere gesellschaftliche Debatte notwendig darüber inwiefern das Potenzial der Nutzung von QS-Daten über die persönliche Selbstvermessung und -verbesserung hinaus, z.B. im Gesundheitswesen oder der Versicherungswirtschaft, mit Risiken für die Privatsphäre vereinbar ist und wie technische Lösungen und Gesetzgebung gestalten werden sollten um eine derartige Nutzung bei gleichzeitiger Respektierung der Privatsphäre zu ermöglichen.

Literatur

- Chancen und Risiken von Gesundheits-Apps (CHARISMHA); engl. Chances and Risks of Mobile Health Apps (CHARISMHA), Albrecht, U.-V. (Hrsg.), Medizinische Hochschule Hannover, 2016. Urn:nbn:de:gbv:084-16040811153. http://www.digibib.tu-bs.de/?docid=00060000. Siehe http://www.charismha.de/
- Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen! Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder Schwerin, den 6./7. April 2016. Siehe https://www.datenschutz-mv.de/
- Davies, N., A. Friday, S. Clinch, C. Sas, M. Langheinrich, G. Ward, and A. Schmidt. 2015. January. "Security and Privacy Implications of Pervasive Memory Augmentation." *IEEE Pervasive Computing,* Special Issue on Pervasive Security and Privacy, January. http://recall-fet.eu/wp-content/uploads/2014-Davies-RecallSecurityPrivacy-IEEEPervasive.pdf
- Barcena, B. M., C. Wueest und H. Lau. 2014. "How safe is your quantified self? - Symantec?" Symantec.
- Knorr, K.: Datensicherheit bei mHealth-Apps. digma 2015.4, S. 162-165
- Reidenberg, J. R., T. D. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. M. McDonald, T. B. Norton, R. Ramanath, N. C. Russell, N. Sadeh, and F. Schaub. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. Berkeley Technology Law Journal, 30(1):39–88, 2015.

[7] Die Federal Trade Commission bietet eine interaktive Webseite an mit der App-Entwickler bestimmen können welche Gesetze auf ihre Mobile Health App zutreffen. https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool