

Die Nutzung von Apps – eine datenschutzrechtliche Einschätzung

L'utilisation d'applications: une analyse sous l'angle du droit de la protection des données

URSULA UTTINGER

Welche Spuren hinterlasse ich im Netz, wenn ich Apps wie «Physiotherapy Exercises», «Fitbit» oder «Catchmypain» nutze? Erläuterungen der Präsidentin des Datenschutzforums Schweiz.

Quelles traces mon utilisation d'applications telles que «Physiotherapy Exercises», «Fitbit» ou «Catchmypain» laisse-t-elle sur internet? Explications de la Présidente du Forum de protection des données Suisse.

Der informierte Patient ist heute eine Tatsache. Oft holt der Patient oder die Patientin Informationen aus dem Internet – ohne sich dabei Gedanken über allfällige Spuren im Netz zu machen. Bereits gibt es verschiedene Artikel, die aufzeigen, dass ein Zusammenhang zwischen Suchanfragen zu einem bestimmten Krankheitsbegriff und der Verbreitung der Krankheit besteht. Offensichtlich ist dies vor allem beim Begriff «Grippe». Die Suchanfragen dazu ermöglichen, ihre Verbreitung über ganze Länder hinweg zu verfolgen. [1]

Durch die Nutzung des Internets werden via IP-Adresse Spuren hinterlassen. Dies ist nicht nur bei der Internetnutzung durch einen Laptop, sondern selbstverständlich auch durch Smartphones so. Der Benutzer hinterlässt eine Spur, die aufzeigt, wann er welche Seiten aufgesucht hat. Dies wiederum führt zu einem Profil des Nutzers. Ausserdem kann herausgefunden werden, mit welchem Betriebssystem ein Nutzer arbeitet, mit welchem Browser und welcher Browserversion.

Spuren bei der Nutzung von Apps

Doch nicht nur bezüglich Spuren im Netz, sondern auch bezüglich Spuren bei der Nutzung von Apps sind viele User nachlässig. Grundsätzlich ist zu unterscheiden zwischen Apps, die einzig Informationen abgeben wie das «Physiotherapy», «Physiotherapy Exercises» oder «Rumpfzirkel»-App, sowie Apps, die Informationen automatisch aufnehmen oder Eingaben verlangen. Bei Ersteren braucht es keine

De nos jours, le patient informé constitue une réalité. Il s'informe souvent sur internet, sans se soucier des éventuelles traces qu'il laisse derrière lui. Divers articles démontrent déjà la relation entre les recherches concernant une certaine pathologie sur Internet et la propagation de cette pathologie. Ce phénomène est particulièrement manifeste avec le terme «grippe». Les recherches qui la concernent permettent de suivre sa propagation sur des pays entiers [1].

L'utilisation d'Internet laisse des traces via l'adresse IP. Ce n'est évidemment pas seulement le cas pour l'utilisation





Syda Productions – Fotolia

Gewisse Apps zeichnen die Aktivitäten permanent auf. I Certaines applications enregistrent les informations en de manière continue.

Online-Verbindung und sie zeigen «nur» Übungen. Abgesehen davon, dass ersichtlich ist, welches Smartphone das App geladen hat, sind diese Apps wenig bedenklich – sofern man sich nicht daran stört, dass solche Informationen an Werbepartner und Statistikfirmen weitergeleitet werden.

Andere Apps zeichnen die Aktivitäten oder/und Fitness permanent auf wie «fitbit», «strava» oder «runtastic». Geschickt nutzen diese Apps den Wettbewerbsdrang der Nutzer: Man will vergleichen, verfolgen, besser sein. Oft können nicht nur die eigenen Daten verglichen werden, sondern man kann auch «gegen Freunde, Einheimische oder Profis» antreten. Bei «strava» gibt es hinterlegte und permanent aktualisierte Bestenlisten nach Alter und Gewicht. Es lässt sich feststellen, welche der Freunde gerade am Trainieren sind. Die meisten Daten beruhen dabei auf einer Eigendeklaration. Doch stimmen diese Angaben? Ist der Beste im Alter 63 nicht erst 43, wurde eine Distanz rennend oder auf dem Velo absolviert? Und vor allem: Welches ist der tatsächliche Nutzen und Mehrwert dieses Wissens?

Die Allgemeinen Geschäftsbedingungen – am Beispiel «fitbit»

Meistens hat der Nutzer in den Allgemeinen Geschäftsbedingungen (AGB) zugestimmt, dass Daten von ihm gesammelt, weitergegeben und statistisch genutzt werden dürfen. Und dennoch sind die Nutzer überrascht, wenn ihnen bewusst wird, was mit den Daten alles gemacht wird. Es ist davon auszugehen, dass die Mehrheit der Nutzer die AGB nicht liest – doch wie weit soll oder muss der Einzelne bevormundet werden?

d'Internet par un ordinateur portable, mais également pour les smartphones et autres appareils. L'utilisateur laisse une trace des pages qu'il a consultées et quand il l'a fait. À partir de là se crée un profil d'utilisateur. Il est par ailleurs possible de déterminer le système d'exploitation de l'utilisateur, son navigateur et la version de ce dernier.

Traces lors de l'utilisation d'applications

En plus des traces laissées sur Internet, bon nombre d'utilisateurs font également preuve d'imprudence face aux traces qu'ils laissent en utilisant des applications. Il s'agit de distinguer entre des applications qui ne font que fournir des informations, telles que «Physiotherapy», «Physiotherapy Exercises» ou «Rumpfzirkel», et les applications qui enregistrent automatiquement des informations ou qui demandent des saisies. La première catégorie ne nécessite pas de connexion internet et ne fait «que» montrer des exercices. Mis à part le fait que le type de smartphone utilisé pour télécharger l'application est détectable, ces applications ne donnent pas vraiment lieu de s'inquiéter à condition que la transmission de telles informations à des partenaires publicitaires et des entreprises de statistiques ne vous dérange pas.

D'autres applications, telles que «fitbit», «strava» ou «runtastic» enregistrent constamment vos activités et/ou vos performances de fitness. Ces applications profitent habituellement de l'esprit de compétition des utilisateurs: on veut se comparer, suivre, être meilleur. En plus de pouvoir comparer ses propres données, il est souvent également possible de se mesurer «avec des amis, des amateurs ou des professionnels». «Strava» dispose d'un classement déposé et régulièrement mis à jour, par âge et poids. Il est possible de voir qui, parmi ses amis, est en train de s'entraîner. La plupart des données se basent alors sur les déclarations des utilisateurs eux-mêmes. Ces informations sont-elles correctes? Le meilleur à 63 ans n'en a-t-il pas plutôt 43; une distance a-t-elle été parcourue à pied ou en vélo? Et surtout, quelle est la véritable utilité et valeur ajoutée de ce savoir?

Les conditions générales de vente, en prenant «fitbit» comme exemple

Les utilisateurs acceptent souvent par les conditions générales de vente (CG) que des données les concernant soient collectées, transmises et utilisées à des fins statistiques. Ils sont tout de même étonnés lorsqu'ils prennent conscience de ce qui advient de ces données. Il faut partir du principe que la plupart des utilisateurs ne lisent pas les CG, mais dans quelle mesure les individus doivent-ils être mis sous tutelle?

Les CG de «fitbit» sont par exemple très complètes et transparentes [2]. Mais certains points sont critiquables d'un point de vue de la protection des données:

Die AGB von «fitbit» sind beispielsweise sehr umfassend und transparent. [2] Einige Punkte sind aus datenschutzrechtlicher Sicht kritisch zu hinterfragen, beispielsweise:

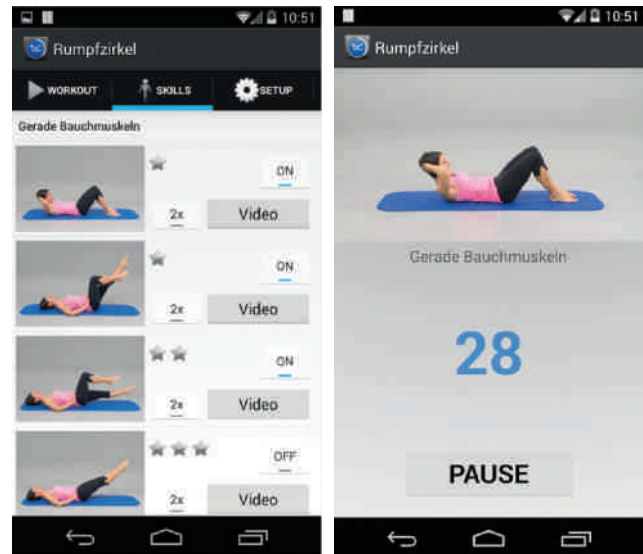
- Gewisse Daten werden von «fitbit» an strategische Partner weitergegeben, für statistische Auswertungen genutzt. Es wird aber nicht definiert, wer die strategischen Partner sind.
- Die Voreinstellungen des «fitbit»-Kontos sind nur bedingt datenschutzfreundlich. Standardmässig öffentlich sind Profilfoto, Spitzname sowie Schritte und Strecke. Für Freunde sind Informationen wie der echte Name, Alter, Geschlecht, Grösse und Ort zugänglich. Doch wer sind die Freunde auf «fitbit»? Verhält es sich ähnlich wie bei Facebook, wo auch Fremde zu Freunden werden, sobald man deren Kontaktanfrage bestätigt? Nicht klar geregelt ist, was Freunde mit den Informationen machen dürfen – das Risiko besteht, dass durch «Freunde» Daten öffentlich werden.
- Sämtliche Daten von «fitbit» werden zudem in den USA gehostet. Der Datenschutz hat in den USA einen anderen Stellenwert als in Europa, der Staat hat mehr Zugriffsmöglichkeiten.
- Die AGB können regelmässig aktualisiert (= abgeändert) werden.

Selbstverständlich sind die Formulierungen so gewählt, dass alles primär zugunsten des Nutzers scheint.

Apps mit Daten zur medizinischen Forschung

Eine andere Art von Apps sind «catchmypain» oder «patientslikeme», bei denen betroffene Personen ihre Erfahrungen teilen. Dieses Teilen von Informationen kann auch als eine Form von Solidarität unter Betroffenen verstanden werden: Durch die grosse Datenmenge können individuelle Faktoren eher ermittelt werden, die Auswirkungen auf Krankheiten haben. [3] In diesem Sinne können die Daten auch der medizinischen Forschung dienen.

Den Teilnehmenden wird gemäss den AGB garantiert, dass einzig über die E-Mail-Adresse auf die Identität geschlossen werden kann und dass diese Daten nie weitergegeben werden. Ebenfalls wird in diesen AGB festgehalten, dass die Schmerzinformationen automatisch ausgewertet und analysiert werden. Die Daten werden unterschieden in Personendaten, Profildaten und Gesundheitsdaten. Bei Profil- und Gesundheitsdaten wird darauf hingewiesen, dass der Benutzer nur diejenigen eingeben soll, bei denen er einverstanden ist, dass sie an Dritte weitergegeben werden – an ähnlich Betroffene, Ärzte, Therapeuten, Forscher von Hochschulen, aber auch an Hersteller von medizinischen Produkten. Korrekterweise wird darauf hingewiesen, dass im Nor-



Andere Apps geben nur Informationen ab, wie zum Beispiel das Rumpfzirkel-App. | D'autres applications ne fournissent que des informations; c'est le cas de «Rumpfzirkel-App».

- Certaines données sont transmises par «fitbit» à des partenaires stratégiques et utilisées à des fins statistiques. Il n'est toutefois pas clairement défini qui sont ces partenaires stratégiques.
- Les pré-réglages du compte «fitbit» ne vont que partiellement dans le sens de la protection des données. La photo de profil, le surnom, les étapes et les trajets effectués sont publics par défaut. Les amis peuvent accéder aux informations telles que le vrai nom, l'âge, le sexe, la taille et le lieu. Mais qui sont vraiment ces amis sur «fitbit»? Est-ce une situation similaire à celle de Facebook où même des inconnus deviennent des amis dès que l'on accepte leur invitation? Ce que les amis sont libres de faire des informations n'est pas clairement réglé, il subsiste le risque que les informations soient rendues publiques par ces «amis».
- L'ensemble des données de «fitbit» est hébergé aux États-Unis. La protection des données ayant un autre statut aux États-Unis, l'État y bénéficie d'un plus grand accès.
- Les CG peuvent régulièrement être mises à jour (= modifiées).

Les formulations sont évidemment choisies de telle façon que tout semble de prime abord aller en faveur du client.

Applications qui comportent des données servant à la recherche médicale

Les applications telles que «catchmypain» ou «patientslikeme», au moyen desquelles des personnes échangent leurs expériences, constituent un autre type d'applications. Ce partage

malfall nicht möglich ist, auf die Identität des Nutzers zu schliessen. Eine Anonymität wird aber nicht garantiert.

Aus datenschutzrechtlicher Sicht ist dies ein Schwachpunkt. Dennoch: Ist die betroffene Person aufgeklärt und nimmt dieses Risiko bewusst in Kauf, ist nichts dagegen einzuwenden. Denn gerade solche Plattformen ermöglichen der Forschung auch Fortschritte. So konnte über die Plattform «patientslikeme» in einer ergänzenden Studie nachgewiesen werden, dass Lithium als Medikament bei Amyotropher Lateralsklerose keine signifikante Wirkung zeigt. [4] Eine Frage bleibt auch hier: Sind die eingegebenen Daten immer richtig?

Datenschutzrechtliche Risiken werden schlecht beachtet

Zusammenfassend lässt sich festhalten, dass zu unterscheiden ist zwischen Apps, die einzig Informationen abgeben, und Apps, die Daten erfassen, sammeln und allenfalls sogar mit Dritten teilen. Insbesondere Letztere sind mit datenschutzrechtlichen Risiken verbunden, die zwar in den AGB meist beschrieben sind, aber kaum wahrgenommen werden. Jeder Nutzer hat heute die Möglichkeit, sich zu informieren und dann zu entscheiden. Analog zu Facebook gilt bei den Apps: Datenschutz finden alle wichtig. Trotzdem gibt es viele Nutzer, die sich keine konkreten Gedanken zu Risiken machen und sorglos (fast) alles von sich preisgeben. Die konkreten Risiken sind meist zu abstrakt – oder wem wurde schon einmal eine Versicherung verweigert mangels genügender Bewegung gemäss Fitbit-Armband? |



«Patientslikeme»: Patienten teilen ihre Erfahrungen. | «Patientslikeme»: des patients échangent leurs expériences.

d'informations peut également être interprété comme une forme de solidarité de la part des personnes concernées entre elles: la grande quantité de données aide à déterminer des facteurs individuels ayant une incidence sur les maladies [3]. Dans ce sens, ces données peuvent également servir la recherche médicale.

Les CG garantissent aux participants que leur adresse e-mail constitue la seule voie d'accès à leur identité et que les données ne sont jamais transmises. Ces mêmes CG assurent que les informations concernant la douleur sont évaluées et analysées de manière automatique. Les données sont réparties en données personnelles, données de profil et données relatives à la santé. En ce qui concerne les données de profil et les données relatives à la santé, on invite l'utilisateur à saisir uniquement les données dont il accepte qu'elles soient transmises à des tiers, à des personnes similairement touchées, des médecins, thérapeutes, chercheurs de hautes écoles, mais également à des fabricants de produits médicaux. Il est signalé qu'il est impos-

Wie man sich schützen kann

Folgende Massnahmen können die eigenen Daten auf dem Handy besser schützen:

- Anonymisierungssoftware einsetzen.
- Surfen via Proxysurfer (Kommunikationsschnittstelle, die über eine eigene Adresse eine Verbindung mit Dritten herstellt).
- Metasuchmaschine nutzen: etools.ch, apollo7.ch (Schweiz) oder ixquick.de, metager.de (Deutschland).
- «Fake permissions»-App aufs Handy laden und nutzen. (Viele Apps greifen auf private Informationen zurück und funktionieren bei Verweigerung nicht richtig. «Fake permissions» liefert den Apps falsche Informationen – so können die Apps trotzdem gut genutzt werden.)
- Möglichst wenige Programme und Apps aufs Handy laden.
- Ortungsdienst nicht einschalten.
- Vor dem Herunterladen der Apps Einstellungen kontrollieren und datenschutzfreundliche Einstellung wählen.
- Keine Einstellung wählen, die Daten mit Dritten teilt.

Comment se protéger

Les mesures suivantes permettent de mieux protéger vos données sur votre téléphone portable:

- Utilisez un logiciel d'anonymisation.
- Naviguez au moyen d'un serveur proxy (interface de communication qui établit une connexion avec des tiers à partir de sa propre adresse).
- Utilisez un méta-moteur de recherche: etools.ch, apollo7.ch (Suisse) ou ixquick.de, metager.de (Allemagne).
- Téléchargez l'application «Fake permissions» sur votre téléphone portable et utilisez-la. (De nombreuses applications demandent à accéder à vos informations privées et ne fonctionnent pas correctement en cas de refus. «Fake Permissions» fournit de fausses informations à l'application, ce qui permet tout de même de bien utiliser les applications.)
- Chargez le moins possible de programmes et d'applications sur votre téléphone portable.
- N'activez pas le service de localisation.
- Avant de télécharger des applications, contrôlez leurs préférences et sélectionnez des préférences protégeant vos données.
- Ne sélectionnez pas de préférences qui partagent des données avec des tiers.

Literatur | Bibliographie

1. Björn & Sören Christensen: Was Google mit der Grippewelle zu tun hat. Schleswig-Holstein Journal, Wochenendbeilage, 19.10.2013. <http://google-produkte.blogspot.ch/2013/09/google-grippe-trends.html> (besucht am 30. Juli 2014).
2. Fitbit Privacy Policy. <http://www.fitbit.com/de/privacy> (besucht am 30. Juli 2014).
3. Rebecca Knoth: Den Wert von Gesundheitsdaten ausschöpfen. Medienrohstoff, August 2013. Verein Daten und Gesundheit. www.datenundgesundheit.ch
4. Peter Mansell: PatientsLikeMe lithium study shows real-time value of social networks. PharmaTimes online. 26. April 2011. http://www.pharmatimes.com/article/11-04-26/PatientsLikeMe_lithium_study_shows_real-time_value_of_social_networks.aspx (besucht am 30. Juli 2014).



Ursula Uttinger, lic. iur., exec. MBA HSG, ist Geschäftsführerin der Activita Care Management AG und Präsidentin des Datenschutz-Forums Schweiz. Sie berät zum Datenschutz, verfasst dazu Gutachten sowie Artikel und ist an diversen Hochschulen als Referentin tätig. www.datenschutz-forum.ch

Ursula Uttinger, licenciée en droit, exec. MBA HSG; directrice d'Activita Care Management AG et présidente du Forum de protection des données Suisse. Elle est conseillère en protection des données, rédige des expertises ainsi que des articles à ce sujet et travaille comme chargée de cours à diverses Hautes écoles. www.datenschutz-forum.ch

sible, en temps normal, d'identifier l'utilisateur. L'anonymat n'est toutefois pas garanti.

Cela constitue un point faible sous l'angle de la protection des données. Si la personne concernée est toutefois informée et consciente du risque, rien ne s'y oppose. De telles plate-formes permettent justement à la recherche de faire des progrès. Ainsi, grâce à la plate-forme «patientslikeme», une étude complémentaire a pu démontrer que le lithium n'a pas d'effet significatif dans le traitement de la sclérose latérale amyotrophique [4]. Une question subsiste: les données saisies sont-elles toujours exactes?

Les risques relatifs à la protection des données ne sont pas suffisamment pris en compte

En résumé, il s'agit de distinguer entre les applications qui se contentent de fournir des informations et celles qui saisissent, collectent, voire partagent des données avec des tiers. Ces dernières comportent certains risques quant à la protection des données qui, bien qu'ils soient souvent décrits dans les CG, sont rarement pris en compte. De nos jours, chaque utilisateur est libre de s'informer et de décider ensuite. À l'instar du cas de Facebook, tout le monde reconnaît l'importance de la protection des données dans le cadre des applications. Il existe tout de même de nombreux utilisateurs qui ne se posent pas de questions concrètes quant aux risques et qui révèlent (presque) tout à leur sujet de manière insouciant. Les risques concrets sont souvent trop abstraits. Qui s'est déjà vu refuser une assurance en raison d'un manque d'activité physique attesté par le bracelet Fitbit? █

Das neue Rechnungslegungsrecht muss spätestens ab

1. Januar 2015

angewendet werden

- › Auch freie Berufe können ab 2015 buchführungspflichtig werden
- › Stellen Sie frühzeitig die Weichen in die richtige Richtung
- › Vereinbaren Sie einen unverbindlichen Termin mit uns

Wir freuen uns auf Sie!



Buchführungen

Mitglied TREUHAND | SUISSE

BW Buchführungen GmbH
Steineggerhof 1
8855 Wangen SZ

Tel.: 055 440 55 11
Fax: 055 440 55 13

info@bw-buchfuehrungen.ch
www.bw-buchfuehrungen.ch