AUFBRUCH

Digitales Ich

Privates schützen, Chancen nutzen

Unser Ich im Spiegel
Wie wir mit Smartphone und Laptop eine digitale Identität erzeugen

Schutz aus München
Leserinnen und Leser erkunden das Google Safety Engineering Center

Der TÜV im Gespräch
So sorgt der Technische Überwachungsverein online für mehr Sicherheit

Google

Editorial

Liebe Leserin, lieber Leser,

ganz selbstverständlich nutzen wir digitale Anwendungen im Alltag: Wir navigieren, buchen, recherchieren, kaufen ein oder kommunizieren. Durch viele dieser Handlungen entstehen Daten, die auch dazu verwendet werden, das Internet und seine Programme weiter zu verbessern.

Alle Spuren, die wir in unserem digitalen Leben hinterlassen, bilden unser »digitales Ich«, eine Art Online-Abbild von uns selbst. Aber was genau bedeutet das? Wie können wir unsere digitale Identität beeinflussen und schützen? Auf den folgenden Seiten wollen wir uns diesen Fragen nähern.

Viel Freude beim Lesen!

Ihr Team von Google

Impressum

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA | Tel.: +1 650 253 0000 | Fax: +1 650 253 0001 |
E-Mail: support-deutschland@google.com | Vertreten durch Sundar Pichai (Chief Executive Officer) |
Google LLC ist eine nach dem Recht des Staates Delaware gegründete Gesellschaft |
Registernummer: 3582691, Secretary of State, State of Delaware | Umsatzsteuer-ID.-Nr.: EU372000041

Dies ist eine Anzeigensonderveröffentlichung von Google.
Danke an das Team von SZ Scala GmbH.

Inhalt

Google Zukunfts-werkstatt
Seite 25

Titelfoto: Westend61/VITTA GALLERY | Fotos: Eva-Maria Feilkas, Google/Markus Mielek | Illustration: Katharina Bitzl


Ich

Essay zur digitalen Identität

Mit unseren Smartphones, Tablets und Laptops erkunden wir die digitale Welt – und schaffen ein Bild unserer selbst: Wer sind wir online? Was tun wir dort? Was gewinnen wir dabei?

ALS STEVE JOBS ANFANG 2007 das erste iPhone vorstellte, sprach er von einem revolutionären Produkt. »Wir haben das Telefon neu erfunden«, sagte er. »Das iPhone ist das Internet für die Hosentasche.« Mithilfe von Google Maps navigierte er, dort auf der Bühne stehend, zuerst zum Eiffelturm, dann zum Kolosseum. »Unglaublich!«, sagte er nicht nur ein Mal. Steve Jobs, der, das kann man so sagen, ein Mann der Visionen war, wird vermutlich geahnt haben, dass Smartphones das Fenster zum »digitalen Ich« werden würden. Weil wir sie immer bei uns tragen und fast alles mit ihnen machen: Kommunizieren. Spielen. Uns orientieren. Uns informieren. Dinge kaufen. Tickets lösen. Bezahlen. Und vieles, vieles mehr. So ein Smartphone weiß ziemlich gut, wer wir sind.

Dieses Wissen, wer man ist, wie sich das eigene Sein definiert, ist auch eine zentrale Frage der Philosophie. Und eine sehr schwierige dazu. Wer es schafft, einen einfachen Zugang zu dieser großen Frage zu finden, kann sich eines Bestsellers so gut wie sicher sein.

Dem norwegischen Autor Jostein Gaarder erging es so, als er ein Mädchen namens Sofie auf die Suche nach dem Ich schickte. Der Roman *Sofies Welt,* der Anfang der 1990er-Jahre erschien, verkaufte sich weltweit mehr als 40 Millionen Mal. Und als der Philosoph Richard David Precht sich und die Leserschaft fragte *Wer bin ich – und wenn ja, wie viele?,* belegte das Sachbuch jahrelang die vorderen Plätze der deutschen Bestsellerlisten.

Identität ist das, was einen Menschen ausmacht: Das können physische Eigenschaften sein, beispielsweise der Abdruck eines Fingers, oder aber auch persönliche Daten wie Name und Geburtsdatum. In einem Personalausweis etwa werden solche Eigenschaften und Daten festgehalten, um darlegen zu können, dass es sich um eine bestimmte Identität handelt. Passend dazu spricht man im Englischen von »identity document«, also einem Identitätsdokument, kurz ID. Rund eine Milliarde Menschen weltweit haben keine solche ID. Sie haben eine Identität, doch nirgends ist festgehalten, wer genau sie sind, weder analog noch digital.

Das Netz als Selbstfindungsraum

Manche Länder gehen hingegen noch einen Schritt weiter. In Estland hat jeder Bürger eine elektronische Identität (siehe Seite 27). Mit dieser hat er Zugang zu einem zentralen Verwaltungskonto, über das alle staatlichen Dienstleistungen – sei es die Steuererklärung oder die digitale Krankenakte – aufgerufen werden können. Ist man bereit, seine Organe zu spenden? Ja oder Nein, klick, fertig, eine lebensbewahrende Entscheidung wurde einfach übermittelt.

So beständig identitätsgebende Eigenschaften wie der eigene Fingerabdruck sind, so unbeständig ist die Identität selbst. Wir verändern uns, immer wieder aufs Neue. Identität ist Gegenwart, sie spiegelt die Jetztzeit.

Zu diesem stetigen Sich-Verändern kommt das Internet als weiterer (Selbstfindungs-)Raum hinzu. So wie wir uns in der realen Welt fortbewegen, so erkunden wir auch die virtuelle und formen ein digitales Ich. So wie in der realen Welt hinterlassen wir auch digital Spuren: Welche Webseiten wir besuchen und welche Apps wir verwenden, sagt viel darüber aus, was wir mögen und wer wir sind.

Auf den folgenden Seiten erkunden wir unsere digitalen Aktionen und wie sie zu so etwas wie unserem digitalen Leben werden:

Kommunizieren und Arbeiten wird digital und persönlich

Erst wenn wir uns mit anderen austauschen, entwickeln wir eine Idee von uns selbst – sei es in echt, am Telefon oder digital

IDENTITÄT SEI DIE SUMME VON BEZIEHUNGEN, heißt es in der Philosophie – und dass das Selbst durch Kommunikation entwickelt werde, als Ergebnis des Zusammenlebens mit anderen.

Überhaupt: Wir können uns unser Selbst nur durch die Beziehung zu anderen Menschen vorstellen. Wir müssen gespiegelt werden, um uns wahrnehmen zu können. Digitale Technik kann dabei helfen – einerseits über soziale Netzwerke wie zum Beispiel Facebook oder Twitter, die gesellschaftliche Strukturen digital abbilden, andererseits über Kommunikationstechnologie, mit der wir uns austauschen, ohne einander gegenüberzusitzen. Über Tausende von Kilometern hinweg können wir Partner, Großeltern, Freunde oder neue Bekannte im Videotelefonat treffen und gemeinsam mit Kollegen an Präsentationen arbeiten. Wir können Hangouts, Chats und Sprachnachrichten nutzen, um uns schnell und umstandsfrei abzustimmen. Und wenn wir sprachlich nicht weiterkommen, bitten wir Programme wie Google Übersetzer oder DeepL um Hilfe.

Foto: Victor Torres/Stocksy.com | Screenshot: Google Maps

Orientieren und Finden wird digital und persönlich

Das Smartphone ermittelt unseren Standort und trägt dazu bei, dass wir uns schnell fortbewegen

MITHILFE DES STANDORTS, den unser Smartphone ermittelt, finden wir schnell und zuverlässig unser Ziel – ganz egal, ob zu Fuß, mit dem Bus, mit dem Fahrrad oder im Auto. Die jeweilige Position kann mithilfe unterschiedlicher Sensoren bestimmt werden, zum Beispiel mittels der GPS-Funktion, die sich in jedem Smartphone befindet. Erst wenn der genaue Standpunkt klar ist, lässt sich auch der beste Weg zu einem Ziel berechnen. Der Superlativ »bester Weg« meint dabei meistens auch »den schnellsten aller Wege«.

Weltweit nutzen mehr als eine Milliarde Menschen Google Maps. Warum sollen wir auch herumirren, wenn wir den direkten Weg angezeigt bekommen können – inklusive möglicher Staus und Verkehrsverzögerungen fast in Echtzeit? Wie viel Zeit wir im Schnitt für eine mögliche Route benötigen, kann nur aufgrund vieler Daten ermittelt werden. Anders ausgedrückt: Gäbe es nicht die – stets anonymisiert zusammengeführten – Daten anderer NutzerInnen, würden wir keine präzise Aussage über Dauer und mögliche Verzögerungen erhalten.

Kaufen und Bezahlen wird digital und persönlich

Das Vertrauen in digitale Zahlungsprozesse wächst – und erleichtert Menschen weltweit Warentausch

AUCH WENN BARGELD IN DEUTSCHLAND NACH WIE VOR das am häufigsten genutzte Zahlungsmittel ist, begleichen immer mehr Menschen ihre Einkäufe oder Rechnungen, ganz ohne eine Münze oder einen Schein in die Hand zu nehmen. Bei uns ist zum Beispiel der Online-Bezahldienst PayPal sehr verbreitet. Aber auch mobile Bezahlangebote erfreuen sich in Deutschland immer größerer Beliebtheit. Dienste wie Google Pay ermöglichen schnelles und sicheres Bezahlen auf Websites, in Apps und in Geschäften. Die Transaktion kann dabei nach Wunsch von den Händlern auch personalisiert werden: Die Nutzer können zum Beispiel durch jede Zahlung im Rahmen von Treueprogrammen Punkte sammeln, mit denen sie weitere Angebote der Händler nutzen können. Vor allem in China ist der Zahlservice WeChat Pay populär, den Millionen von Menschen mithilfe ihrer Smartphones aus dem Messengerdienst WeChat heraus ansteuern und nutzen.

Lernen und Verstehen wird digital und persönlich

Auf Online-Plattformen bilden sich Menschen ganz nach ihrem Wissensstand und ihren Bedürfnissen weiter

WER SICH FRAGT, wie noch mal die Serie heißt, in der Jennifer Aniston zehn Jahre lang mitspielte; wer wissen will, wie der Dreisatz funktioniert; wer ein Gulasch kochen möchte, aber das Rezept nicht parat hat – das Internet kennt alle Antworten, sie sind nur eine Suche entfernt. Aber damit nicht genug. Das Internet ist zur Volkshochschule geworden. Ganze Plattformen wie »Coursera« oder »Udacity« vermitteln Fachwissen in allen nur denkbaren Branchen. Auf YouTube werden Strickkenntnisse ebenso gelehrt wie Gitarren-Know-how. Auf der Webseite der TED-Talks stehen alle Vorträge der Innovationskonferenz kostenlos zur Verfügung. So kann jeder Michelle Obama oder Greta Thunberg zuhören – letztere wurde mit ihrem Vortrag bei YouTube bereits mehr als vier Millionen Mal gesehen.

Fotos: Sergio Marcos/Stocksy.com, Myrzik & Jarisch, Jose Luis Carrascosa/DEEPOL by plainpicture

Spielen und Unterhalten wird digital und persönlich

Im Digitalen ist Unterhaltung so einfach verfügbar geworden wie nie – präzise zugeschnitten auf unseren Geschmack

DER GRÜNDER DES INTERNET-STREAMINGDIENSTES Netflix formulierte einmal das Geheimnis seines Angebots: »Unsere Website passt sich an den individuellen Geschmack des Nutzers an.« Mit jeder gesehenen Serie, mit jedem geschauten Film lernt Netflix mehr über die Vorlieben und auch die Abneigungen der Zuschauerinnen und Zuschauer. Entsprechend passen die Algorithmen die persönlichen Empfehlungen immer wieder aufs Neue an, um dem jeweils aktuellen Geschmack entgegenzukommen.

Inzwischen arbeiten viele weitere Dienstleister nach ähnlichen Prinzipien, sie heißen »Prime Video«, »Joyn«, »MagentaTV« und »Apple TV+«. Das Angebot der Streaminganbieter wächst und scheint unerschöpflich zu sein. Aber nicht nur Serien und Filme werden im Internet gestreamt: Google brachte kürzlich »Stadia« auf den Markt, eine Plattform zum Streamen von Videospielen. Auch Konsolen wie Playstation und Xbox lassen sich mit dem Internet verbinden – um Spielpartner aus aller Welt zu Hause zu empfangen.

Unterhaltung immer dabei: Im Auto vertreibt sich Roy die Zeit mit Hörbüchern, bei Busfahrten zu Auswärtsspielen zockt er gern Videospiele auf dem Smartphone.

Fotos: Eva-Maria Feilkas

Roy, 31, lässt sich von digitalen Programmen durch den Tag begleiten: Familie, Beruf und sein Engagement in der zweiten Volleyball-Bundesliga organisiert er mit zwei Smartphones

MEIN DIGITALES COCKPIT

Ein digitaler Kalender für die ganze Familie

»ICH HABE ZWEI SMARTPHONES, eines davon ist mein Dienst-Handy. Auf meinem privaten Telefon habe ich 49 Apps, von denen ich aber nur 30 nutze. Der Rest war vorinstalliert. Morgens verwende ich als Erstes Facebook und suche dann mit Google aktuelle Sportergebnisse, zum Beispiel Football in Nordamerika – die meisten Spiele finden dort statt, wenn wir schlafen, in der Nacht von Sonntag auf Montag.

Ich arbeite als Techniker für Sicherheitsanlagen und pendle jeden Tag von Taufkirchen nach Freising. Weil ich kein großer Radio-Fan bin, höre ich während der 45 bis 60 Minuten Autofahrt lieber Hörbücher mit der App von Audible. Die Reihe *Die Zwerge* von Markus Heitz habe ich zwar schon gelesen, finde aber den Sprecher Johannes Steck so gut, dass ich sie gerade noch einmal durchhöre. In meiner Freizeit spiele ich seit Jahren Volleyball, früher professionell in der ersten Bundesliga, inzwischen in der zweiten. Wenn wir mit dem Bus zu Auswärtsspielen fahren, nehme ich mir auf dem Kindle immer Bücher mit – meistens hänge ich aber am Smartphone und zocke *Gardenscapes* oder gucke über die Amazon-Prime-App Filme und Serien.

E-Mails schreibe ich vor allem in der Arbeit, privat nutze ich meistens WhatsApp. Für den Sport bin ich in mehreren Gruppen-Chats, in denen wir ausmachen, wann und wo das nächste Training stattfindet oder wann der Bus zum Auswärtsspiel abfährt. Meine Frau und ich haben zwei Töchter, die zwei und fünf Jahre alt sind. Mit meiner Mutter und den Schwiegereltern verabreden wir uns manchmal zum Videotelefonieren über Facetime, so können die Kinder regelmäßig Oma und Opa sehen, obwohl sie weit weg wohnen. Ich empfange immer häufiger Sprachnachrichten, tippe selbst aber lieber und achte dabei auf Rechtschreibung und Groß- und Kleinschreibung, was heute nicht mehr ganz so selbstverständlich ist. Wenn es dringend ist, rufe ich lieber an.

Meine Kalender führe ich nur noch digital, die beruflichen Termine habe ich auf dem Arbeitshandy, die privaten verwalte ich auf meinem privaten Telefon. Meine Frau und ich nutzen die App TimeTree: Dort können wir beide Termine eintragen, auch für unsere Kinder, etwa die Turnstunden oder Arzttermine. Das ist sehr praktisch, das Handy hat man ja immer dabei. Dass wir nebenbei und unterwegs Bankgeschäfte und Einkäufe erledigen können, macht unseren Alltag sehr viel einfacher. Wir erfahren auch, wie es ist, wenn die Technik mal nicht funktioniert. Im Sommer waren wir auf Mittelmeerkreuzfahrt, als sich mein Handy ausschaltete. Ich gab dreimal die falsche PIN ein und wusste den PUK nicht. In den acht Tagen ohne Smartphone wurde mir bewusst, wie sehr ich es gewohnt bin, jederzeit alles nachsehen zu können.« ●

Mark Risher arbeitet als Sicherheitsexperte und Produktmanager bei Google in den USA, ist aber häufig zu Gast bei seinen europäischen Kollegen: Das Bild entstand im Züricher Büro, während er am Laptop mit Sandra Matz sprach.

Wie schützen wir uns im Digitalen?

Psychologin Sandra Matz erforscht, welche Spuren wir online hinterlassen, und Mark Risher kümmert sich bei Google darum, dass Nutzerkonten sowie persönliche Daten sicher und privat bleiben. Ein Gespräch über unsere digitale Identität – was sie ausmacht und wie wir sie am besten sichern

» Daten, die wir online hinterlassen, können mitunter sehr sensibel sein «

SANDRA MATZ, PSYCHOLOGIN

Frau Matz, Sie sind in einem kleinen Dorf im Süden Deutschlands aufgewachsen. Was haben Sie dort über Identität gelernt?

SANDRA MATZ: Individuelle Identität bedeutete dort einerseits, Teil einer gemeinschaftlichen Identität zu sein: Die Gruppe bot dir Sicherheit und Schutz, und wenn man sie brauchte, bekam man Empfehlungen und wertvolle Ratschläge. Das Leben auf dem Dorf bedeutet aber auch, dass die persönliche Identität sehr offenliegt.

Was sind Ihre Erfahrungen mit Identität, Herr Risher?

MARK RISHER: Für mich ist immer die spannende Frage: Was ist mit Identität gemeint? Identität ist ein sich entwickelndes Konzept. Wir kennen natürlich den Moment, in dem uns jemand auffordert, unsere Identität mithilfe eines Ausweises zu belegen. Was ich spannender finde, vor allem für die Zukunft: Wie können wir im digitalen Raum wissen, mit wem wir gerade sprechen? Was macht dort unsere Identität aus?

MATZ: Ich denke auch, dass wir unsere Identität ständig mit unserer Umwelt verhandeln. Der britische Philosoph Andy Clark sagte dazu kürzlich auf dem »World Frontiers Forum« *(siehe Seite 34, Anm. d. Red.)*: »Deine Identität ist Teil des mentalen Raums anderer.« Das ist eine wichtige Beobachtung, die nicht mal unbedingt digital gemeint sein muss. Im Dorf, in dem ich groß wurde, geschieht dieser Austausch, dieses Überlappen der Identitäten von alleine – etwa wenn ich beim Bäcker Brötchen kaufe und die Verkäuferin aus Erfahrung bereits weiß, was ich gern hätte. Jeder kennt jeden, jeder ist Teil des mentalen Raums des anderen.

RISHER: Das ist interessant. Ich wuchs in Washington, D.C. auf, einer Großstadt, sehr anonym also. Ich kenne es nicht, zum Bäcker zu gehen und ungefragt das zu bekommen, was ich kaufen möchte.

»In Deutschland ist man, anders als in den USA, sehr empfindlich, wenn es um die Privatsphäre geht«, sagt Psychologin Sandra Matz im Doppelinterview mit Mark Risher von Google.

Fotos: Thomas Eugster

Was sind die Unterschiede zwischen Europa und den USA, wenn es um Identität geht?
MATZ: In Deutschland ist man, anders als in den USA, sehr empfindlich, wenn es um die Privatsphäre geht. Dafür aber herrscht in Deutschland ein größeres Vertrauen in die Regierung – zumindest ist das mein Eindruck.
RISHER: Ja, im Vergleich zu Europa ist Amerika noch sehr jung: Wo sich heute das Silicon Valley befindet, war vor 70 Jahren noch Ackerland. Europa hat einfach eine längere Geschichte, wenn es um Identität geht.

Sie blicken aus verschiedenen Perspektiven auf den Begriff Identität: Sie, Frau Matz, als Psychologin. Ihnen geht es um Kaufverhalten, Marketing, psychologische Zielgruppenansprache. Sie, Herr Risher, interessiert vor allem der Sicherheitsaspekt. Gibt es Schnittmengen?
MATZ: Ich denke auch viel über Sicherheit und Privatsphäre nach und erkenne zwei Seiten einer Medaille. Die Menschen wollen einerseits Teil eines Kollektivs sein, in dem sie von anderen Menschen, aber auch von Unternehmen verstanden werden – sie schätzen es zum Beispiel, wenn sie vor Kaufentscheidungen Empfehlungen erhalten. Andererseits möchten sie nur so wenig Privates wie möglich teilen. Die Frage ist nun: Wie kann eine digitale Architektur aussehen, die ein Gleichgewicht zwischen beiden Bedürfnissen herstellt? Wie können wir jedem die Möglichkeit geben, dieses Gleichgewicht herzustellen und dabei sicher zu bleiben?

Mark Risher leitet bei Google das Produktmanagement in den Bereichen Digitale Identität, Sicherheit und Datenschutz. Er arbeitet fast täglich mit seinen Kollegen am Münchner Google Safety Engineering Center zusammen: g.co/safetyengineeringcenter

Sandra Matz studierte Psychologie an der Universität Freiburg und promovierte an der University of Cambridge. Heute forscht sie als Professorin an der Columbia Business School in New York und beschäftigt sich unter anderem mit der Frage, wie sich aus großen Datenmengen Rückschlüsse auf menschliche Verhaltensweisen ziehen lassen.

Wie könnte das gehen?
MATZ: Mein Eindruck ist, dass nur wenige Nutzer die Privatsphäre-Einstellungen ihrer digitalen Anwendungen selbst setzen. Sie belassen die Einstellungen der Anbieter und ermöglichen zum Beispiel das Setzen von Cookies.

> » Europa hat eine längere Geschichte, wenn es um Identität geht «
>
> MARK RISHER, SICHERHEITSEXPERTE

Cookies sind kleine Textdateien, die eine Website auf dem Computer eines Nutzers hinterlässt. So kann sich der Browser an einen Nutzer erinnern und zum Beispiel die Adresseingabe vereinfachen. Herr Risher, Sie befassen sich bei Google mit der Sicherheit von Daten und der Privatsphäre der Nutzer. Wie blicken Sie auf das Thema?
RISHER: Das Problem ist, dass Cookies für besseres Marketing und bessere Sicherheit gleichermaßen genutzt werden. Mit Cookies lässt sich zu Marketingzwecken das Verhalten von Nutzern verfolgen. Cookies sind aber auch ein wichtiges Werkzeug, um Sicherheit im Netz zu garantieren: Wenn ein Anbieter sicherstellen will, dass es Sandra ist, die sich gerade eingeloggt hat – und nicht jemand, der keinen Zugriff haben darf –, braucht er Cookies. Mit ihnen kann er Online-Aktivitäten einzelnen Nutzern zuordnen. Was die Privatsphäre-Einstellungen angeht: Wir raten unseren Nutzern, die Einstellungen ihres Google-Kontos zu prüfen und so anzupassen, dass sie sich damit wohlfühlen. Zum Google-Konto gelangt man in den meisten Anwendungen, indem man auf sein Profilbild klickt oder über meinkonto.google.de.

Frau Matz, als Wissenschaftlerin haben Sie eine Reihe von Studien geleitet, in denen es um digitale Identität und die damit zusammenhängende Kundenansprache ging. Können Sie das kurz erläutern?
MATZ: Ich beschäftige mich mit der Personalisierung von Werbebotschaften auf Basis der Persönlichkeitsprofile von Kunden. Es geht mir um die Frage, ob sich menschliches Handeln mithilfe von Daten vorhersagen lässt. In unserer Forschungsarbeit stützen wir uns vor allem auf Facebook-Daten, es können aber auch andere sein.

Was lesen Sie aus diesen Daten?
MATZ: Anhand dessen, was Menschen auf Facebook liken, können wir zum Beispiel herauslesen, ob sie eher introvertiert oder stärker extrovertiert sind. Mit diesem Wissen kann ein Produkt unterschiedlich beworben werden, indem man die Ansprache verändert – einmal für einen introvertierten Nutzer, einmal für einen extrovertierten Nutzer.

Welches Ziel verfolgen Sie dabei?
MATZ: Wir wollen erkunden, ob persönlichkeitsbasiertes Marketing die Effektivität steigern und zugleich die Kunden zufriedener machen kann.
RISHER: Viele sorgen sich, ihre Identität würde gläsern: Was gebe ich preis, ohne zu wissen, dass ich etwas preisgebe? Worüber habe ich Kontrolle? Werde ich manipuliert?
MATZ: Wir sagen den Menschen seit Jahren, dass ein Facebook-Like intimer ist, als sie annehmen. Daten, die wir online hinterlassen, können mitunter sehr sensibel sein.
RISHER: In meinem Team arbeiten wir deshalb daran, den Nutzern Kontrolle und Transparenz über ihre Daten zu ermöglichen.

Herr Risher, Sie haben es angedeutet: Menschen haben Sorge, dass sie manipuliert werden können, wenn ihre digitale Identität zu sehr sichtbar wird.
RISHER: Ja. Das führt uns zu der Frage, die wir immer wieder diskutieren müssen: Wie viel Transparenz wünschen sich Menschen, wie behalten sie die Hoheit über ihre digitale Identität – und wie erhält man dennoch den Nutzen der digitalen Anwendungen?
MATZ: Ich denke, die Menschen müssen begreifen, was Daten Positives herbeiführen und wie sehr wir alle durch die Analyse von Daten profitieren. Warum funktioniert Google Maps? Weil viele, viele Daten analysiert werden.
RISHER: Diese Vorteile müssen noch viel transparenter gemacht werden. Daran arbeiten wir. ●

MEHR HINTERGRUND

Sandra Matz, Mark Risher und viele weitere diskutierten auf dem »World Frontiers Forum« in Berlin über digitale Identität. Unterstützt wurde die Konferenz unter anderem vom Google Safety Engineering Center (GSEC) in München: Im GSEC führt Google die weltweite Arbeit für Sicherheit und Datenschutz zusammen. Mehr Infos auf worldfrontiersforum.org und g.co/safetyengineeringcenter

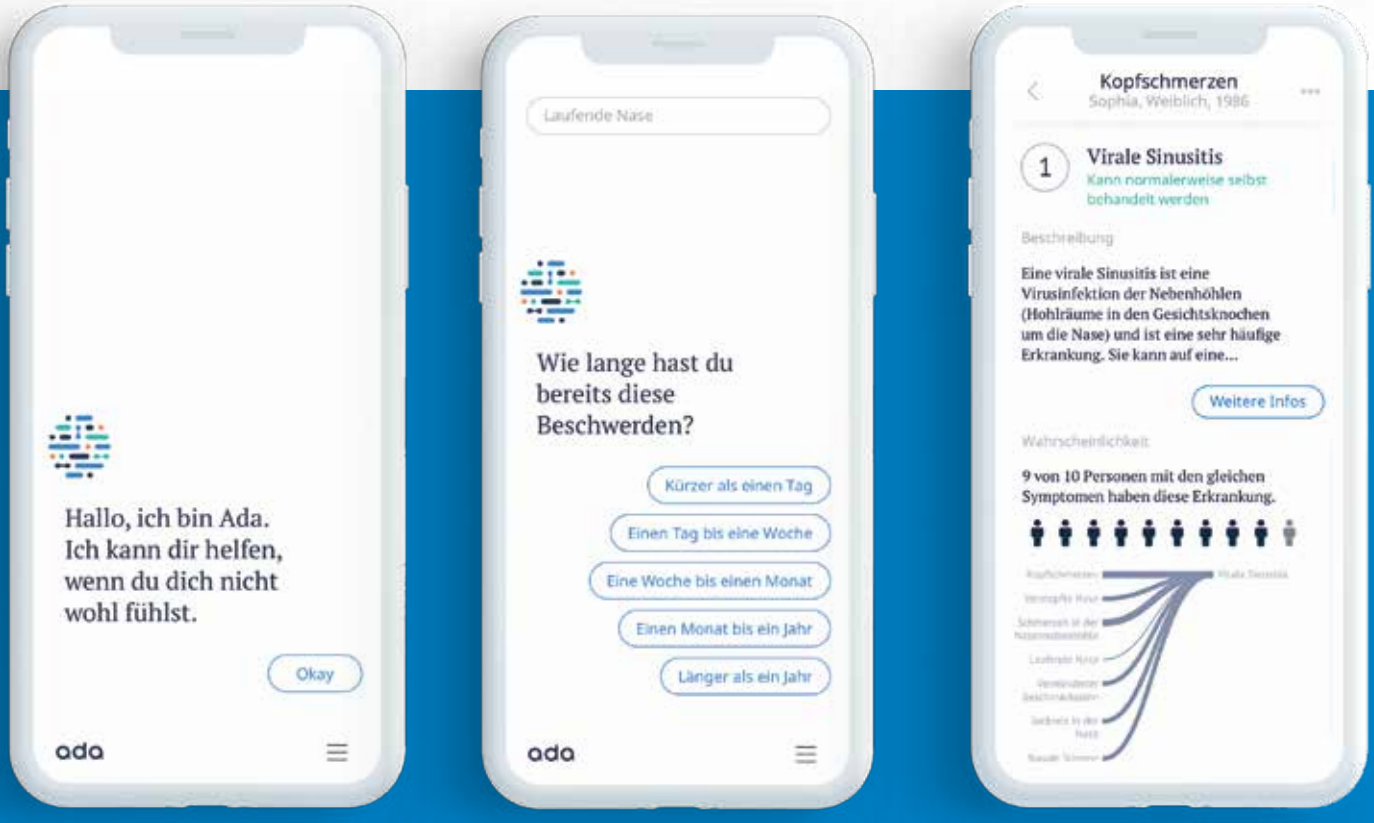
Die einen bringen Fahrgäste und Busse schneller zusammen, die anderen helfen Ärzten beim Diagnostizieren oder führen Kunden zu Kleidung, die ihnen wirklich gefällt: Wenn Daten analysiert und richtig verknüpft werden, entstehen Innovationen, die unseren Alltag verbessern

Wie aus Daten Ideen werden

WENN TAREK MÜLLER EINE BÜHNE BETRITT – was bei einem wie ihm derzeit ziemlich häufig passiert –, geht es schnell um die Frage: Wie macht ihr das? Müller ist einer der Gründer des Fashion Online Shops About You. Und weil About You derart erfolgreich ist – mehr als 25 Millionen Nutzer sind monatlich auf der Website des Unternehmens aktiv, für das Geschäftsjahr 2019 wird ein Umsatz von mehr als 700 Millionen Euro erwartet – erhält Müller eine Auszeichnung nach der anderen: 2018 nahm *Forbes* ihn in die Liste der besten Unternehmer unter 30 Jahren auf, im September 2019 wurde er zum »CMO of the Year«, zum besten Markenstrategen des Jahres gekürt. Medien bezeichnen Müller als einen der »vielversprechendsten jungen Unternehmer Europas«. Also ist die Frage durchaus berechtigt: Wie macht About You das?

»Als wir 2014 starteten, glaubten wir bereits daran, dass das Smartphone das wichtigste Kaufgerät werden wird«, sagte Tarek Müller vor wenigen Monaten auf der Bühne eines Kongresses. Immerhin 40 Millionen Menschen in Deutschland benutzten damals ein Smartphone. Heute sind es mehr als 57 Millionen, und About You führt 80 Prozent des Umsatzes auf Smartphone-Bestellungen zurück. Wer heute als Online-Händler einen Platz auf den Telefonen der Menschen erobert, ist seinen möglichen Kunden so nah wie nie zuvor. Tarek Müller nutzt diese Nähe mit About You, so gut er nur kann: Er will den Einkaufsbummel weiter digitalisieren und vor allen Dingen auch personalisieren. Deshalb versteht sich das Unternehmen heute als Kreuzung zwischen Modehändler und Modemagazin. Denn Mode wird anders konsumiert als beispielsweise ein Fernsehgerät: Der große Bildschirm ist ein Mittel zum Zweck und wird natürlich nicht in der gleichen Häufigkeit gekauft wie etwa ein Pullover oder Hemden. Wer 20 Hemden im Schrank hat, kann dennoch Interesse an Hemd 21 haben. Der Kauf von Mode bedeutet auch, zu entdecken, sich inspirieren zu lassen. An der Stelle setzt About You an: Kunden sollen in Inhalten und Angeboten stöbern können, die möglichst

Illustration: Birgit Henne



Schritt für Schritt und Frage für Frage leitet die Gesundheits-App Ada ihre Nutzer durch die Symptomanalyse. Die Anwendung gleicht die Angaben mit einem umfangreichen Krankheitsverzeichnis ab.

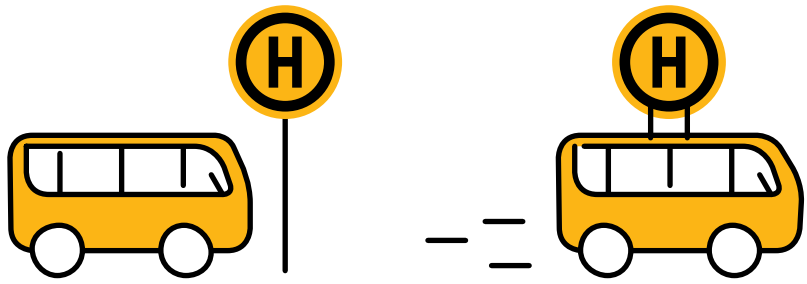
gut auf ihren Geschmack zugeschnitten sind. »Unser USP ist, dass wir den Kunden einladen, mit der App bei uns zu stöbern, und das Ganze immer weiter personalisieren«, sagte Müller dem Magazin *Capital*. »Wir verstehen den Kunden mit jedem Klick besser und machen dann Vorschläge mit Outfits und Produkten, die passen könnten.« Daten als Grundlage für neue Produkte und zufriedene Kunden: Der Hamburger Online-Versandhändler ist seit 2018 mit mehr als einer Milliarde US-Dollar bewertet. In der Unternehmenswelt spricht man in diesem Fall von einem Einhorn. In Deutschland eine noch seltene Spezies.

Mit einer App die eigene Gesundheit besser verstehen

Eine Branche, die noch Aufholbedarf hat, wenn es um Digitalisierung geht, ist die Gesundheitsbranche. Daniel Nathrath, Claire Novorol und Martin Hirsch erkannten dies bereits vor einiger Zeit und versuchen, daran etwas zu verändern. Im Jahr 2016 brachten sie »Ada« auf den Markt, eine Patienten-App. Ursprünglich wollten die drei Gründer eine Anwendung bauen, die Ärzte bei der Diagnose unterstützt, indem sie medizinisches Wissen und künstliche Intelligenz kombiniert. Entstanden ist aber eine Anwendung für Patienten, die auf Basis der vom Nutzer eingegebenen Informationen eine erste Anamnese vornehmen kann – um anschließend eine Diagnose oder, falls nötig, einen Arztbesuch vorzuschlagen. Die App wurde nicht entwickelt, um Ärzte zu ersetzen. Sie soll vielmehr Menschen helfen, ihre eigene Gesundheit besser zu verstehen und passende nächste Schritte für die richtige Behandlung zu finden.

Gut 60 Ärzte haben die medizinische Datenbank hinter Ada erstellt und befüllen sie weiterhin. Dank dieses Wissens kennt Ada Zehntausende Krankheiten. Während einer Symptomanalyse berücksichtigt das Programm eine Vielzahl von Gesundheitsinformationen des Patienten – zum Beispiel Alter, Geschlecht oder Risikofaktoren wie Vorerkrankungen. Grundlage der Technologie, mit der Ada arbeitet, ist ein sogenanntes probabilistisches System: Basierend auf der Häufigkeit einer Krankheit, den eingegebenen Symptomen und den Risikofaktoren des Patienten berechnet das Programm die wahrscheinlichste Ursache für die beschriebenen Symptome. Mit jeder neuen Information wird die Wahrscheinlichkeit neu berechnet. Die Krankheitsfälle, mit denen sich die Menschen an Ada wenden, seien vergleichbar mit denen, die auch in Arztpraxen vorkommen, sagen die Macher. Inzwischen verwenden weltweit mehr als acht Millionen Menschen Ada.

Illustrationen: Birgit Henne | Fotos: Ada, www.aboutyou.de



Neues Zeitalter der Mobilität: Die Haltestelle wird flexibel, wenn Fahrgast und Chauffeur ihre Standorte miteinander teilen.

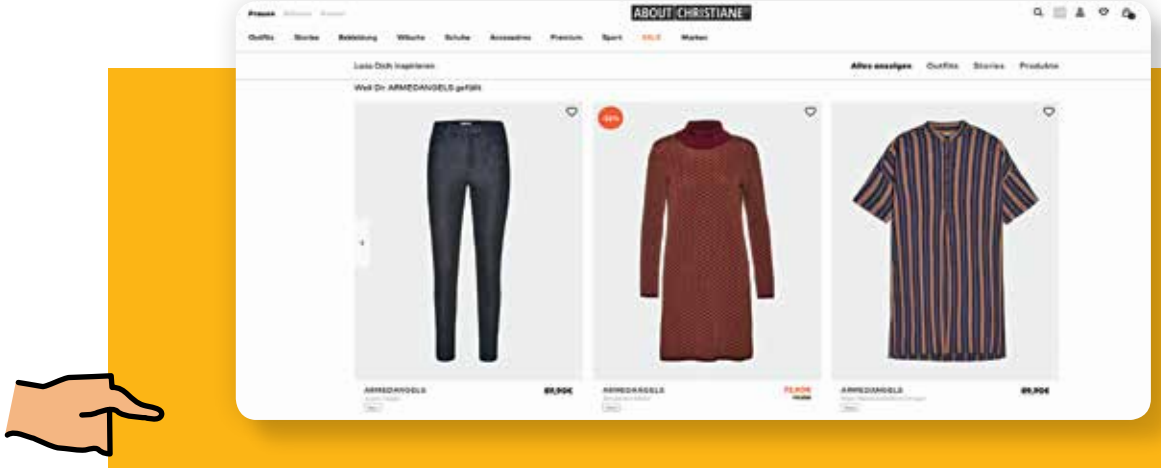
Besonders großes Potenzial sehen die Gründer im Bereich seltene Erkrankungen: Ada möchte Patienten und Ärzten helfen, schneller die richtige Diagnose zu finden. In Deutschland leiden etwa vier Millionen Menschen an einer seltenen Erkrankung, und im Schnitt muss ein Patient fünf bis sechs Jahre warten, um eine korrekte Diagnose gestellt zu bekommen. Dies liegt vor allem daran, dass es etwa 7000 seltene Erkrankungen mit vielen unterschiedlichen Symptomkonstellationen gibt. Ein Mensch kann sich diese Vielzahl an Informationen und Zusammenhängen nicht merken. Die Medizinische Hochschule Hannover hat kürzlich in einer Studie untersucht, ob und wie Ada bei der Erkennung von seltenen Erkrankungen unterstützen kann. Das Ergebnis: In vielen Fällen hätte Ada früher einen Hinweis auf eine mögliche seltene Erkrankung geben können.

Passagier und Bus gleichen ihren Standort ab und finden zusammen

Deutschland ist Autoland: Drei Viertel aller privaten Haushalte verfügen über mindestens einen Pkw, in jedem vierten Haushalt sind zwei oder mehr Autos vorhanden, weiß das Umweltbundesamt. Rund 80 Prozent der Verkehrsleistung gehen auf Autos und motorisierte Zweiräder zurück. Im März 2019 deutete Verkehrsminister Andreas Scheuer in einer Rede vor dem Bundestag an, dass dies nicht so bleiben könne, dass die Personenbeförderung modernisiert werden müsse. »Das Auto wird sicherlich anders gemanagt werden müssen«, so Scheuer. »Einen Mobilitätsmix wird es in der Zukunft mehr denn je geben, und das in ganz neuen Formen der Fortbewegung.« Die Digitalisierung, sagte Scheuer, werde dabei helfen.

Das Szenario, das der Verkehrsminister da andeutete, ist in einigen deutschen Städten bereits Wirklichkeit. Smartphones und Algorithmen haben eine neue Mobilitätsbranche entstehen lassen. Die Anbieter heißen Uber, Free Now, CleverShuttle oder Moia. Moia zum Beispiel, eine VW-Tochter, ist ein sogenannter Ride-Pooling-Dienst, der in seinen elektrisch betriebenen Kleinbussen die Fahrten von verschiedenen Fahrgästen kombiniert: Die Kundinnen und Kunden teilen sich ein Fahrzeug und damit auch die Kosten. Das System ermittelt aus den angegebenen Start- und Zieladressen die für alle beste Route. Wer zusteigen möchte (derzeit gibt es Moia in Hannover und Hamburg), installiert die App auf seinem Smartphone, erlaubt den Zugriff auf den aktuellen Standort und gibt sein Ziel ein. Im nächsten Schritt wird der nächstgelegene Einstiegspunkt angezeigt.

Dass solche Modelle Sinn ergeben, zeigen Zahlen des Statistischen Bundesamts: Knapp 70 Prozent aller Berufstätigen in Deutschland pendeln mit dem eigenen Auto – und fahren meist alleine. Hinzu kommt, dass in Städten laut Umweltbundesamt die Hälfte aller Autofahrten kürzer als fünf Kilometer ist. Grund genug, über die moderne Form der Fahrgemeinschaft nachzudenken. ●



Gleich nach dem Login bekommen die Kunden von About You eine Ahnung davon, wie der Hamburger Online-Versandhändler die Idee von der personalisierten Einkaufserfahrung umsetzt: Aus »About You« im Seitentitel wird, wie hier in unserem Beispiel, »About Christiane«.

Stets die Lieblingsmusik im Ohr, passende Serien in der Streaming-App und den E-Mail-Eingang wegen der Hausaufgaben im Blick: Sunique erlebt das Digitale als selbstverständlichen Teil ihres Alltags.

Fotos: Felix Brüggemann

Sunique, 18, nutzt digitale Anwendungen in der Schule und zur Unterhaltung: Mit Netflix streamt sie Serien, neue Aufgaben bespricht ihre Klasse im Messenger. Nur die Schlaf-App war nichts

MEIN DIGITALES COCKPIT

Das Smartphone als Mathe-Helfer

»GANZ AUSGESCHALTET IST MEIN SMARTPHONE SO GUT WIE NIE. Wenn ich tagsüber in der Schule bin, ist es natürlich auf lautlos gestellt, ich will ja nicht den Unterricht stören. Auf WhatsApp haben wir eine Klassengruppe. Steht ein Referat an, machen wir eine neue Gruppe auf, die dann wieder geschlossen wird, sobald das Referat gehalten ist. Eine der 99 Apps, die ich auf meinem Smartphone habe, heißt ›Photomath‹ und wurde mir von meinem Mathelehrer empfohlen: Mithilfe der Anwendung kann ich Aufgaben abfotografieren, anschließend bekomme ich die Lösung und den Weg dorthin angezeigt. Wir sollen das natürlich nicht immer machen, das sagte unser Lehrer schon auch, aber wenn wir allein zu Hause sind und bei den Hausaufgaben nicht weiterkommen, kann das schon sehr nützlich sein.

Längere Hausaufgaben schreibe ich daheim auf dem PC, und auch Referate, die ich halten muss, tippe ich lieber, als dass ich sie per Hand aufschreibe. Die meisten meiner Lehrer wollen auch, dass wir ihnen Hausaufgaben oder Ähnliches per E-Mail schicken – dafür nutze ich dann eine meiner drei aktiven E-Mail-Adressen. Eigentlich habe ich noch mehr, aber zu ihnen fällt mir das Passwort nicht mehr ein.

Da wir zu Hause keinen Internetanschluss haben, benutze ich meinen PC ausschließlich für Textaufgaben. Netflix habe ich auf meinem Smartphone installiert, über die App schaue ich Serien und Filme, die ich mir vorher zur Offline-Nutzung heruntergeladen habe. Was mir aufgefallen ist: Wie ich mein Smartphone nutze, hängt vor allem davon ab, ob ich WLAN habe. Zu Hause, wo es ja kein Internet gibt, bin ich weder bei Instagram noch bei TikTok. Diese Apps verbrauchen einfach zu viel Datenvolumen. Bei meinem Freund hingegen gibt es WLAN, was bedeutet, dass ich dann ständig bei Instagram und so online bin.

Wenn ich kann, höre ich Musik: auf dem Weg zur Schule, in den Pausen, manchmal sogar im Unterricht. Das dürfen wir etwa, wenn wir still für uns arbeiten sollen – manche Lehrer erlauben uns, währenddessen über Kopfhörer Musik zu hören.

Meinen Zyklus überwache ich mit ›Clue‹, meinen Kontostand mit der App meiner Bank. Vor Kurzem habe ich eine App runtergeladen, die meinen Schlaf kontrollieren sollte: Wie oft ich mich umdrehe, ob ich schnarche, vielleicht sogar im Schlaf rede. Die Auswertung fand ich aber nicht sehr aufschlussreich – die App habe ich also direkt wieder gelöscht. Das mache ich nicht oft. Viele der Spiele, die ich installiert habe, spiele ich eigentlich nicht mehr. Allerdings denke ich mir: Man weiß ja nie – vielleicht wird eine Bahnfahrt unerwartet lange dauern, sodass ich froh sein werde, dieses eine Spiel doch zu haben.« •

Auf Stippvisite

Sie hatten Gelegenheit, das Google Safety Engineering Center in München (Bild rechte Seite) aus nächster Nähe zu entdecken: Studentin Stellina Argyriadou, Apothekerin Sibylle Reinicke, IT-Experte Michael Jositz sowie Gründer Anton Eder (im Uhrzeigersinn von links oben).

Das Google Safety Engineering Center (GSEC) in München ist Googles größtes Zentrum für Sicherheit und Datenschutz weltweit. Vier *Aufbruch*-Leser besuchten die Einrichtung für Netzsicherheit und befragten vier Entwickler zu ihrer Arbeit

Protokoll: Philipp Hauner | Fotos: Lara Freiburger (4), Google/Markus Mielek (1)

JANINA VOIGT: Hallo und herzlich willkommen! Ich bin Janina Voigt und arbeite seit fünf Jahren bei Google. Anfangs war ich als Software-Ingenieurin tätig, jetzt manage ich eines der hier ansässigen Privatsphäre-Teams.

CHRISTOPH SPERL: Und ich bin Christoph Sperl und arbeite jetzt im vierten Jahr bei Google hier in München. Unser Team, das sich »Fundamental Notices and Consents« nennt, erstellt E-Mail-Kampagnen, mit denen wir mehr als eine Milliarde Nutzer über relevante Neuigkeiten informieren – zum Beispiel eine Änderung in unserer Datenschutzerklärung.

STELLINA ARGYRIADOU: Dazu gleich eine Frage: Ist Internetsicherheit an diesem Standort schon länger ein Thema?

JANINA VOIGT: Absolut. Schon 2009 entschied Google, die Entwicklung von Datenschutz- und Sicherheitsprodukten hier in München anzusiedeln. Mit der Eröffnung des GSEC im Mai 2019 wollten wir ganz bewusst ein Zeichen setzen – und unser Engagement verstärken.

CHRISTOPH SPERL: Außerdem ist Deutschland ein Land mit sehr hohen industriellen Standards. Da wir als globales Unternehmen weltweit agieren, ergibt es Sinn, dort zu entwickeln, wo Wert auf Datenschutz gelegt wird.

SIBYLLE REINICKE: Frau Voigt, Sie sagten, Sie leiten ein Privatsphäre-Team. Was machen Sie da genau?

JANINA VOIGT: Mein Team ist Teil des horizontalen großen Datenschutz-Teams in München, welches insgesamt 300 Leute beschäftigt. Wir helfen produktübergreifend allen anderen Teams hier bei Google. Bei der Entwicklung neuer Produkte sind wir meist früh involviert und stellen von Beginn an sicher, dass privat eingestufte Daten auch privat bleiben.

ANTON EDER: Ist das für Google erst ein großes Anliegen geworden, seit im Mai 2018 die

Im Mai 2019 eröffnete in München das Google Safety Engineering Center: Informatiker aus aller Welt entwickeln dort Anwendungen für die ganze Welt, mit deren Hilfe Nutzerdaten im Internet sicher und geschützt bleiben sollen.

Interessierte sich unter anderem für die Datenschutz-Grundverordnung: Anton Eder im GSEC.

neue Datenschutz-Grundverordnung in Kraft getreten ist?

JANINA VOIGT: Nein, die Frage nach den persönlichen Daten war schon vorher ganz präsent. Seit 2011 kann beispielsweise jeder über die Anwendung »Google Takeout« seine eigenen Daten herunterladen.

CHRISTOPH SPERL: Und übrigens wird jedem, der die Google-Suche nutzt, ohne über ein eigenes Google-Konto eingeloggt zu sein, ein Banner mit »Hinweisen zum Datenschutz« angezeigt. Wer das Banner ignoriert, dem wird es nach vier Tagen automatisch wieder eingeblendet – wir versuchen also, die Nutzer wirklich dazu zu bringen, die Datenschutzhinweise zu lesen, und verständlich zu machen, wie wir mit Daten umgehen.

ANTON EDER: Verstehe.

CHRISTOPH SPERL: Auch wenn Sie nicht eingeloggt sind, können Sie übrigens unter g.co/privatsphaerecheck anpassen, ob zum Beispiel Ihre Suchanfragen gespeichert werden sollen. Löschen Sie die Cookies, löschen Sie allerdings auch diese Einstellung. Und auch das Banner erscheint erneut.

JANINA VOIGT: Wenn Sie die Google-Suche benutzen, sollten Sie über ein Google-Konto nachdenken. Das ist einem Cockpit vergleichbar, in dem man alles so einstellen kann, wie man es haben möchte.

MICHAEL JOSITZ: Jeder, der eine Gmail-Adresse benutzt, hat ja bereits automatisch ein Google-Konto. Was ist in dieser Anwendung neu?

JANINA VOIGT: Wir haben das Google-Konto über die vergangenen Jahre hinweg stark verbessert. Nicht ganz neu, aber sehr praktisch ist der Privatsphärecheck. Dort können Sie einstellen, welche Aktivitätsdaten in Ihrem Google-Konto gespeichert und zur Personalisierung genutzt werden dürfen. Neu ist, dass Sie jetzt festlegen können, dass Ihre Aktivitätsdaten nach drei oder achtzehn Monaten automatisch gelöscht werden sollen.

ANTON EDER: Mal eine generelle Frage, da Sie den gesetzlichen Bestimmungen ge-

Fotos: Lara Freiburger (3), Google/Markus Mielek (1)

nügen müssen: Arbeiten Sie hier viel mit Anwälten?

CHRISTOPH SPERL: Es gibt von Anfang an eine enge Zusammenarbeit mit den datenschutzrechtlichen Experten hier im Haus. So stellen wir bei jedem Vorhaben sicher, dass die rechtlichen Anforderungen von Beginn eines Entwicklungsprozesses an eingehalten werden.

JANINA VOIGT: Wir investieren viel Zeit, um unsere Datenschutzprodukte so einfach wie möglich zu gestalten und sicherzustellen, dass Nutzer sie weltweit verstehen. Deshalb recherchieren wir auch direkt: Wir fahren zum Beispiel in ein bestimmtes Land, laden aktive Google-Nutzer ein, zeigen ihnen den Prototyp einer neuen Anwendung und fragen sie dann nach ihrer Meinung. Mit den Ergebnissen gehen wir in die Design-Phase und rollen das Produkt langsam im Markt aus.

> » Wir erheben Daten nicht als Selbstzweck «
>
> **CHRISTOPH SPERL, GOOGLE**

SIBYLLE REINICKE: Aber jetzt noch mal zur Daten-Einstellung: Ich will es einerseits bequem haben und wünsche mir gute Ergebnisse bei der Suche. Andererseits will ich nicht, dass Google alles über mich weiß. Was tun?

JANINA VOIGT: Ich denke, die neue Option »Automatisch löschen« in den Aktivitätseinstellungen stellt da ein Gleichgewicht her. Sie bekommen Personalisierung und sorgen dafür, dass wir Ihre Aktivitätsdaten nach drei oder achtzehn Monaten löschen.

CHRISTOPH SPERL: Und Sie müssen auch sehen, dass wir Daten nicht als Selbstzweck erheben. Google würde niemals Daten seiner Nutzer verkaufen. Wir erfassen Daten, damit wir unsere Produkte individuell auf die Nutzer anpassen können, und wir erfassen nur Daten, für die wir auch einen Verwendungszweck haben.

STELLINA ARGYRIADOU: Die dann wo genau lagern?

CHRISTOPH SPERL: Sie sind verteilt in Datenzentren auf der ganzen Welt.

JANINA VOIGT: So hat der Nutzer von überall aus Zugriff. Und die Daten sind auch sicher, falls ein Datenzentrum zum Beispiel durch eine Umweltkatastrophe zerstört werden sollte.

MICHAEL JOSITZ: Stichwort Sicherheit: Ich habe Bedenken, Ihrem Passwortmanager alle meine Passwörter anzuvertrauen. Andererseits ist das natürlich sehr praktisch. Da bin ich etwas im Konflikt. Was empfehlen Sie?

JANINA VOIGT: Natürlich darf Ihr Google-Konto nicht gehackt werden. Und da kann man sehr gut vorsorgen, nämlich mit der Zwei-Faktor-Authentifizierung. Das heißt, dass Sie sich nicht nur mit einem – hoffentlich sehr sicheren – Passwort einloggen. Sie bekommen in einem zweiten Schritt von uns einen Code auf Ihr Handy gesandt, den Sie beim Einloggen eingeben müssen.

MICHAEL JOSITZ: Alles klar, dieses Verfahren kennt man ja vom Onlinebanking.

CHRISTOPH SPERL: Genau. Und es ist wirklich um so vieles sicherer als das gewöhnliche Login. Der Name Zwei-Faktor-Authentifizierung kommt übrigens daher, dass man Wissen – das Passwort – und Besitz – in der Regel ein Smartphone – haben muss, um sich erfolgreich einloggen zu können.

Empfiehlt die Verwendung des Google-Kontos: Janina Voigt leitet eines der Google-Privatsphäre-Teams.

JANINA VOIGT: Aber vielleicht sollten wir jetzt an Andreas und Patrick übergeben, sie beschäftigen sich intensiv mit dem Passwortmanager.

ANDREAS TÜRK: Hallo, ich bin Andreas Türk und arbeite seit 14 Jahren bei Google. Ich habe YouTube und Google Street View mitentwickelt. Derzeit liegt mein Fokus auf dem Passwortmanager.

Erfahrene Google-Entwickler und interessierte Besucher diskutieren am Münchner Google-Standort nahe der Hackerbrücke über Internetsicherheit.

PATRICK NEPPER: Und mein Name ist Patrick Nepper, ich arbeite im Chrome-Team. Dort bin ich für die integrierten Passwort- und Autofill-Funktionen zuständig. Schon als 17-Jähriger wollte ich allen Menschen guten Zugang zum Netz verschaffen und gründete damals eine Firma namens Web Access.

STELLINA ARGYRIADOU: Eine Frage an Herrn Türk: Wieso braucht man überhaupt einen Passwortmanager?

ANDREAS TÜRK: Weil Passwörter viele Probleme verursachen. Zum Beispiel kommt es sehr oft vor, dass dasselbe Passwort für mehrere Konten oder Webseiten verwendet wird. Umfragen haben außerdem gezeigt, dass rund ein Viertel aller Nutzer weltweit extrem triviale Passwörter verwenden.

PATRICK NEPPER: Einfache Zahlenreihen sind zum Beispiel sehr leicht zu knacken. Im Netz existieren ganze Listen mit Passwörtern, die verkauft werden.

SIBYLLE REINICKE: Kann ich denn herausfinden, ob mein Passwort schon mal geknackt worden ist?

ANDREAS TÜRK: Inzwischen gibt es den Google Passwortcheck: Er zeigt an, ob Passwörter gehackt worden sind.

PATRICK NEPPER: Als Nutzer des Browsers Chrome sind Sie automatisch geschützt. Den Google Passwortcheck haben wir nämlich direkt in Chrome eingebaut. In Zukunft werden Sie daher bei jedem Login auf einer Webseite gewarnt, wenn Ihr Benutzername und Passwort gehackt wurde.

ANTON EDER: Woher wissen Sie überhaupt, welche Passwörter geknackt wurden?

ANDREAS TÜRK: Wir haben eine Datenbank mit vier Milliarden öffentlich bekannten Passwörtern, die kontinuierlich ergänzt wird. Wir bezahlen aber nie für Passwortlisten, das würde die Kriminalität fördern.

SIBYLLE REINICKE: Ich kann also aufspüren, ob meine Passwörter im Netz kursieren. Aber mir leuchtet immer noch nicht ganz ein, warum der Passwortmanager für zusätzliche Sicherheit sorgt.

PATRICK NEPPER: Die meisten Passwörter werden per Phishing geklaut: Sie als Nutzer werden auf eine falsche Internetseite geleitet, die täuschend echt aussieht, loggen sich ein – und schon ist das Passwort dahin. Unser Browser Chrome unterscheidet automatisch zwischen echten und falschen Seiten. Wer auf einer falschen Seite unterwegs ist und seine Passwörter im Manager gespeichert hat, dem verweigert unsere Autofill-Funktion den Dienst. Sprich: Es wird nicht wie üblich das Passwort eingetragen, sobald man sich auf der falschen Seite anmelden möchte.

ANDREAS TÜRK: Seit 2018 gibt es auch die Möglichkeit, von Chrome automatisch sichere Passwörter generieren zu lassen, die gleich gespeichert werden – jedoch nur, wenn sie mit dem Google-Konto synchronisiert werden. So vermeiden wir, dass Passwörter verloren gehen.

PATRICK NEPPER: Man kann von jedem Browser auf seine gespeicherten Passwörter zugreifen. Insgesamt macht der Manager die Mobilität im Netz nicht nur angenehmer, sondern auch sicherer. Aber: Das Google-Konto gut schützen!

ANTON EDER: Sagen Sie, nehmen Sie auch externe Firmen in Anspruch, wenn es ums Entwickeln geht?

ANDREAS TÜRK: Nein, dafür ist der Komplexitätsgrad einfach zu hoch.

MICHAEL JOSITZ: Denken Sie über biometrische Daten anstelle von Passwörtern nach?

ANDREAS TÜRK: In China kann man ja bereits an so manchem Kiosk mit seinem Gesicht bezahlen. Ich finde das schwierig. Biometrie kommt bei uns nur zum Einsatz, um lokale Nutzer wiederzuerkennen. Zum Beispiel der Fingerabdruck auf dem Smartphone.

PATRICK NEPPER: Dabei soll es auch bleiben. Biometrische Merkmale gehören auf den Chip, im Netz haben sie nichts verloren. Anders als bei einem Passwort, können biometrische Merkmale nach einem Datenleck auf einer Webseite oder App nicht einfach neu generiert werden. ●

Das GSEC

Seit Jahren arbeitet Google in München an Daten- und Sicherheitsprodukten, jetzt wird das Engagement weiter verstärkt: Das Google Safety Engineering Center (GSEC) ist ein Zentrum, in dem ein sicherer Rahmen für das Internet der Zukunft entwickelt wird. Der Google-Standort in der bayerischen Landeshauptstadt wächst durch diese und weitere Anstrengungen – schon heute arbeiten in den Büros nahe der Hackerbrücke knapp 1000 Menschen.

g.co/safetyengineeringcenter

Die vier Entwickler aus dem Google Safety Engineering Center

PATRICK NEPPER arbeitet bei Google in München am Browser Chrome.

JANINA VOIGT managt bei Google eines der Privatsphäre-Teams.

CHRISTOPH SPERL hilft, dass Google-Nutzer von relevanten Neuigkeiten erfahren.

ANDREAS TÜRK entwickelte bei Google unter anderem den Passwortmanager mit.

Fotos: Lara Freiburger

Digitale Weiterbildung für alle

Die Google Zukunftswerkstatt vermittelt Fähigkeiten und Grundlagenwissen für das Leben und Arbeiten in der digitalen Welt. Vom Angebot profitieren alle – egal ob angestellt, selbstständig oder in der Ausbildung

Foto: Google/Matthias Haslauer

IN FAST ALLEN LEBENSBEREICHEN spielt das Digitale inzwischen eine große Rolle. Viele Anwendungen, zum Beispiel auf dem Smartphone, erschließen sich dem Nutzer dabei wie von selbst. An anderen Stellen kann es hilfreich sein, sich eingehender mit den Chancen und Möglichkeiten der Digitalisierung zu befassen. Die Google Zukunftswerkstatt bietet deshalb online sowie in Hamburg, Berlin und München kostenlose Kurse, mit denen jeder sein digitales Verständnis erweitern oder das Wachstum seines Unternehmens fördern kann. Unter anderem setzte die Google Zukunftswerkstatt erst kürzlich zusammen mit der Vereinten Dienstleistungsgewerkschaft ver.di und den Industrie- und Handelskammern Düsseldorf sowie München und Oberbayern die »Basisbox« auf. Sie enthält kostenfreie Grundlagentrainings der Partner zu Themen wie »Big Data und Algorithmen«, »Herausforderungen im Management der digitalen Transformation« oder auch »Datenschutz, Auftragsvergabe und Cloud-IT«. Alle Module sind im Internet abrufbar.

Doch nicht nur die berufliche Weiterbildung, auch persönliche Entwicklung spielt in den Angeboten der Google Zukunftswerkstatt inzwischen eine wichtige Rolle. Im Training »#IamRemarkable« sind die Teilnehmer eingeladen, ihre Bescheidenheit abzulegen und selbstbewusst über ihre persönlichen wie beruflichen Erfolge zu sprechen. Das Training ist interaktiv gestaltet und bindet alle mit offenen Diskussionsrunden und Übungsaufgaben ein. Gemeinsam werden Herausforderungen besprochen sowie Lösungen erarbeitet, die den Teilnehmern ein positives Gefühl und eine Sicherheit bei der persönlichen Selbstvermarktung vermitteln sollen. ●

Jetzt kostenlos anmelden

Eine Auswahl der »Basisbox«-Trainings

- **Big Data und Algorithmen**
- **Herausforderungen im Management der digitalen Transformation**
- **Datenschutz, Auftragsvergabe und Cloud-IT**

Gemeinsam lernen – vor Ort in Ihrer Nähe

Die Inhalte der Google Zukunftswerkstatt werden in Berlin, Hamburg und München vermittelt. Zudem eröffnet vom 16. bis 27. März 2020 in Düsseldorf ein Pop-up-Trainingszentrum in Kooperation mit der Handelsblatt Media Group.

Jederzeit online lernen

Entdecken Sie das Kursangebot der Google Zukunftswerkstatt – Methoden des Design Thinking werden genauso unterrichtet wie beispielsweise Grundlagen des Onlinemarketings (mit Zertifikat).

Alle Kurse finden Sie hier:
zukunftswerkstatt.de

Einfach schneller Dinge regeln

Weltweit entstehen digitale Verfahren, die dem Einzelnen mehr Kontrolle über seine persönlichen Daten geben. Die Beispiele aus der Schweiz, Belgien, Südkorea und Estland zeigen: Stets geht es darum, mithilfe von sicheren elektronischen Identitäten den Alltag im Umgang mit Behörden, Banken oder Unternehmen zu vereinfachen

Illustrationen: Katharina Bitzl

WIE WÄRE ES, wenn sich alle Online-Dienste in einem Land mit nur einem Login benutzen ließen? Dann könnte jeder mit nur einer digitalen Identität – und ohne sich in verschiedene Benutzerkonten ein- und auszuloggen – zum Beispiel ein Auto mieten, eine Jacke kaufen oder online Rechnungen überweisen. In der Schweiz soll dies durch die »E-ID« voraussichtlich ab 2021 möglich sein. Mit der staatlich geprüften und anerkannten elektronischen Identität sollen dann auch Behördengänge online abgewickelt und andere öffentliche Dienstleistungen digital genutzt werden können. Elektronische Zertifikate sorgen dafür, dass jegliche Daten verschlüsselt ausgetauscht werden und vor ungewolltem Zugriff

geschützt sind. Die Zwei-Faktor-Authentifizierung bietet zusätzliche Sicherheit, weil beim Login ein Code eingegeben werden muss, der dem Nutzer per SMS aufs Smartphone gesendet wird. Das kürzlich verabschiedete E-ID-Gesetz legt außerdem fest, dass Benutzerdaten von Identitätsdaten getrennt und nur auf Schweizer Servern gespeichert werden dürfen. Dabei entscheidet der Nutzer selbst, welche Freigaben er für welche Online-Dienste erteilt. Wofür er die E-ID einsetzt, ist von staatlicher Seite nicht nachvollziehbar.

Der Einzelne entscheidet, was er teilt

Die Stadt Antwerpen setzt ebenfalls auf digitale Identifikationstechniken, speichert die Daten allerdings dezentral: In einem Pilotprojekt soll getestet werden, wie die Verwaltung der Daten aller Einwohner per Blockchain-Technologie einfacher und sicherer werden kann. Die Blockchain-Technologie ist ein neutrales System der Informationsverarbeitung, eine riesige Datenbank, verteilt über viele Computer. Sie gilt als sehr sicher, kann kaum gehackt oder manipuliert werden. Ziel in Antwerpen ist es, den Bürgern die Kontrolle über ihre eigene digitale Identität zu geben. Im Gegensatz zu zentralen Datenbanken basiert das System auf dem Konzept der »Self-Sovereign Identity« (auf Deutsch: Selbstsouveräne Identität): Die persönlichen Daten werden nur auf dem Smartphone des Nutzers gespeichert und nicht als Benutzerkonto von Unternehmen oder Behörden verwaltet. Der Einzelne entscheidet, mit wem er welche Information teilt. Im Pilotprojekt sollen Bürger zum Beispiel ihre neue Adresse nach einem Umzug an das Einwohnermeldeamt übermitteln. Die Daten werden dabei nicht nur dezentral mithilfe der Blockchain-Technologie gespeichert, sie werden auch dezentral mit den teilnehmenden Behörden oder Unternehmen geteilt. Die Technologie ist in ihrer Funktionsweise vergleichbar mit einem digitalen Tresor. Er kann nur von denjenigen geöffnet werden, die einen Schlüssel haben; und es können auch nur jene Daten ausgelesen oder weitergegeben werden, die wirklich benötigt werden.

Nur eine ID für mehrere Bankkonten

Dezentrale digitale Identitäten werden auch in Südkorea eingeführt, das Potenzial ist dort besonders im Finanzbereich groß: Südkoreaner haben im Schnitt fünf Bankkonten und drei Kreditkarten. Der Weg zur einzelnen Online-Überweisung war, wie in vielen Ländern der Welt, bislang mit vielen Passworteingaben und Klicks verbunden. Ein Blockchain-basiertes Identifikationssystem für Finanzdienstleistungen vereinfacht die Handhabung der vielen Accounts nun: Mehr als 30 Finanzdienstleister, Versicherer und öffentliche Einrichtungen unterstützen das neu eingeführte ID-System. Per Smartphone können sich Nutzer nun ganz einfach mit jeder ihrer Banken verbinden und beispielsweise Kredite verlängern, indem sie die erforderlichen Dokumente wie Lohnbescheinigungen und Steuerbescheide digital freigeben. Die Datenhoheit behält jeder Nutzer, weil die Dokumente nicht von den Banken gespeichert werden.

Das vielleicht digitalste Land der Welt

»Wir haben eine digitale Gesellschaft gebaut«, wirbt Estland auf der Seite e-estonia.com stolz für die Errungenschaften der vergangenen zwanzig Jahre. Tatsächlich gilt das baltische Land als Vorreiter in der Nutzung digitaler Technologien zugunsten der Gesellschaft. 99 Prozent aller Verwaltungsangebote sind heute online verfügbar – selbst die Geburt eines Kindes kann den Meldebehörden vom

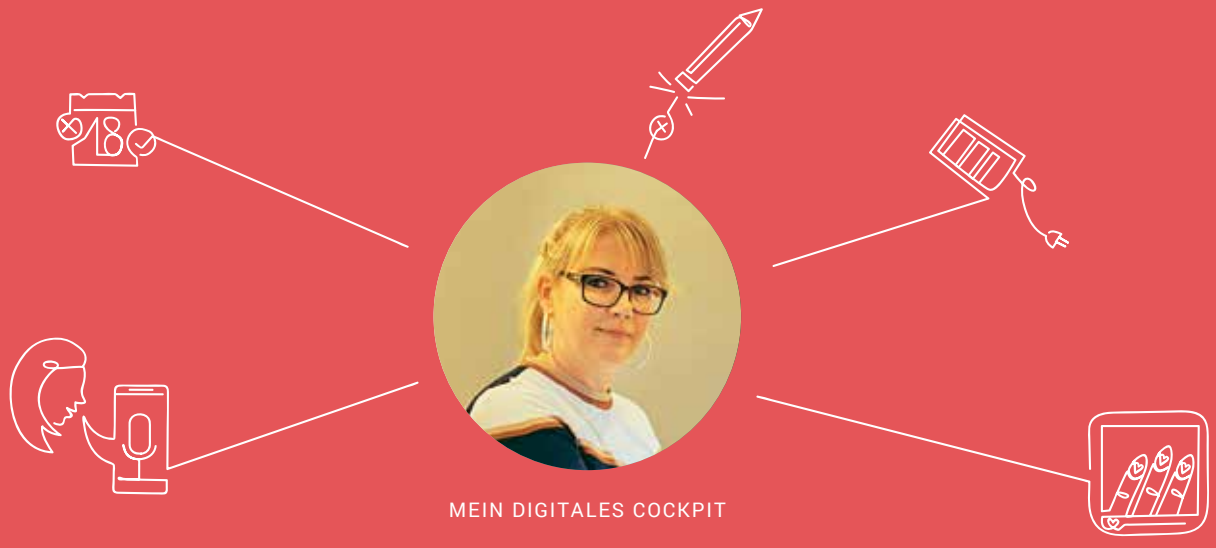
heimischen Computer aus mitgeteilt werden. 2005 war Estland das erste Land der Welt, in dem Menschen online ihre Kommunalvertreter wählten, seit 2008 machen die Krankenhäuser Patientendaten den Betroffenen online zugänglich. So haben Ärzte auch in Notfällen dank einer App Zugriff auf die Krankheitsgeschichte eines Patienten. Die Sicherheit des Systems wird dabei in Estland wie auch in anderen Ländern durch die Blockchain-Technologie ermöglicht.

Auch vor dem Schulsystem macht die Idee von der digitalisierten Gesellschaft keinen Halt: Schulnoten oder Hausaufgaben können jederzeit von Schülerinnen und Schülern sowie ihren Eltern digital eingesehen werden. ●

Der Sprachassistent hilft beim Notieren neuer Termine, Rechnungen kommen über PayPal: Yvonne nutzt für ihren Maniküre- und Pediküresalon unterschiedliche digitale Möglichkeiten.

Fotos: Felix Brüggemann

Yvonne, 42, hat ihr Nagelstudio digitalisiert: Neue Designs präsentiert sie auf Instagram, Termine reservieren Kundinnen und Kunden online. Ihre Bank sieht sie lediglich beim Einzahlen der Tageseinnahmen



MEIN DIGITALES COCKPIT

Die Geschäfte vereinfachen

»DAS ERSTE, WAS ICH MORGENS nach dem Aufstehen mache, ist, meine Termine für den Tag zu checken: Haben Kundinnen oder Kunden abgesagt? Soll womöglich ein Termin verschoben werden? Ich bin Inhaberin eines Maniküre- und Pediküresalons in Berlin-Prenzlauer Berg; meinen Laden manage ich inzwischen komplett über Tablet und Smartphone.

Das fängt bei den Terminen an, die Kundinnen und Kunden seit Anfang des Jahres online buchen können. Ich habe mich lange gegen diesen digitalen Kalender gewehrt, weil ich dachte, dass ich mit ihm die Kontrolle über mein Leben verliere. Das klingt blöd, ich weiß, aber so war es eben. Im Laden hatte ich jahrelang einen dicken Kalender, mit Bleistift trug ich dort die Termine ein. Sagte eine Kundin ab, radierte ich ihren Namen aus. Doch als immer mehr Kundinnen fragten, ob sich Termine nicht auch einfacher vereinbaren ließen, entschloss ich mich, online zu gehen. Heute weiß ich: Ich hätte es viel früher machen sollen. Mein Arbeitsalltag ist so viel einfacher geworden.

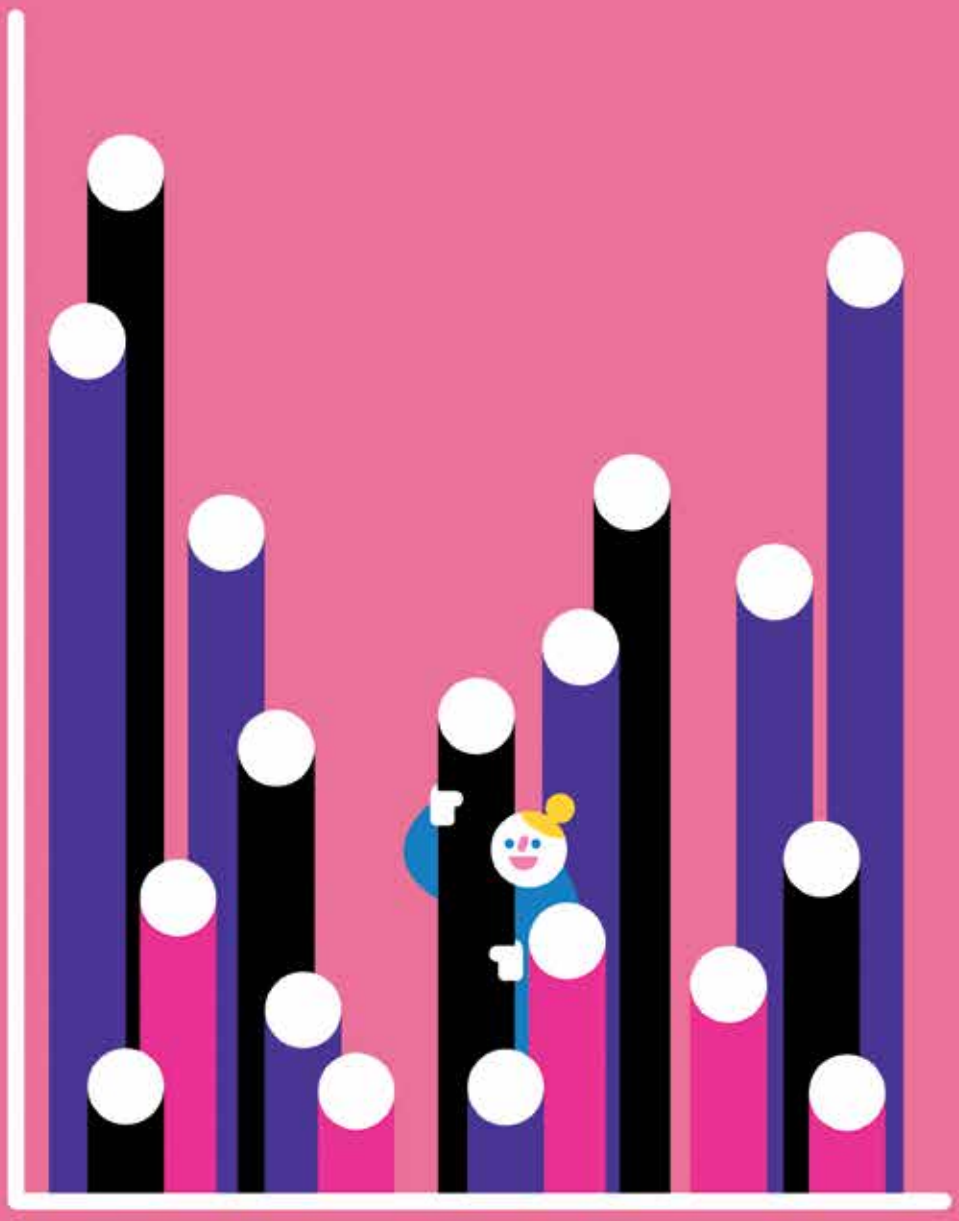
79 Apps habe ich auf meinem Handy, die Spiele für meine beiden Kinder nicht mitgezählt. Mein Smartphone nutze ich als Privatperson und als Geschäftsfrau. In den sozialen Netzwerken habe ich Accounts wie @studio_yvonne_b, wo ich zum Beispiel neue Shellac-Designs präsentiere. In eine Bankfiliale gehe ich nur noch, um die Einnahmen des Tages auf das Geschäftskonto einzuzahlen. Den Rest erledige ich über die App meiner Bank. Kundinnen können bei mir mit EC-Karte bezahlen, auch das funktioniert über eine App. Diese zeigt mir auch an, wie hoch der aktuelle Monatsumsatz ist.

Bestelle ich neue Nagellacke, Gele oder UV-Geräte, bitte ich die Händler, mir die Rechnung über PayPal zu schicken. Ich muss dann nur auf einen Link klicken, zack, fertig. Klassische Einzugsermächtigungen oder Überweisungen, für die ich extra Formulare aufrufen muss, sind mir inzwischen zu aufwendig.

In der Regel bin ich den Tag über durchgehend beschäftigt. Ein Grund, weswegen ich lieber telefoniere, als Nachrichten zu schreiben. Die Zeit, viel Text zu tippen, habe ich einfach nicht. Ruft eine Kundin an, um einen Termin zu vereinbaren, bitte ich anschließend meinen digitalen Sprachassistenten, diesen im Kalender zu vermerken.

Weil ich mein Smartphone durchgehend brauche, habe ich immer einen externen Akku in der Handtasche – ich kann es mir nicht erlauben, offline zu sein. Einmal war der Bildschirm schwarz, nichts ging mehr. Da wurde ich nervös. Wenn mein Telefon nicht funktioniert, funktioniert mein Leben nicht.« •

Die Persönlichkeit hinter den Daten schützen



Innovationen entstehen unter anderem dann, wenn Entwickler digitale Nutzerinformationen analysieren: Sie sehen Zusammenhänge und werden zu Ideen und Produkten inspiriert. Neue Methoden sorgen dafür, dass dabei der Nutzer hinter den Daten nicht mehr kenntlich wird

DER ÖFFENTLICHE NAHVERKEHR WIRD BESSER, wenn die Verantwortlichen mehr über die Menschen erfahren, die ihn nutzen: Zu welchem Zeitpunkt reisen wie viele Passagiere? Wann steigen besonders viele Mütter oder Väter mit Kinderwagen in einen Bus? Gibt es Menschen, die in der Straßenbahn arbeiten möchten? Wollen sie unterwegs Nachrichten sehen? Die Antworten auf diese Fragen sind nichts anderes als Daten, mit denen die Verantwortlichen ihr Angebot verbessern können – indem sie zum Beispiel zu Stoßzeiten mehr Waggons zur Verfügung stellen, ausreichend Stellplätze vorhalten sowie bei Bedarf WLAN oder womöglich Videoabspielflächen in den Wagen installieren. Wer mehr Informationen über Nutzer zur Verfügung hat, kann also bessere Angebote und Dienstleistungen entwickeln. Das gilt im Analogen so sehr wie im Digitalen, wo zum Beispiel Nutzerdaten eine wichtige Ressource zur Entwicklung von Innovationen darstellen.

Zugleich lassen größere Datenmengen zu einer bestimmten Person bisweilen Rückschlüsse auf die Identität zu – selbst wenn in einem Datensatz keine Adressen oder Namen verzeichnet sind. Das ist ein Problem, denn alle Menschen haben ein Recht darauf, dass ihre Privatsphäre geschützt bleibt. Die Nutzerinnen und Nutzer des öffentlichen Nahverkehrs möchten sich nicht mit ihren täglichen Fahrgewohnheiten, ihren Reisezielen und Bewegungsprofilen kenntlich machen, nur damit ein Angebot, das sie verwenden, besser wird. Viele Menschen stellen sich gern in Umfragen für medizinische Forschungsprojekte zur Verfügung, möchten ihre Angaben aber nicht mit ihrer persönlichen Krankheitsgeschichte verbunden wissen. Viele reagieren auch sensibel auf Werbetreibende, die Informationen über ihre Kunden sammeln, um Angebote maßzuschneidern.

Lässt sich zwischen dem Bedürfnis nach Innovation und Privatheit vermitteln? Tatsächlich gibt es heute Ansätze, Forschungsdrang und Datenschutz in Einklang zu bringen. Zwei dieser Methoden heißen »Differential Privacy« und »Private Join and Compute«.

Differential Privacy oder: Weiterentwicklung mit weniger Informationen

Differential Privacy wurde von der Informatikerin Cynthia Dwork gemeinsam mit anderen Forschern entwickelt und lässt sich mit einem Beispiel erklären. Angenommen, ein Unternehmen widmet sich mit seinen Produkten Autofahrerinnen und Autofahrern und möchte mehr über diese Personengruppe wissen. Im Rahmen einer Werbeanzeige auf einer Online-Plattform stellen die Verantwortlichen deshalb die Frage »Haben Sie Punkte in Flensburg?« und verbinden sie mit den Antwortmöglichkeiten »Ja« oder »Nein«.

Klickt ein Nutzer auf »Ja«, wird diese Antwort vom Programm des Online-Portals nicht einfach an das Unternehmen übertragen. Vielmehr wirft ein Algorithmus bildlich gesprochen eine Münze in die Luft. Bei »Kopf« gibt er die korrekte Antwort weiter. Liegt aber »Zahl« oben, wirft er die Münze noch ein weiteres Mal. Liegt bei diesem zweiten Wurf abermals »Kopf« (also »Ja«) oben, gibt der Rechner des Online-Portals wieder die korrekte Antwort weiter. Liegt »Zahl« (also »Nein«) oben, übermittelt er die falsche Antwort.

Die Daten aus der Umfrage werden durch dieses Verfahren absichtlich zu einem bestimmten Prozentanteil mit falschen Angaben versehen. Es entsteht ein sogenanntes Rauschen im Datensatz, Rückschlüsse auf bestimmte Identitäten sind nicht mehr möglich. Und doch sind die Daten verwendbar: Experten kennen den Prozentsatz, zu dem durch das Kopf-Zahl-Verfahren die Angaben verfälscht werden. Sie können dadurch eine Berechnung anstellen, das »Rauschen« in den Daten unterdrücken und die richtigen Ergebnisse »herausrechnen«. So bekommt das Unternehmen trotz der Verfremdung ein korrektes und nützliches Umfrageergebnis zur Ausgangsfrage.

Eingesetzt wird die Differential Privacy bereits an vielen Stellen. Für Software-Entwickler stellte Google im Herbst 2019 eine Open-Source-Bibliothek bereit, die ihnen hilft, Daten nach dem Prinzip der Differential Privacy zu analysieren. So könnten theoretisch beispielsweise die Programmierer eines App-basierten Fahrradverleihdienstes zwar einsehen, wann welches Fahrrad ausgeliehen und wo es wieder abgestellt wurde – nicht aber, wer es benutzte. Die Privatsphäre bliebe geschützt und relevante Daten würden dennoch übermittelt. Google will an dieser Stelle zu mehr Datenschutz im Digitalen beitragen.

Private Join and Compute oder: Daten verschlüsselt teilen und nutzen

Besonders viel Erkenntnisgewinn kann entstehen, wenn Datensätze verknüpft werden. Angenommen, die Inhaber von Geschäften in einem Stadtviertel werben bei den Verantwortlichen des öffentlichen Nahverkehrs um einen besseren Bus- oder Bahn-Anschluss, weil sie ihre Umsätze steigern möchten. Dann entstehen Fragen: Wie viele Menschen fahren bislang ins Stadtviertel? Wie viel Geld geben sie dort aus? Ist die Annahme der Geschäftsleute richtig? Für die Antworten auf diese Fragen sind Datenanalysen nötig. Allerdings dürfen die Verantwortlichen des Nahverkehrs womöglich ihr Wissen um Passagierbewegungen nicht einfach mit anderen teilen, während die Unternehmer ihr Wissen um die Ausgaben der Menschen nicht weitergeben möchten. Mit dem Programmiergerüst des »Private Join and Compute«, das bei Google entwickelt wurde, können beide Seiten ihre Daten verschlüsseln und es der jeweils anderen für statistische Berechnungen zur Verfügung stellen. Durch doppelte Verschlüsselung ist es beiden Parteien möglich, statistische Erkenntnisse zu vereinen, ohne persönliche Daten auszutauschen. Im Ergebnis stehen verwendbare Informationen, aus denen sich wesentlich weniger Rückschlüsse auf die Identität einzelner Personen ziehen lassen. Und die Unternehmer und die Verantwortlichen des Nahverkehrs können dennoch errechnen, wie viel Geld ein Passagier durchschnittlich in dem bewussten Stadtviertel ausgibt. Ein Fortschritt für beide Seiten sowie für den Schutz der Privatsphäre. •

Illustration: Sven Kalkschmidt

Stefan Vollmer, Chief Technology Officer beim TÜV Süd, erklärt, wie sich digitale Anwendungen prüfen und zertifizieren lassen – und wie jeder seine Privatsphäre schützen kann

» Ich weiß bis ins Detail, welche Daten ich im Netz preisgebe «

Herr Vollmer, der TÜV prüft traditionell Produkte und Anlagen. Wann brauchen digitale Anwendungen eine technische Überprüfung?
Seit der Gründung vor mehr als 150 Jahren ist es die Mission von TÜV Süd, Menschen, Umwelt und Sachgüter vor technischen Risiken zu schützen. Sobald digitale Anwendungen für breitere Zielgruppen oder den Massenmarkt zum Einsatz kommen, ist technische Überwachung wichtig, um die Risiken zu beherrschen. Das gilt umso mehr, wenn Digitalisierung mit der Vernetzung von Geräten einhergeht. Denn eine vernetzte Welt bietet ein Vielfaches an Angriffsmöglichkeiten.

Sie meinen Haushaltsgeräte oder Autos, die über das Internet der Dinge verbunden sind?
Ja, zum Beispiel. Aber auch kritische Infrastruktur wie Energieversorger und Kliniken oder vernetzte Fabriken sind gefährdet.

Macht es einen Unterschied, ob der TÜV analoge Geräte oder digitale Systeme prüft?
Der größte Unterschied ist die Dynamik. Wenn ein analoger Aufzug einmal jährlich geprüft wird, ändert sich dazwischen wenig. Es kommt nichts Neues hinzu. Digitale Produkte dagegen können kurz nach der Prüfung aktualisiert werden und sich verändern. Deshalb entwickelt sich Cyber Security hin zu kontinuierlichen Überprüfungen. Es reicht nicht, einmal im Jahr eine Checkliste abzuhaken.

Sind Sie dann dauerhaft mit den jeweiligen Systemen oder Geräten verbunden?
Technische Prüfung funktioniert auch ohne Verbindung zum Gerät. Man kann den Stand der Software abspeichern und nur sie permanent samt Aktualisierungen überprüfen. Tauchen dort Fehler auf, gibt es wahrscheinlich auch im Gerät ein Problem – beziehungsweise in vielen Tausend oder Millionen Geräten.

Geht es in Ihrer Arbeit mehr um Datenschutz oder um Cyber Security?
Um beides, wobei meist das eine auf dem anderen aufbaut. Die Europäische Datenschutz-Grundverordnung bildet die wichtigste rechtliche Grundlage in der digitalen Welt. Smarte Haushaltsgeräte etwa speichern oder verarbeiten personenbezogene Daten, damit sie einen Mehrwert bieten. Damit fallen sie unter die Datenschutzgesetze und müssen sicher vor Angriffen sein – dazu aber gibt es oft keine verbindlichen technischen Vorgaben.

Wie kann ich dann erkennen, ob ein vernetztes Gerät sicher ist?
Der TÜV-Verband und andere arbeiten an einem Zertifikat für vernetzte Geräte. Im Idealfall signalisiert ein TÜV-Siegel – oder ein Zeichen anderer Prüfgesellschaften – Verbrauchern, dass sie dem Gerät vertrauen können. Dafür müssen einheitliche Minimalanforderungen der IT-Sicherheit definiert werden.

Interview: Christoph Henn | Foto: Constantin Mirbach

Können für unterschiedliche Arten von vernetzten Produkten überhaupt einheitliche Kriterien gelten?
Minimale IT-Standards betreffen alle. Sie müssten etwa sicherstellen, dass ein Gerät regelmäßig mit Updates versorgt werden kann, um Sicherheitslücken zu beseitigen. Oder sie müssten den Anwender zwingen, bei der Inbetriebnahme ein individuelles Passwort festzulegen. Heute gibt es oft ein Standardpasswort. Wer es kennt, kann sich auf alle Geräte gleicher Bauart einloggen.

Neben vernetzten Geräten prüfen Sie unter anderem Webseiten, IT-Systeme und ganze Unternehmen, etwa mit Test-Angriffen. Wie viele sind absolut sicher?
Niemand ist zu 100 Prozent geschützt vor Cyber-Attacken. IT-Sicherheit hängt von drei Faktoren ab: Technologie, Menschen und Prozesse. Wir sind in allen drei Bereichen gleichermaßen aktiv. Früher haben sich viele auf Technologie wie Virenschutzprogramme verlassen. Das hilft aber wenig, wenn der Mensch als schwächstes Glied Fehler macht – etwa auf einen Link in einer bösartigen Mail klickt oder einen manipulierten USB-Stick in den PC steckt. Deshalb ist Aufklärung sehr wichtig. Zum anderen haben die Prozesse an Bedeutung gewonnen. Wenn man davon ausgeht, dass sich Angriffe nicht komplett verhindern lassen, sollte man zumindest optimal darauf reagieren, um den Schaden gering zu halten – so wie jeder im Unternehmen wissen sollte, wo der Feuerlöscher steht oder welche Nummer bei einem Brand zu wählen ist.

Wie können Verbraucher erkennen, ob ein digitaler Dienst sicher ist?
Grundsätzlich sind nur Webseiten sicher, die nach dem HTTPS-Standard verschlüsselt sind – zu erkennen in der Adressleiste. Zudem gibt es Prüfzeichen für Onlineshops. Um zu prüfen, ob diese Siegel gültig und nicht gefälscht sind, können Verbraucher daraufklicken. Sie sollten dann auf die Webseite des Prüfhauses gelangen. Dort sieht man, was genau geprüft wurde und ob das Zertifikat noch gilt.

Wo lauern aktuell die größten Gefahren für Verbraucher und ihre Daten im Netz?
Viele tun sich schwer damit, seriöse von unseriösen Webseiten zu unterscheiden, und vertrauen zum Beispiel blind auf den billigsten Anbieter eines Produkts. Ich persönlich hinterlasse meine Daten nur auf Webseiten, die ich kenne. Das ist meine Grundregel.

Nach Stationen als Bundesbeamter im öffentlichen Dienst und bei Airbus kam Stefan Vollmer zur TÜV Süd Sec-IT, der auf IT-Sicherheit spezialisierten Geschäftseinheit des TÜV Süd. Als Chief Technology Officer ist er dort für die Entwicklung neuer Services zuständig.

Was empfehlen Sie noch?
Jeder sollte mindestens zwei E-Mail-Adressen nutzen: eine für persönliche und finanzielle Angelegenheiten und eine für Onlineshopping, Newsletter und Ähnliches. Außerdem sollte man bewusst mit Daten umgehen. Dazu gehört, dass man seine Bankdaten nicht in Onlineshops speichert. Oder würden Sie im Kaufhaus dauerhaft Ihre Kreditkarte abgeben?

Wie verhindere ich das, wenn ich bequem online einkaufen will?
Ich empfehle grundsätzlich Passwort-Safes oder Passwortmanager: Diese Programme speichern unterschiedliche und sichere Passwörter für jeden Ihrer Accounts, Sie brauchen sich aber nur ein Master-Passwort merken. In diesen Safes lassen sich auch Kreditkarteninformationen speichern und mit einem Klick beim Bezahlvorgang eintragen. Zusätzlich nutze ich eine Zwei-Faktor-Authentifizierung, bei der mir vor jedem Einloggen ein Code aufs Smartphone geschickt wird.

Was ist mit den Daten, die ich beim Surfen im Internet hinterlasse? Raten Sie dazu, anonym unterwegs zu sein?
Sie können das ausprobieren, aber es wird keinen Spaß machen, weil dadurch die Personalisierung und damit Komfort verloren geht. Aber man kann bei allen großen Online-Diensten und Browsern die Privatsphäre-Einstellungen regulieren. Ich jedenfalls tue das und weiß bis ins Detail, welche Daten ich im Internet preisgebe. ●

Wie verändern wir uns, wenn das Leben digital wird? Wie müssen wir Technik denken, die unsere Persönlichkeit und unsere Bedürfnisse spiegelt? Auf Einladung des Google Safety Engineering Center (s. Seite 20) trafen sich Forscher, Künstler und Philosophen zum »World Frontiers Forum« in Berlin und widmeten sich der Frage, wie wir eine humanistische Vision unserer digitalen Identität entwickeln und realisieren können

Das Ich im Digitalen

EIN MÄCHTIGES THEMA hatten sich die Teilnehmer des »World Frontiers Forum« (WFF) mit der Frage nach einer wünschenswerten Architektur für unsere »digitalen Identitäten« gegeben. Der Begriff bezeichnet nicht nur die digitale Version des Personalausweises – digitale Identität ist die Summe der Daten, die wir mit unseren Nutzerkonten oder Cookies bei unseren Bewegungen im Digitalen hinterlassen. Diese Daten sind sehr viel wert, sagte etwa der Informatiker Alex »Sandy« Pentland beim WFF: Er rief dazu auf, Daten als einen Wertstoff wie Land, Arbeitskraft oder Kapital zu behandeln.

Rechtsprofessor Lawrence Lessig von der Harvard University blickte aus anderer Richtung auf das Thema. Er verwies darauf, dass manche Länder digital immer mehr Wissen über ihre Bürger sammeln, um sie besser kontrollieren zu können. Andere Staaten wiederum erfassen Menschen digital und geben ihnen auf diese Weise eine Identität, mit der sie Zugang zu Gesundheitsvorsorge oder Versicherungen erhalten. Digitale Identität kann also systemische Kontrolle, aber auch Ermächtigung des Einzelnen durch Zugang zu Informationen, Wissen und Diensten ermöglichen.

Überhaupt vereint der Begriff vielfältige Facetten, das wurde beim WFF deutlich. Biologin Michal Preminger zeichnete das Bild einer Zukunft, in der jeder Mensch eine Art digitalen Zwilling hat, mit dem sich errechnen lässt, welche Wirkung eine Entscheidung erzeugt, die wir heute treffen: Wie beeinflusst das, was wir essen, sehen oder lernen, das Ich der Zukunft? Mit einem digitalen Zwilling ließe sich potenziell genau das vorhersagen.

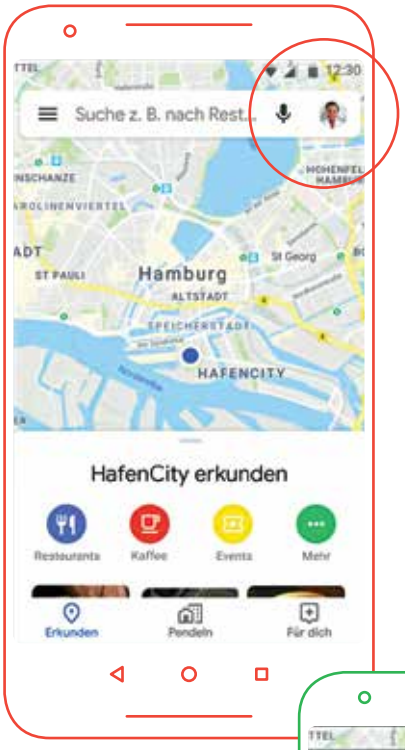
Ein Gedanke zog sich durch viele der WFF-Debatten: Die Digitalisierung verändert uns und dadurch unser Selbstbild im Digitalen. Deshalb sollten wir darüber nachdenken, was uns ausmacht, was uns wichtig ist – und was es für das Technologiedesign der Zukunft bedeutet. ●

Eine Ideen- und Gedankenbörse mit Teilnehmern aus der ganzen Welt: Erfahren Sie mehr über »The World Frontiers Forum« unter: worldfrontiersforum.org

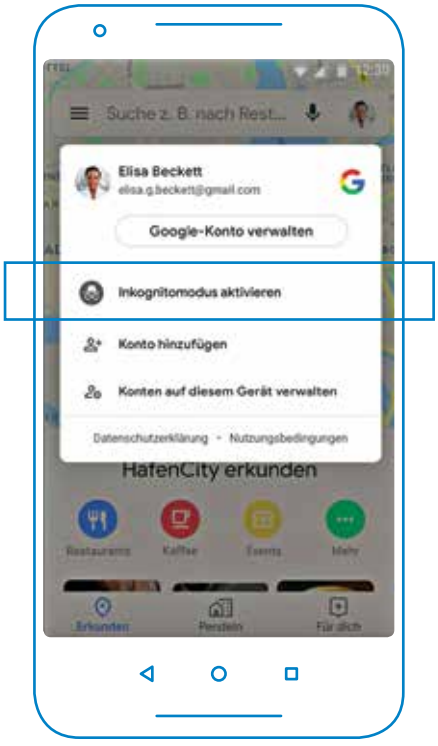
Fotos: Jessica Safko/WFF

Der Inkognitomodus bei Google Maps

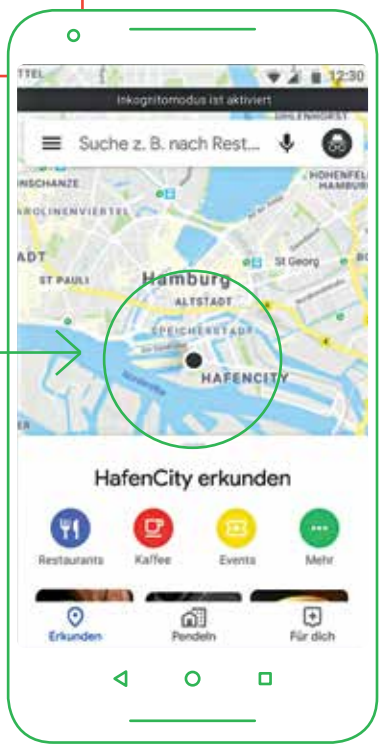
Sie möchten, dass Google Maps Ihre Routen oder Suchen nicht in Ihrem Google-Konto speichert? Kein Problem: So leicht aktivieren Sie den Inkognitomodus bei Google Maps



1. Öffnen Sie die Google Maps App und tippen Sie auf Ihr Profilbild oben rechts.



2. Tippen Sie nun auf die Zeile »Inkognitomodus aktivieren«.



3. Der Standortpunkt verändert seine Farbe: Ihre Aktivitäten in Google Maps werden nicht in Ihrem Google-Konto gespeichert.

UNSER TIPP

Prüfen Sie in Ihrem Google-Konto die Einstellungen für Web- und App-Aktivitäten und anschließend die Settings für den Standortverlauf. Dort können Sie generell entscheiden, ob Ihr Standort und andere Aktivitätsdaten im Google-Konto gespeichert werden sollen. Weiteres auf **meinkonto.google.de** sowie auf **g.co/datenschutz**

Wie erreiche ich meine Kunden online? Wie erstelle ich eine Webseite für mein Unternehmen? Wie eröffne ich einen Onlineshop? Wie werde ich in den Suchergebnissen gefunden? Wie funktioniert Suchmaschinenwerbung? Wie entwickle ich eine Onlinestrategie? Wie nutze ich Social Media für mich und mein Unternehmen? Wie funk international expandier en auf meiner Webseit ten besser erreichen? Wie find oogle Maps? Wie nutze ich Vide e ich aus Daten die Internehmensprofil in den Suchergebnissen? Wie funktioniert maschinelles Lernen? Wie vermeide ich Sicherheitslücken beim Onlinegeschäft? Wie kann ich agiles Arbeiten im Unternehmen einführen? Wie fördere ich unternehmerisches Denken und Handeln im Unternehmen? Wie entwickle ich neue Geschäftsmodelle? Wie kann ich mein Auftreten in Bewerbungsgesprächen verbessern? Wie schütze ich mich online? Wie kann ich produktiver arbeiten? Wie kann ich Probleme kreativ lösen? Wie spreche ich selbstbewusst über meine Erfolge?

Neue Fähigkeiten für Ihren Erfolg in der digitalen Welt

Machen Sie sich mit kostenlosen Trainings fit für die Digitalisierung – online und vor Ort in Berlin, Hamburg und München.

Jetzt anmelden

zukunftswerkstatt.de

Google Zukunftswerkstatt