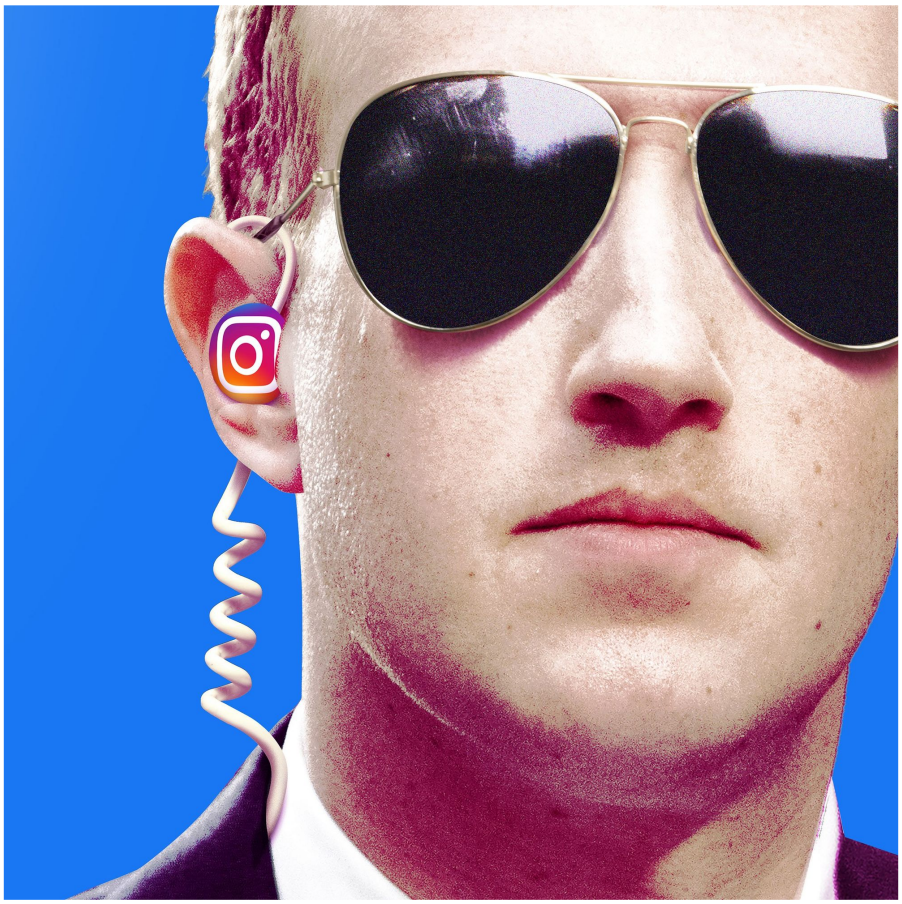
Nein, Instagram hört (sehr wahrscheinlich) nicht Ihr Handy ab

Sie haben am Telefon über Verhütungsmittel geredet und sehen danach im Internet Werbung für Verhütungsmittel. Ist das Zufall? Oder werden Sie von Facebook und Co. belauscht? Was wir darüber wissen.

Von Adrienne Fichter, Marie-José Kolly (Text) und Doug Chayka (Illustration), 27.10.2021



Chef von Facebook, zu dem auch Instagram gehört: Was weiss Mark Zuckerberg über uns?

Bei vielen Fragen foutierte sich Mark Zuckerberg, er vertröstete auf später oder wusste schlicht die Antwort nicht: *«I can have my team follow up with you»,* sagte er etwa. Als Senator Gary Peters den Facebook-Gründer in den Tech-Hearings von 2018 aber fragte, ob Facebook seine Nutzer über die Smartphone-Mikrofone abhöre, antwortete Zuckerberg ganz klar: «Nein.»

Wirklich nicht?

Der Verdacht hält sich. «Mein Phone hört mit» ist eine der hartnäckigsten Legenden des Internets. Auch die Redaktion der Republik erreichen immer wieder Zuschriften zu dieser Frage. Etwa: Sie haben gestern beim Kaffee über einen bestimmten Staubsauger gesprochen (ja, das bedeutet auch: Sie sind nicht mehr ganz so jung, wie Sie gerne wären). Und nun zeigt Ihnen Facebook ausgerechnet heute Werbung für dieses Produkt.

Wir haben die technische sowie die psychologische Literatur dazu gelesen und mit Privacy-Forscherinnen gesprochen. Viele Teilantworten können wir Ihnen am Beispiel des Facebook-Universums geben: weil es dank vieler Medienenthüllungen am besten dokumentiert ist und weil einige seiner Dienste Werbung anzeigen. Werbung – vielleicht für einen Staubsauger, vielleicht für ein Verhütungsmittel –, die eben den Verdacht weckt, dass die App via Smartphonemikrofon mitgehört hat, als man sich am Vorabend in intimer Runde über ein bestimmtes Produkt unterhalten hatte.

Belauschen also Facebook, Google, Amazon und Co. Sie rund um die Uhr?

Die kurze Antwort Stand jetzt: mit grosser Wahrscheinlichkeit nicht.

Erstens aus einem sehr einfachen Grund nicht: Die grossen Techfirmen haben das gar nicht nötig. Ihre Browser-Historie, Ihre Suchmaschinenabfragen, Ihre App-Nutzungsdaten, Ihre Standortdaten, Ihre Einkäufe: Sie alle verraten mehr als genug. Sie verraten insbesondere, was Sie zurzeit interessiert, woran Sie gerade denken. Und das sind gute Hinweise auf das, worüber Sie auch mit anderen reden. «Man kann durch die Überwachung des Standorts, der Surfgewohnheiten, der Interaktion mit Anwendungen und vieler anderer Metadaten zuverlässig und ausserordentlich präzise auf die Vorlieben einer Person schliessen», sagt der Privacy-Forscher und Professor Juan Tapiador, der an der Universität Carlos III de Madrid lehrt.

Zweitens müssen wir auf eine weitere bittere Wahrheit verweisen, die erklären kann, warum Sie jene Staubsaugerwerbung sehen. Sie denken zwar, es könne kein Zufall sein, dass ausgerechnet Sie – Sie mit Ihrem ganz spezifischen Geschmack, Ihren individuellen Interessen, Ihrem Wissen und Ihren Gesprächen –, dass eben Sie diese Werbung sehen und nicht eine andere. Höhere Mächte müssten das geplant haben, denn es passt einfach zu perfekt. Wir müssen Sie enttäuschen: Wie wir noch sehen werden, sind Sie leider nicht ganz so einzigartig, wie Sie denken könnten.

Drittens spielt Ihnen Ihre Kognition den einen oder anderen Streich. Sie sind leider auch nicht ganz so vernunftgetrieben, wie Sie denken könnten.

Und viertens müssen wir, ebenfalls leider, sagen: Dass Sie abgehört werden, ist grundsätzlich nicht ausgeschlossen. Aber die Belauschung kommt vermutlich nicht aus der Richtung, in die Sie bisher geschaut haben.

Lassen Sie uns die detaillierteren Antworten Schritt für Schritt durchgehen.

1. Ich habe gestern beim Kaffee zum ersten Mal über diesen Staubsauger gesprochen, heute sehe ich auf Facebook Werbung für das Ding. Das kann doch kein Zufall sein?

Kann es doch. (Zu den technischen Details kommen wir gleich. Lassen Sie uns aber kurz über den Zufall sprechen.)

Wir Menschen sind Expertinnen im Erkennen von Mustern. Wir sind geradezu dafür geschaffen, aus solchen Mustern Zusammenhänge abzuleiten: So lernen wir von Geburt an, wie unsere Umgebung funktioniert. Und so eignete sich unsere Spezies im Lauf ihrer Geschichte immer mehr Wissen an.

Eine sehr nützliche Fähigkeit also, die aber einen Nachteil hat: Wir interpretieren Begebenheiten, die nur zufällig gemeinsam auftreten, *zu* häufig als bedeutsamen Zusammenhang. Und je mehr wir über die Welt schon wissen – je mehr Zusammenhänge wir schon kennen –, desto häufiger begegnen wir auch Regelmässigkeiten, die eben nicht durch einen Kausalzusammenhang entstanden sind, sondern durch Zufall.

Es entspricht unserer Natur, mutmassliche Zufälle tendenziell mit Argwohn zu betrachten. Wir tun aber ganz gut daran, diese Tendenz im Hinterkopf zu behalten: Denn vieles von dem, was auf den ersten Blick nach einer Verschwörung aussieht, kommt durch ganz banale Zufälle zustande.

1a. Okay, vielleicht ein Zufall. Gibt es alternative Erklärungen?

Sie haben also den Namen dieses Produkts oder der Produktkategorie gestern zum ersten Mal verbal ausgesprochen. Dennoch ist die Wahrscheinlichkeit hoch, dass Sie – vielleicht unbewusst – vorher schon damit in Kontakt gekommen sind. Die cleveren Techniken der Werbeindustrie sind gut dokumentiert: Sie verfolgt Ihre digitale Reise mittels Ihrer Browser-Historie und mittels geräteübergreifender Identifizierung. Das heisst: Was Sie auf dem Smartphone suchen und sehen, weiss auch Ihr Tablet oder Ihr Laptop. Sämtliche Tracker – kleine Programme, die Ihnen im Internet folgen – sind in Websites von Medienunternehmen, E-Commerce-Shops und in fast alle öffentlich zugänglichen Websites integriert. Dasselbe gilt für Smart-

phone-Apps. All diese Dienste wissen sehr gut darüber Bescheid, wann Sie sich wo im Internet herumtreiben und was Sie dabei tun.

Rekonstruieren wir dies doch am Beispiel Facebook: Der soziale Riese integriert seit 2014 ganze Browser-Historien in die Nutzerprofile. Also quasi: Ihre ganzen Reisen ausserhalb des Facebook-Universums werden mitverfolgt und in den Datenkosmos eingespeist.

Doch wie ist das möglich? Jeder «Gefällt mir»- oder «Teilen»-Button sowie das allgemeine Facebook-Pixel, das ja auch auf vielen Websites ausserhalb von Facebook integriert ist, übermitteln die URL der entsprechenden Seite und damit auch die Information darüber, was Sie gerade lesen, an Facebook.

Der Konzern weiss dann zum Beispiel, welche politischen Seiten Sie angesurft haben (zumindest wenn die entsprechende Partei das Pixel integriert hat). Und er weiss, dass Sie sich gerade für Haushaltsgeräte interessieren. All das geschieht, damit Parteien oder Unternehmen Ihnen «relevantere» Werbung auf Instagram und Co. ausspielen können.

Sie brauchen also den Namen des Staubsaugers nicht laut ausgesprochen zu haben – Facebook hat andere Mittel, um zu wissen, dass Sie für dieses Haushaltsgerät zum jetzigen Zeitpunkt sehr empfänglich sein könnten.

1b. Aber Ähnliches ist auch meiner Cousine passiert. Und sie hat weder ein Facebook-Konto noch die Instagram-App

Dennoch ist sie leider nicht vor dem Datenhunger des Facebook-Universums geschützt. Es spielt keine Rolle, ob sie Instagram oder Facebook überhaupt nutzt. Das Facebook-Pixel aus anderen Websites folgt ihr dennoch, denn Facebook erstellt für jede Nicht-Nutzerin ein Schattenprofil. Übrigens kommt es bei Ihnen, die Sie Facebook und Instagram nutzen, auch nicht gross darauf an, ob Sie dabei eingeloggt sind oder nicht: Ihre Bewegungen im Netz gehen so oder so an Facebook (sofern eben die von Ihnen besuchten Websites die kleinen Datenspione integriert haben).

Hinzu kommt: Ihre Cousine nutzt vielleicht keine Facebook-Dienste, dennoch aber Google oder Amazon oder andere Tech-Dienstleister. Unangefochtener Platzhirsch im Tracking-Business ist Alphabet, die Dachgesellschaft von Google. Eine Studie der Universität Oxford zeigt, dass Googles Tracker in über 88 Prozent der analysierten Apps integriert waren. Google sieht also, ähnlich wie Facebook, auch ausserhalb von Google.com verdammt viel von dem, was vor sich geht. (In einer jüngst veröffentlichten Anklageschrift aus den USA wird übrigens deutlich, *wie sehr* die beiden Konzerne anhand von Absprachen ihre Monopole im Online-Werbemarkt gegenseitig stärkten.) Und das alles, weil Sie für den Download Ihrer Gaming-App ein Häkchen unter die Nutzungsbedingungen gesetzt haben und damit Google, Werbefirmen und Co – wahrscheinlich unwissentlich – eine Lizenz zur freien Datenverwertung erteilten.

Folgendes passiert zum Beispiel, wenn Ihre Cousine etwa am Morgen beim Kaffee die Website Tagesanzeiger.ch aufruft:

- Die Analysetools von Google untersuchen ihr Verhalten auf dem Nachrichtenportal.
- Zudem wird Ihre Cousine vom Google-Subunternehmen Doubleclick einer Kunden-ID zugeordnet.

– Nun stürzt sich eine ganze Armada von Akteuren auf ihre Daten, sobald sie einen Artikel aufruft. All diese Akteure nehmen an einer millisekundenschnellen Echtzeitauktion teil (noch während der Artikel auf ihrem Smartphone geladen wird).
– Die Aufmerksamkeit und die Daten Ihrer Cousine werden dann an jenes Unternehmen «versteigert», in dessen Werbegruppen sie passt.
– Dieses Unternehmen darf Werbung an Ihre Cousine ausspielen (und bezahlt dafür), doch alle anderen profitieren ebenfalls mit: Sowohl der Auktionsvermittler Doubleclick wie auch Datenhändler und digitale Werbedienstleister sowie weitere mitbietende Unternehmen wissen von ihrem Besuch beim «Tages-Anzeiger» und integrieren dieses «Interesse» in das Werbeprofil über Ihre Cousine. Auch ohne dafür bezahlt zu haben.

2. Kann ich mich vor diesem Tracking schützen?

Jein. Es gibt zwar durchaus wirksame Blocker wie etwa Privacy Badger oder uBlock Origin (auch um die unliebsame Werbung von Ihnen fernzuhalten). Doch die datenhungrige Werbeindustrie hat leider eine Reihe von Ausweichtaktiken erfunden. Etwa das Browser-Fingerprinting, also die Grundeinstellungen in Ihrem Browser, der alle von Ihnen angesteuerten Websites weiterverrät und Sie ziemlich zuverlässig identifizieren kann. (Mit diesem Tool finden Sie selber heraus, wie einzigartig Ihr Browser ist.)

Auch wenn Sie tunlichst darauf achten, weder in sozialen Netzwerken noch auf Suchmaschinen Spuren zu hinterlassen: In jedem neuen Android-Smartphone gibt es eine Reihe von vorinstallierten Apps. Sie erkennen diese gleich, wenn Sie Ihr neues Smartphone zum ersten Mal in Betrieb nehmen. Einige davon haben sogar die Relevanz einer Systemkomponente, wie etwa die vorinstallierte Telefon-App, sind also verwoben mit der Hardware Ihres Geräts. Andere wirken eher beliebig, wie Wetter-Apps.

Doch was nach Beliebigkeit aussieht, geht auf handfeste geschäftliche Deals zwischen Smartphoneherstellern (Samsung), Betriebssystemanbietern (Android gehört Google), Mobilfunkunternehmen (zum Beispiel Swisscom) und Big-Tech-Konzernen (Amazon) zurück.

Eine Studie von 2019 zeigt zum Beispiel, dass diese «privilegierten» Apps gespickt sind mit allerlei Datenspionen für die Big-Tech-Firmen und die Werbeindustrie. Das bedeutet im Klartext: Obwohl Sie Ihr nigelnagelneues Smartphone erst taufrisch gekauft haben, ist es bereits voll mit Code von Amazon, Twitter, Facebook, Microsoft und Netflix. Und dieser Code saugt einiges ab, dem Sie vorher nicht zugestimmt haben.

Big Tech und zahlreiche weitere beteiligte Firmen erhalten im Hintergrund automatisch «Sonderberechtigungen» auf persönliche Kennungen wie Ihre IMEI-Nummer (das ist Ihre eindeutige Mobile ID, die eindeutige Seriennummer jedes Telefons) oder Ihre Advertising ID (Ihre Werbeidentität). Und sie haben teilweise Zugriff auf SMS-Metadaten und Ihre Netzwerkkonfiguration: Sie wissen also, wem Sie wann geschrieben haben und wer Ihnen. Und noch schlimmer: «Diese Berechtigungen können auf den Geräten nicht zurückgesetzt werden», sagt Juan Tapiador.

Zwar können Sie versuchen, diese Apps manuell zu deaktivieren, aber es ist fraglich, ob Ihr Smartphone danach noch richtig funktioniert.

3. Ich habe auf meinem Smartphone den Standort nicht freigegeben. Wie kann Google wissen, dass ich in diesem Kleidergeschäft war?

Unsere Mobilität ist eine wahre Datengoldgrube. Ihren Aufenthaltsort werden Sie kaum vor Big Tech, Ihrem Mobilfunkanbieter oder Werbeunternehmen verbergen können. Da können Sie sich noch so bemühen.

Sollten Sie zum Beispiel regelmässig eine Freundin in Ihrem Lieblingscafé treffen, so verraten Ihre gemeinsamen GPS-Daten Ihre Verbindung. Und plötzlich werden Ihnen die neuen Kopfhörer irgendwann angezeigt, die Ihre Freundin ein paar Mal googelte.

3a. Ich habe doch gesagt: Den Standort NICHT freigegeben

Genau, wir haben Sie gehört. Sie haben die Standortfreigabe ausgeschaltet. Aber Ihre IP-Adressen und Ihre MAC-Adressen (die Adressen Ihres Geräts) können Sie nicht verbergen. Und die sind verräterisch: In Kombination mit anderen sogenannten *identifiers* lässt sich immer sicherstellen, dass *Sie* auch tatsächlich *Sie* sind. Sofern Sie kein VPN oder den Tor-Browser beim Aufruf von Websites benutzen, kann Ihr Gerät mit wenigen Klicks geortet werden.

Anhand solcher Ortsdaten lassen sich ganze Bewegungsprofile erstellen – und die verraten eine ganze Menge über Sie. Sie geben Aufschluss über Ihre sexuelle Orientierung (vielleicht waren Sie gestern in einer Gay-Bar), Ihren Gesundheitszustand (Sie waren mehrmals beim Arzt), Ihren Reichtum (Sie verkehren in bestimmten Milieus) wie auch Ihre Religion (wie oft waren Sie in welchem Gotteshaus?). Alles wertvolle Informationen, die an App-Entwicklerinnen, an Google, Facebook und viele Werbeunternehmen fliessen werden, die Sie, vielleicht nach dem Besuch in einer Szenebar oder einer Kirche, mit «passender» Werbung beliefern möchten.

Und auch wenn Sie in Ihrem Lieblings-«Starbucks» im öffentlichen WLAN niemals Instagram aufrufen und schon gar nicht auf Amazon.com surfen, sondern lediglich ab und zu die News checken und sonst einfach ein Buch lesen: Die auf den Newsportalen integrierten Tracking-Pixel – Sie erinnern sich – werden Ihren Standort trotzdem an Big-Tech-Unternehmen ausliefern. Und diese ziehen das Fazit: Sie mögen wohl «Starbucks»-Kaffee.

Übrigens gibt es noch einen Twist: Auch ohne diese Ortung können Detailhandelsunternehmen Sie mit lokaler Werbung in den sozialen Netzwerken beliefern. Denn bei Facebook gibt es die sehr umstrittene Funktion «Custom Audiences»: Damit lassen sich Offline- und Online-Welt verknüpfen, etwa indem ein Schuhgeschäft sein Kundenbonusprogramm (denken Sie an das Migros-Cumulus-Programm oder die Coop-Supercard) in das Facebook-Datenuniversum einspeist. Durch den Abgleich der Kundenlisten mit der Facebook-Nutzerdatenbank (Name, Vorname, E-Mail-Adresse oder Geburtsdatum reichen) erfährt Facebook, dass Sie soeben bei diesem Schuhgeschäft eingekauft haben. Das Geschäft – ein Werbekunde von Facebook – könnte Ihnen nun auf Instagram die neuesten Sneakerschuhe als Werbung präsentieren. Und das, obwohl Sie auf keinem digitalen Gerät nach irgendwelchen Schuhen gesucht haben.

4. Ich habe ein Produkt auf meinem Computer angeschaut. Nun sehe ich Werbung dafür auf dem Smartphone

Auch wenn Sie zum Beispiel Netflix-Serien nur auf einem internetfähigen Samsung-Fernseher schauen, ist es trotzdem möglich, dass Sie danach auf Ihrem Computer Serientipps dieser Streamingplattform erhalten.

Das kann mehrere Gründe haben:

1. Sie nutzen für das Benutzerkonto Ihres Fernsehers und das Ihres Computers dieselbe E-Mail-Adresse.
2. Wenn nicht: Sie sind mit Computer und Fernseher im gleichen Netzwerk eingeloggt. Damit kommunizieren Ihre Geräte nach aussen dieselbe IP-Adresse.

Sie sehen: Es gibt immer eindeutige *identifiers,* die *Sie* als *Sie* und damit als Besitzer unterschiedlicher Geräte identifizieren und orten. Sollten Sie das eine ausschalten, so weicht die datensammelnde Armada auf ein anderes aus. Sie verknüpft, kombiniert und sammelt weiter.

5. Ich habe gestern mit einer Freundin telefoniert und über ein neues Verhütungsmittel gesprochen. Heute sehe ich Werbung für das Produkt. Woher wissen die Big-Tech-Unternehmen vom Gespräch?

Falls Ihre Freundin ein Android-Smartphone besitzt, so hat Facebook die Berechtigung, ihre Anrufe und auch den Versand ihrer SMS mitzuverfolgen – vorausgesetzt, sie hat der Firma eine Freigabe für ihr Adressbuch und ihre Telefoniefunktion gestattet. Indem sie vor Jahren bei der Anmeldung auf Facebook ein Häkchen gesetzt hat beim «Kontakt-Upload» (weil sie vermutlich wissen wollte, welche ihrer Freundinnen und Bekannten sich ebenfalls auf Facebook tummeln).

Zwar protokolliert Facebook damit «nur» ihre Metadaten: Den Inhalt der SMS speichert die Firma also nicht, das Gespräch hört sie nicht mit. Doch auch Metadaten geben allerlei preis: Ihre Identität und die Ihrer Freundin. Von wo Sie anrufen. Wann das Gespräch begonnen hat und wann es endete. Damit also: die Länge des Gesprächs und damit die Intensität der Beziehung. Ach ja, und falls Sie über Whatsapp mit Ihrer Freundin telefonieren, ist die Beziehung zwischen Ihnen für Facebook noch offensichtlicher. Denn der Konzern verknüpft alle Ihre Profilinformationen und Ihre Adressbücher auf Facebook, Instagram und Whatsapp (die Facebook gehören) zu einer einzigen Super-ID in seiner Datenbank, sofern Sie dem nicht aktiv widersprechen und das ständig auftauchende nervige Kästchen wegklicken.

Der Slogan des investigativen Portals «Netzpolitik.org» heisst nicht umsonst: «Wer hat uns verraten? Metadaten».

6. Okay, Metadaten. Aber warum wissen Instagram oder Werbekunden, dass wir über Verhütung gesprochen haben? Das ist Inhalt, nicht Meta

Genau. Und damit kommen wir zur eingangs erwähnten bitteren Wahrheit: Sie sind gar nicht so individuell, wie Sie vielleicht denken. Sorry.

Die Werbeindustrie teilt uns Internetnutzer in Segmente auf. Also konkret: «Menschen, die zu einer bestimmten Zeit derselben Gruppe angehören, sich dieselben Inhalte im Netz ansehen und dieselben Interessen haben», sagt Privacy-Forscher Tapiador. Diese Segmente sind so detailliert, dass wir denken könnten, wir seien mit den entsprechenden Charakteristika einzigartig. Mitnichten. Lassen Sie uns das wieder anhand von Facebook erklären.

Die «New York Times» hat die Granularität dieser Nutzersegmente anschaulich aufgeschlüsselt. Und zeigt, dass Sie auf Facebook als Werbekundin, wenn Sie mögen, etwa folgende Zielgruppe erreichen können:

> Jeden, der in Philadelphia lebt, Philosophie studiert, 21 Jahre alt ist, im letzten Jahr ein blaues T-Shirt gekauft hat, neurotisch ist, weniger als 28'000 Dollar im Jahr verdient, wahrscheinlich in den nächsten sechs Monaten einen Minivan kaufen wird, sich für Camping interessiert und dessen Interessen mit denen von Afroamerikanern übereinstimmen. Ausserdem jeden auf Facebook, der Ihnen ähnlich ist.

Lassen Sie uns diesen Abschnitt im Detail analysieren:

1. Facebook weiss relativ leicht Bescheid über Alter, Wohnort und besuchte Universitäten, den Kauf des Shirts und Interessen wie Camping. Dies dank seiner eigenen Datenquellen, also aufgrund der Informationen, die Sie selber der Plattform mitteilen. Aber auch aufgrund Ihrer Surfaktivitäten und via die Unternehmen, die Kundenlisten auf Facebook hochgeladen haben (Sie erinnern sich an das Schuhgeschäft).
2. Das Attribut «neurotisch» und die Höhe Ihres Einkommens erhält Facebook mit der Hilfe weiterer *data broker* – oder Big-Data-Firmen –, in den USA früher etwa durch die Firma Cambridge Analytica. (Es sei hier aber auch erwähnt, dass Facebook die Integration externer Datenquellen aufgrund des öffentlichen Drucks einstellte und auch die Zugriffsberechtigungen für die App-Entwicklerinnen restriktiver handhabt.)
3. Vielleicht haben Sie den letzten Satz im oben erwähnten Nutzersegment überlesen oder schon vergessen. Es ist der eigentliche Killersatz: «Ausserdem jeden auf Facebook, der Ihnen ähnlich ist.» Diese berühmte Facebook-Funktion «Lookalike Audiences» könnte dafür verantwortlich zeichnen, dass das Verhütungsmittel, von dem Ihre Freundin sprach (und das sie vorher gegoogelt hatte), nun auch Ihnen angezeigt wird. Weil Sie und Ihre Freundin einander vermutlich in vielen Attributen (Alter, Ethnie, Interessen, Lebenssituation) ähnlich sind.

7. Okay, aber warum sehe ich die Werbung ausgerechnet am Tag nach dem Gespräch? Das kann doch kein Zufall sein

Sie haben insofern recht, als der Zufall nicht die einzige Erklärung für das zeitliche Aufeinandertreffen ist. Einfach eine von mehreren:

Vielleicht sehen Sie die Werbung nur zufällig heute.

Vielleicht sehen Sie sie heute, weil Facebook (und damit auch Instagram) weiss, dass Sie gestern mit Ihrer Freundin telefoniert haben, die ja im Netz nach dem Verhütungsmittel gesucht hatte.

Und vielleicht funktioniert auch Ihr Erinnerungsvermögen nicht ganz so einwandfrei, wie Sie denken. Wir Menschen können zwar gut logisch, vernünftig, abwägend denken. Insbesondere dann, wenn wir uns Zeit lassen können. Unsere Kognition hat aber noch eine Strategie: eine, die sehr schnell reagiert – dafür aber weniger präzise.

Eine solche Strategie kommt möglicherweise auch zur Anwendung, wenn Sie (und wir!) eine Werbung sehen und dann denken: «Ha! Darüber haben wir doch gestern erstmals gesprochen, und wir hattens nie gegoogelt. Insta hört offensichtlich mit!»

Psychologen kennen eine kognitive Verzerrung, die sie *survival bias* nennen: Wir Menschen tendieren dazu, uns auf Dinge zu konzentrieren – Menschen, Firmen, Objekte –, die einen Auswahlprozess «überlebt» haben. Die anderen Dinge, die bei dieser Auswahl gescheitert sind, vergessen wir gern.

Im konkreten Fall: Vielleicht haben Sie mit Ihrer Freundin nicht nur über ein spezifisches Verhütungsmittel gesprochen, sondern auch über Schwangerschaftstests, eine Lampe, die Ihnen gefällt, und über eine bestimmte Laufschuhmarke. Vermutlich führen Sie, ohne gross darüber nachzudenken, ständig Gespräche, in denen Produkte vorkommen, die Ihnen nie als Werbeanzeige begegnen: weil diese Produkte den Auswahlprozess – datengetriebene Algorithmen erachten es als sinnvoll, sie *Ihnen* als Werbung zu zeigen – nicht bestanden.

Sie wundern sich aber nicht darüber, dass das Internet Ihnen keine Werbung für Laufschuhe anzeigt. Sie konzentrieren sich auf das Produkt, das den Auswahlprozess überlebte. Ihre Kognition hat Ihnen einen Streich gespielt.

Weiter könnte es sein, dass wir Menschen es als besonders auffällig und besonders störend empfinden, wenn so ein Muster – erst das Gespräch, dann die Werbung – intime Bereiche betrifft. Hätten wir auch einen Zusammenhang vermutet, hätte es sich beim Produkt um Laufschuhe gehandelt? Oder hätten wir die Werbung einfach gedankenlos weggeklickt?

8. Brauche ich vor Belauschung also heute keine Angst zu haben?

Es wäre also wirtschaftlich unsinnig für Facebook, Google und Co., die absolut enorme Menge an Audiodaten samt allen Hintergrundgeräuschen ständig nach bestimmten Schlüsselwörtern (Staubsauger, Verhütung, Schuhe) abzuhören, um sie für Werbezwecke in Echtzeit auszuwerten – wenn sie doch quasi die gleichen Informationen, wie beschrieben, viel billiger erhalten können. «Eine Sprachverarbeitung für Werbezwecke wäre viel zu ressourcenintensiv. Vom technischen Standpunkt aus gesehen ergibt das überhaupt keinen Sinn», sagt Tapiador. Ein ähnlich geringes Risiko sieht auch Sandy Parakilas, ein ehemaliger Facebook-Mitarbeiter, der die Werbeabteilung aufbaute und heute dem sozialen Riesen sehr kritisch gegenübersteht: «Audioaufnahmen wären viel zu datenlastig und aufwendig», sagt er. Die Qualität dieser Daten sei schlecht.

Stand jetzt also: Nein, Big-Tech-Unternehmen hören Sie wohl kaum ab.

9. Und wie ist das in Zukunft …?

Nun kommt das kleine Aber: Es gibt heute noch einige unbekannte Variablen bei diesem Thema und einige Entwicklungen, die auf eine dystopische Zukunft hindeuten.

Facebook hatte in der Tat ein Patent angemeldet für die Aktivierung von Handy-Mikrofonen: und zwar zur Erkennung von Interaktionen mit TV-Werbung, also ob Sie sich zum Beispiel einen TV-Werbespot bis zum Ende ansehen, vorausgesetzt, Ihr Smartphone oder Ihr Notebook liegt in

Nähe. Die künstliche Intelligenz Ihrer Facebook-App würde dann die laufende Reklame für ein Haarshampoo und die Firma erkennen (wieder vorausgesetzt, dieses Patent würde tatsächlich umgesetzt).

Ausserdem: Facebook hatte 2014 eine Funktion namens «Audio Recognition» lanciert, mit der er auf Mikrofone zurückgreifen kann. Sie ist dazu da, die im Hintergrund laufende Musik in Ihrem Wohnzimmer oder die Musik, die aus Ihrem Fernseher schallt, nach Songtitel und Band zu erkennen (vielleicht kennen Sie die Funktion von der App Shazam). Das Magazin «Business Insider» vermutet, dass diese Funktion sogar der Hauptgrund für die «Abhör-Legende» rund um unsere Smartphones ist.

Doch auch hier gilt: Facebook erkennt nur Musik «aus der Konserve», sprich: keine Livemusik, sondern nur ab Band. Diese Funktion soll der Stimmungsauswertung für Statusmeldungen dienen. Dasselbe gilt für die Töne und Laute der abgespulten TV-Reklame aus dem Fernseher. Ob sie aber effektiv Gesprochenes auswerten kann, ist bis dato nicht bekannt. (Sie können die Mikrofonaktivierung bei allen Apps manuell in den Einstellungen Ihres Smartphones deaktivieren).

Dann wären da noch die smarten Assistenten Alexa (Amazon), Siri (Apple), Google Assistant (Google) und Cortana (Microsoft), die auf unsere Sprachbefehle reagieren: Wir wissen, dass Mitarbeiterinnen von Amazon, Microsoft und Apple Ihre Gespräche mittels smarter Lautsprecher belauschen und transkribieren. Angeblich nur zur «Verbesserung des Dienstes». Wie und in welcher Form die Transkripte auch für Werbeprofile mit weiteren Daten angereichert werden, ist aber bis dato nicht bekannt.

Und noch zuletzt: Facebook arbeitet seit langer Zeit daran, seine Investitionen in Augmented Reality (erweiterte Realität) und Virtual Reality endlich in konkrete Produkte umzumünzen. So präsentierte Mark Zuckerberg vor einigen Wochen die erste Facebook-Datenbrille in Zusammenarbeit mit dem Brillenhersteller Ray Ban. In dieser Brille sind allerlei Sensoren verbaut, die unsere ganze Umgebung via Video und Ton aufnehmen. Auf den Brillen-Bildschirmen werden künftig zum Beispiel Zusatzinformationen zum historischen Gebäude eingeblendet, vor dem man gerade steht. Gemäss eigenen Angaben soll das Audiomaterial – also Töne durch Videoaufnahmen – nicht in die entsprechenden Werbeprofile fliessen.

Genau, «gemäss eigenen Angaben», was bei Facebook immer etwas mit Vorsicht zu geniessen ist, wie wir aus der Vergangenheit wissen: Der Konzern hat eine unrühmliche Geschichte von gebrochenen Datenschutzversprechen.

Das soziale Netzwerk ist übrigens mit dieser «Vision» nicht allein: Ziemlich alle Big-Tech-Unternehmen arbeiten am sogenannten Metaverse – an der kompletten Verschmelzung der Realität, also der Offline-Welt, mit dem Internet. Sie nutzen dazu smarte Brillen und andere Innovationen. Die Erkennung und Verarbeitung von menschlichen Stimmen und anderen Livegeräuschen ist damit nur noch eine Frage der Zeit.

10. Wer also hört heute mit, wenn nicht Big Tech?

Zum Beispiel: Ermittlungsbehörden, Fussballligen, vielleicht auch Ihr Partner.

Ein Trost: Die brisantesten Abhörfälle kommen in der Regel ans Licht, wie etwa die App der spanischen Fussballliga. Damit wollten die Funktionäre illegale Übertragungen von Fussballspielen in Bars und Kneipen über-

wachen, um Gastronominnen ohne Lizenz zu erwischen. Die App verschaffte sich dafür Zugriff auf die Mikrofone der Handys von Fussballfans. Die Abhöraktion sorgte für einen kleinen Skandal in Spanien.

Zuletzt ein weiterer, schwacher Trost: Sollte man Sie tatsächlich überwachen, werden sich die Überwacher tunlichst darum bemühen, Sie das nicht wissen zu lassen. Kantonale Polizeibehörden, der Nachrichtendienst und auch die eidgenössische Bundespolizei könnten tatsächlich eingekaufte Spionagesoftware auf Ihr Smartphone lotsen und damit Ihr Mikrofon aktivieren (sofern man Sie einer terroristischen Aktivität verdächtigt). Es wäre nicht schlau, wenn diese Institutionen Ihnen danach Werbung unterjubeln würden. Da es sich um eine Art verdeckte Ermittlung handelt, werden Strafverfolgerinnen penibel darauf achten, dass diejenigen, die sie belauschen, keinen Verdacht schöpfen. Dasselbe gilt auch für sogenannte Stalkerware-Apps, mit denen sich Partner in Beziehungen gegenseitig verfolgen können.

Fazit: Bleiben Sie ruhig wachsam. Und seien Sie öfter mal ohne Ihr Telefon unterwegs, wenn Sie mögen.