

Mittlerweile dürfte es sich bereits bis zum arglosesten Internetnutzer herumgesprochen haben, dass die Dienste der beiden Internetgiganten Google und Facebook im großen Maßstab Nutzerdaten speichern und zu einem Profil zusammenfügen, das von ihnen vor allem zu Werbezwecken genutzt wird. Welche Daten dieses Profil erhält, lässt sich über die gut versteckte Selbstauskunftsfunktion dieser Dienste in Erfahrung bringen. Das Ergebnis lädt dabei zunächst zum Schmunzeln ein. Erst beim zweiten Blick offenbart sich die Gefahr der gesammelten Daten - vor allem dann, wenn Geheimdienste Zugriff auf die Daten haben.
Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/130710_NDS_Google_Facebook.mp3

Podcast: [Play in new window](#) | [Download](#)

Es gibt eine goldene Regel für Internetdienstleistungen, die leider nur wenigen Nutzern wirklich bekannt ist: Kostet ein Dienst nichts, dann bist Du die Ware. Der Umkehrschluss ist hierbei übrigens leider nicht gestattet, auch kommerzielle Dienste handeln oft mit den Daten ihrer Nutzer. Facebook generiert pro Jahr Werbeeinnahmen in Höhe von fast sechs Milliarden US\$, womit statistisch durch jeden Nutzer rund fünf US\$ Werbeeinnahmen generiert werden. Google nimmt rund 50 Mrd. US\$ pro Jahr durch die Vermarktung von Werbeflächen ein.

Das Pfund, mit dem Google und Facebook am hart umkämpften Werbemarkt wuchern können, ist die Möglichkeit, personalisierte Werbung zu vermarkten. Was nutzt es einem Anbieter von Seniorenreisen, wenn seine Werbung Teenagern gezeigt wird und was sollen reifere Surfer mit Werbung für Klingeltöne anfangen? Google und Facebook gehen jedoch noch weiter und versprechen ihren Werbekunden, dass deren Werbung nicht nur zielgruppengerecht, sondern auch interessenspezifisch eingeblendet wird. Wer sich im Netz beispielsweise häufig über Norwegen informiert, ist natürlich genau der richtige Werbekunde für Anzeigen für Direktflüge nach Oslo oder Ferienhäuser am Sognefjord. Wie gut diese interessenspezifische Werbung funktioniert, sieht man auf der Suchmaschine von Google, bei der bezahlte Anzeigen recht präzise zu den verwendeten Suchbegriffen eingeblendet werden.

Wie Google aus ihnen ein Profil macht

Google ist jedoch viel mehr als eine Suchmaschine. Der Konzern ist auch der [weltweit größte Anbieter](#) von Werbeflächen, die auf herkömmlichen Internetseiten angezeigt werden. Hier funktioniert die kontextbasierte Werbung nur unzureichend. Um die Interessen der Nutzer zu identifizieren, nutzt Google dabei sogenannte [Cookies](#), die entweder zu anonymen oder (für eingeloggte Google-Nutzer) zu personalisierten Profilen zusammengesetzt werden. Je nachdem, was sie über Google suchen oder welche Seiten sie im Netz besuchen, bei denen Google das Surfverhalten der Leser auswertet ([Tracking](#)), versucht Google ein Profil über sie und ihre Interessen zusammenzustellen. Wenn Google beispielsweise der Überzeugung ist, dass sie ein Mann in den besten Jahren sind, der einen soliden finanziellen Hintergrund hat und „konsumorientiert“ ist, kann es durchaus sein, dass sie beim Besuch verschiedener Seiten häufiger Werbeanzeigen für Luxusuhren angezeigt bekommen, während sie von Werbung für Damenhygieneprodukte eigentlich verschont sein sollten. Für diese Dienstleistung zahlen die Werbekunden übrigens einen fürstlichen Aufschlag, da der sogenannte Streuverlust eines der größten Probleme im Marketing ist.

Doch hier stellt sich die Frage, ob die Profilbildung von Google und Co. überhaupt funktioniert. Aufgrund der Datenschutzbestimmungen können sie übrigens selbst testen, wie ihr Werbeprofil bei Google aussieht. Über [diesen Link](#) erhalten Sie Zugriff auf den sogenannten Anzeigeeinstellungsmanager von Google, der ihnen - je nachdem, welche Google-Dienste Sie nutzen - zahlreiche Informationen über sie selbst und ihre Interessen ausspuckt.

Ein Selbstversuch

Mein Selbstversuch ergibt dabei folgendes Profil, das sich lt. Google immerhin auf über 30.000 Datensätze stützt:

Geschlecht: Männlich

Alter: 55-64

Interessen (u.a.): Bankwesen, Essen und Trinken, Haarpflege, Hygiene- und Toilettenartikel, Ostasiatische Musik, Rap und Hip-Hop, Spielzeug

Dieses Ergebnis überraschte mich dann doch. Ich bin zwar männlich, aber rund zwanzig Jahre jünger als von Google errechnet. Es ist vollkommen korrekt, dass ich mich (rein beruflich) sehr für das Bankwesen und (rein privat) auch für Essen und Trinken interessiere. Haarpflege und Hygiene- und Toilettenartikel zählen jedoch ganz sicher nicht zu meinen Interessengebieten und ich schließe zudem aus, dass ich je in nennenswertem Umfang

Suchbegriffe oder Artikel dieser Interessengebiete verwendet bzw. gelesen habe[*]. Dass ich mich für ostasiatische Musik, Rap und Hip-Hop und Spielzeug interessieren soll, finde ich auch sehr amüsant - auch diese Punkte sind an den Haaren herbeigezogen und lassen sich mit Sicherheit nicht durch mein Surfverhalten herauslesen. Andere Dinge, die mich persönlich interessieren und über die ich mich auch im Internet gerne informiere, fehlen in der Liste komplett.

Ähnlich sieht es bei Facebook aus. Auch hier beinhalten die personalisierten „Ads Topics“, an die man nur herankommt, wenn man sein komplettes Profil als Zip-Datei herunterlädt[**], einige zutreffende Punkte (z.B. Journalismus, Mindestlohn, Ökonomie und Solidarität) und jede Menge Ungereimtheiten - so soll ich mich beispielsweise für Bergbautechniken (shaft mining), eine bestimmte Schmetterlingsart (*Colias croceus*) und den ausgestorbenen Dodo interessieren, was mir alles komplett neu ist.

Interessanter und aus Datenschutzsicht gefährlicher ist, dass sich bei Facebook offenbar lokale Interessen ins Profil mogeln, die sich einzig und allein aufgrund der vom Smartphone abgefangenen GPS-Daten ergeben. Warum sonst sollte ich mich sonst auch für „Köln“, „Düsseldorf-Hafen“ und „Dänemark“ interessieren? Ich habe anscheinend über mein Smartphone von diesen Orten aus auf die Dienste von Facebook zugegriffen. Das heißt jedoch auch, dass Facebook meine GPS-Koordinaten speichert, was eigentlich ein Unding ist. Dass diese Technik jedoch nicht ausgereift ist, zeigt der Eintrag „Cârța (Sibiu)“ in meinen „Ads Topics“. Ich kann ausschließen, dass ich oder mein Smartphone sich je in diesem 900-Seelen-Dorf in Siebenbürgen befanden und dass die Gemeinde ein großer Anzeigenkunde von Facebook ist, darf wohl auch bezweifelt werden.

Was sagen mir diese Ergebnisse? Vor allem eins: Google und Facebook sind Blender, die Werbekunden personalisierte Anzeigen für teures Geld verkaufen und dabei eine Zielgruppenorientierung vorgaukeln, die gar nicht vorhanden ist. Ich passe beispielsweise exakt ins Profil eines Anbieters für Tinkturen gegen Haarausfall, da ich ja angeblich rund sechzig Jahre alt bin und mich brennend für Haarpflege und Hygieneartikel interessiere. In Wirklichkeit wäre ich jedoch ein lupenreiner Streuverlust für diese Werbung. Ob das der Anbieter von Haartinkturen auch weiß?

Gefahrenpunkt GPS-Daten

Es wäre jedoch naiv, sich nur über die Unvollkommenheit der Profilanalyse von Google und Facebook lustig zu machen. Denn die Daten, die diese Dienste erheben, können dann sehr gefährlich werden, wenn sie von dritter Stelle mit anderen personenbezogenen Daten kombiniert werden. Und dass dies systematisch geschieht, hat Edward Snowden mit seinen

Prism-Enthüllungen ja lückenlos belegt. Es mag noch witzig sein, wenn man grob falsche Werbung angezeigt bekommt. Wenn man bei der Einreise in die USA ins Visier der Geheimdienste gerät (oder einem gar die Einreise verwehrt wird), weil man die Dienste von Facebook öfters auch in Ägypten, Jordanien oder gar Pakistan genutzt hat, ist dies gar nicht mehr witzig. Und wenn die Dienste aus meinen tatsächlich vorhandenen Interessen (Mindestlohn, Ökonomie und Solidarität) nun schließen, ich sei ein potentieller „Links-Terrorist“, ist dies für mich auch alles andere als lustig.

Daher kann man den Nutzern nur raten, die personalisierte Datenspeicherung durch diese Dienste zu verhindern. Dazu hier eine kurze Anleitung:

1. **Google**

Im [Google-Anzeigeeinstellungsmanager](#) klicken sie im untersten Punkt (Deaktivierungsanzeigen bzw. Opt-out settings) auf „Deaktivieren bzw. Opt-out“ und bestätigen diese Auswahl. Dann sollte Google, so behauptet es das Unternehmen zumindest, keine Daten mehr über ihr Surfverhalten erheben und kein Profil mehr über sie erstellen.

2. **Facebook**

Gehen sie über das „Zahnrad“ rechts oben auf „Konteneinstellungen“ und wählen sie auf der linken Seitenleiste den Punkt „Werbeanzeigen“. Nun kommen sie auf eine Seite, auf der sie bei den Punkten „Webseiten Dritter“ und „Werbeanzeigen & Freunde“ jeweils die Option „Niemand“ wählen sollten. Desweiteren sollten sie die Einstellungen unter dem Punkt „Privatsphäre“ nach ihren eigenen Vorstellungen vornehmen.

3. **Cookies blockieren**

Unerwünschte Cookies blockieren sie am besten mit einem dafür vorgesehenen Plugin für ihren Browser. Gute Ergebnisse erzielt beispielsweise das Plugin „[Edit this Cookie](#)“ für Google-Chrome oder der „[Cookies-Manager+](#)“ für Firefox.

4. **Tracker und Scripts blockieren**

Für diese Aufgaben ist ebenfalls ein Plugin für ihren Browser zu empfehlen. Das Plugin „[Ghostery](#)“ ist empfehlenswert und für alle modernen Browser verfügbar.

5. **Datensparsamkeit**

Gehen sie generell mit Daten sparsam um und geben sie so wenig wie möglich von sich preis. Was die Dienste nicht finden, können sie auch nicht wissen.

6. **GPS**

Deaktivieren sie bei Bedarf die GPS-Funktion ihres Smartphones oder verbieten sie bestimmten Programmen den Zugriff auf die GPS-Daten. Beim iPhone können sie einzelnen Programmen (Apps) verbieten auf die GPS-Daten zuzugreifen, wenn sie die

nötigen Einstellungen unter „Einstellungen -> Datenschutz -> Ortungsdienste“ vornehmen.



[<<*] Da meine Lebensgefährtin ihren eigenen Rechner hat, ist es auch auszuschließen, dass ihre Interessen sich hier mit den meinen vermengt haben.

[<<**] Dafür klicken sie rechts oben auf das „Zahnrad“ und wählen den Punkt „Kontoeinstellungen“ aus. Auf der nun erscheinenden Seite sehen sie ganz unten im zarten grau den Punkt „Lade eine Kopie deiner Facebook-Daten herunter“. Nach Bestätigung via Email erhalten sie dann nach einigen Minuten einen Link auf eine Zip-Datei, die ihre gesamten Daten enthält. Wenn sie die Datei entpacken und die entpackte Datei index.html aufrufen sehen sie in der linken Seitenleiste die Rubrik „Ads“, wo sie die gesuchten Informationen finden.