**Auf Umwegen in die Unsichtbarkeit**

*Google und Facebook wissen mehr über ihre Nutzer als so manche ahnen. Wie lässt sich das verhindern? Sechs Methoden, digitale Spuren zu verwischen.*

von Philipp Brandstädter

Das eine begann 1998 als Onlineprojekt, das in einer Garage in Kalifornien Daten aus der ganzen Welt sammeln sollte. Dann entwickelte es sich zum mono­polistischen Internetimperium mit etlichen Unterfunktionen – und erhielt ein eigenes Verb.

Das andere startete als kleines Jahrbuchnetzwerk im Zimmer eines Studentenwohnheims. Acht Jahre später wird es von rund 10 Prozent der Weltbevölkerung genutzt.

Google.

Und Facebook.

Unruhe macht sich hin und wieder breit, wenn sich simple Ideen verselbstständigen und ungewiss bleibt, wer die Ideen steuert und welche Ausmaße sie noch annehmen. Google und Facebook entsagen? Das geht. Computer und Handy ausgestellt und im Keller einen Helm aus Alufolie gebastelt, damit „die da oben“ nicht mehr unsere Daten erfassen können, ganz einfach.

Aber auch Nutzer, die nicht komplett auf digitale Navigation und digitale Gesellschaft verzichten wollen, können sich im Netz besser schützen. Sechs Tipps für den sicheren Umgang mit Google und Facebook:

Infokrake Google

Kein anderes Unternehmen sammelt mehr Informationen über Internetnutzer als Google Inc. Inzwischen personalisiert der Konzern auch die Suchergebnisse, um bessere Treffer zu erzielen. Oder um Nutzer präziser mit Werbung zu versorgen.

1. Werbung filtern

Google nutzt sogenannte Cookies, um dem Rechner Seitenaufrufe zuzuordnen. Diese kleinen Dateien halten fest, auf welchen Websites gesurft und was dort alles angeklickt wurde. Die Funktion liefert Google Informationen über die Interessen seiner Nutzer, mit denen sich wiederum individuell zugeschnittene Anzeigen über den Browser schalten lassen. Ausschalten lässt sich die digitale Werbezustellung zum Beispiel auf Googles Anzeigenmanager oder unter [www.google.com/ads/preferences/html/intl/de/plugin/](http://www.google.com/ads/preferences/html/intl/de/plugin/).

1. Gedächtnis löschen

Welche und wie viele Informationen von einem selbst nun erfasst werden, kann spätestens dann nicht mehr überblickt werden, wenn sich die Datensammler miteinander vernetzen. Verfügt man über ein Google-Konto oder nutzt verwandte Dienste, so werden die Anfragen auch mit dem eigenen Namen und der Postadresse verknüpft. So wird das Surfverhalten personalisiert. Jede einzelne Suchanfrage wird 180 Tage lang gespeichert, wodurch Google die Interessen seiner Nutzer ermittelt und individuelle Anzeigen zuweist. Diese Personalisierung lässt sich unterbinden, indem man ganz einfach sein Webprotokoll entfernt. Dafür braucht es keinen Aluhelm, sondern bloß einen Klick auf [www.google.com/history/?hl=de&ctz=-120](http://www.google.com/history/%3Fhl%3Dde%26amp;ctz%3d-120).

1. Analytics abdrehen

Google Analytics ist das Werkzeug, mit dem die meisten Betreiber beobachten, wer ihre Websites anklickt und wo ihre Besucher herkommen. Google kann diese Daten bündeln und Personen zuordnen. Die Empörung der Datenschützer über Google Analytics ist deshalb groß. Wer sich nicht länger davon beobachten lassen will, kann in seinem Browser die Trackingdienste blockieren, mit denen Google die Besucherdaten übermittelt. Beim Firefox-Browser eignet sich dafür zum Beispiel die Erweiterung „Noscript“. Nach deren Installation erscheint ein kleines Symbol, über das man die Dienste per Mausklick zulassen oder stoppen kann.

Datenkrake Facebook

Facebook ist praktisch, um miteinander in Kontakt zu bleiben und zu erfahren, was die Freunde am Wochenende so treiben. Schwierig wird es, wenn die Freunde gar nicht wollen, dass andere wissen, was sie so treiben.

1. Überblick behalten

Fotomarkierungen, Ortsangaben, Party­resümees: Facebook lebt davon, dass Nutzer nicht nur selbst Informationen preisgeben, sondern auch andere. Wie das zu verhindern ist? So: Die Privatsphäre-Einstellungen von „öffentlich“ auf „Freunde“ umstellen, damit Privates weiterhin privat bleibt. Und: Listen für Freunde, Verwandte und Kollegen unter [www.facebook.com/bookmarks/lists](http://www.facebook.com/bookmarks/lists) anlegen. Die automatische Gesichtserkennung unter „Markierungs­vorschläge“ deaktivieren und nie, nie Facebook-Freunden erlauben, einfach so Fotos zu markieren, auf denen man selbst abgebildet ist.

2. Anzeigen blockieren

Facebook verdient Geld mit Werbung und der Weitergabe von Nutzerdaten. Nutzer, die Unternehmen und Markenprodukte „liken“, landen schnell mit ihrem Namen auf Anzeigen. Das nervt. Gewaltig. Bitte, liebe Leser, verhindern Sie den Zugriff von Facebook-Partnern, indem Sie in den Privatsphäre-Einstellungen das Häkchen bei „umgehende Personalisierung auf Partnerseiten zulassen“ entfernen und so in Ihren Kontoeinstellungen die Werbeanzeigen unsichtbar machen. Eine radikale Lösung bietet auch die Freeware „Adblock“, die sämtliche Werbeanzeigen deaktiviert, die Ihr Browser anzeigen kann.

3. Auf Apps verzichten

Nicht zu vergessen! Versende ein Herz. The Daily Horoscope. My Top Ten Stalkers. Wer braucht diese Sinnlosanwendungen überhaupt? Sie treiben Facebook-Freunde in den Wahnsinn und machen es Spam, Würmern und Viren einfach. Die Auswirkungen reichen vom ungewollten „Like“-Posting rufschädigender Inhalte bis zu Trojanern, die den Computer infizieren. Schutz gefällig? Neben gängigen Virenscannern helfen Plug-ins – also Programmzusätze – wie „WOT“, mit dem Facebook kooperiert und das schadhafte Links kenntlich macht. Vor allem aber: Vorsichtig mit Genehmigungen umgehen, die man Anwendungen erteilt. Um sich und Freunde nicht mit Spam zu überfluten.

Aus: TAZ, http://www.taz.de/!91873/, 20.04.12