

# Unbeobachtet im Internet, gibt's das noch?

„Intelligenz ist die Fähigkeit, sich dem Wandel anzupassen.“

Stephen Hawking

Bei jedem Besuch einer Webseite erzeugen wir Datenspuren. Technische Parameter werden übermittelt wie Größe des Bildschirms, Schriftarten des Systems, unterstützte Dateiformate etc. Ohne diesen Austausch wäre eine Kommunikation zwischen dem Server und Ihrem Rechner nicht möglich. Doch gibt die Gesamtheit der übertragenen Informationen ein so genaues Bild vom Nutzer und der Nutzung, wie man es sich kaum vorstellen mag. Letztlich werden alle Bewegungen im Netz sichtbar und, was noch gravierender ist, gespeichert. Wie weit das Rechercheverhalten Rückschlüsse auf Lebensumstände, Befindlichkeiten und sogar Krankheiten zulässt, zeigt eine Studie: [www.aerztezeitung.de/medizin/krankheiten/krebs/article/915763/google-bing-co-kann-internet-suchmaschine-gefährlichen-krebs-frueherkennen.html](http://www.aerztezeitung.de/medizin/krankheiten/krebs/article/915763/google-bing-co-kann-internet-suchmaschine-gefährlichen-krebs-frueherkennen.html)

Wie können wir dem rasanten Wandel der Technologie, der Gefahr der großen Datensammlungen begegnen, was kann jeder für sich tun, um weniger beobachtbar und transparent zu sein?

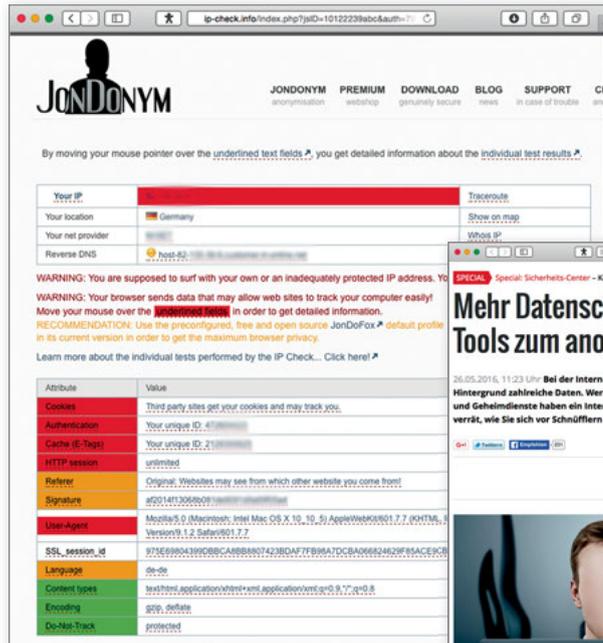
## Unsere Spuren im Internet

Was gebe ich eigentlich alles Preis beim Surfen? Das ist eine gute Frage und die Antwort ist recht umfangreich, umfangreicher, als viele Nutzer sich vorstellen können: [www.netzwelt.de/news/150518-surfen-internet-verraet-browser-ueber-dich.html](http://www.netzwelt.de/news/150518-surfen-internet-verraet-browser-ueber-dich.html)

Die Gesamtheit der Merkmale eines Rechners und Browsers sind meist so individuell, dass damit ein Zurückverfolgen möglich wird, das Browser-Fingerprinting. Wer sehen möchte, wie es dabei mit seinem eigenen Rechner steht, kann diese Tests machen:

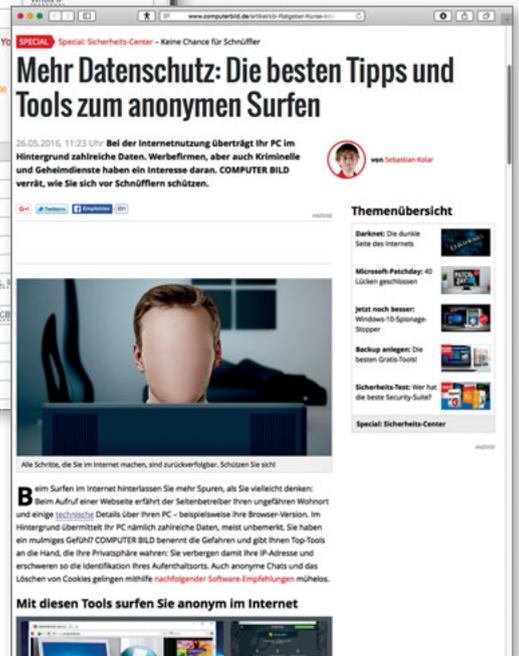
- » <https://panopticklick.eff.org>
- » <https://fingerprint.pet-portal.eu/>

Eine Diplomarbeit zum Thema gibt es ebenfalls schon: <http://bfp.henning-tillmann.de/downloads/Henning%20Tillmann%20-%20Browser%20Fingerprinting.pdf>



Bei einem Test zeigt diese Seite alle offenen Stellen: <http://ip-check.info/?lang=en>

Zur Löschung von Nutzungsprotokollen wurde von „Computer Bild“ ein Programm entwickelt: [www.computerbild.de/download/Ereignisanzeige-loeschen-11225850.html](http://www.computerbild.de/download/Ereignisanzeige-loeschen-11225850.html)



Über die Internetverbindung kann auch der Aufenthaltsort ermittelt werden: [www.utrace.de](http://www.utrace.de)

Im Browsercheck des Heise-Verlages kann man alles über Technologien und deren Schwachstellen erfahren und seine eigenen Einstellungen testen. Dort gibt es auch einen detaillierten Artikel dazu:

- » [www.heise.de/security/dienste/Browsercheck-2107.html](http://www.heise.de/security/dienste/Browsercheck-2107.html)
- » [www.heise.de/ct/ausgabe/2013-20-Vonder-Schwierigkeit-sich-unerkannt-im-Internet-zu-bewegen-2315028.html](http://www.heise.de/ct/ausgabe/2013-20-Vonder-Schwierigkeit-sich-unerkannt-im-Internet-zu-bewegen-2315028.html)

## Gegenmaßnahmen

Browser-Hopping, also das regelmäßige Wechseln von Browsern kann Datenspuren vermindern oder fragmentieren. Eine Liste aktueller

Browser findet sich hier: [www.aktuelle-browser.eu/index.php](http://www.aktuelle-browser.eu/index.php)

Der Google-Browser Chrome ist ein schlechter Verwalter der Privatsphäre, weil Googles Datenhunger weiter wächst. In Zukunft wird sogar die gesamte Suchhistorie ausgewertet. Es ist davon auszugehen, dass Google auch andere Mechanismen in den Browser integriert hat, die der Nachverfolgung dienen: [www.golem.de/news/chrome-browser-google-wertet-gesamte-browserhistorie-fuer-werbung-aus-1607-122171.html?xing\\_share=news](http://www.golem.de/news/chrome-browser-google-wertet-gesamte-browserhistorie-fuer-werbung-aus-1607-122171.html?xing_share=news)

Ein weiterer Schritt um Datenspuren zu vermeiden ist, den privaten Modus des Browsers zu verwenden, wie hier für Firefox: <https://support.mozilla.org/de/kb/privater-modus>

Auch mobil lässt sich privates Surfen aktivieren:

Überblick über Anonymisierungsmöglichkeiten: [www.spiegel.de/netzwelt/tech/anonym-im-netz-welchen-diensten-kann-man-vertrauen-a-440066.html](http://www.spiegel.de/netzwelt/tech/anonym-im-netz-welchen-diensten-kann-man-vertrauen-a-440066.html)



### Tracking the Trackers

von Dr. Marc-Al Hames, Geschäftsführer der Cliqz GmbH

**Wer schaut Ihnen im Web über die Schulter?**

Dass Sie nicht anonym durchs Internet surfen, ist Ihnen wahrscheinlich bewusst. Dass sich kostenlose Internet-Dienste meist über Werbung finanzieren und dafür Daten von Ihnen sammeln, akzeptieren Sie bestimmt auch mehr oder weniger zähneknirschend. So läuft das Internet eben. Aber haben Sie sich einmal Gedanken darüber gemacht, in welchem Ausmaß und völlig unbemerkt Werbepattformen mittlerweile in Ihre Privatsphäre eindringen? In unserer Studie „Tracking the Trackers“ haben wir genau das untersucht. Eins vorweg: Die Ergebnisse sind gelinde gesagt erschreckend.

84 Prozent der von uns getesteten Seiten hatten im Hintergrund mindestens einen Tracker laufen. Das sind kleine Programme, die Ihr Verhalten messen, etwa, welchen Browser Sie benutzen, welche Auflösung Ihr Bildschirm hat oder von welcher Webseite und – wenn möglich – mit welchem Suchbegriff Sie gerade auf die Webseite gekommen sind.

Die starke Verbreitung von Trackern ist erst einmal gar nicht so erstaunlich. Erstens sind darunter viele News-Seiten, deren Geschäft eben aus dem Verkauf von Werbung besteht, zweitens nutzen fast alle kommerziell betriebenen Webseiten einen Analysetracker wie Google Analytics, um zu zählen, wie viele und welche Besucher auf ihre Seite kommen.

#### Tracking – ein Risiko für die Privatsphäre

Website	Reichweite (%)
Google	42%
Facebook	18
AppNexus	10
Criteo	8
ADITION	8
Twitter	6
Adform	6
Cormscore	6
Amazon	5
Meetrics	5

Nur auf 26,4 % der Websites werden keine unsicheren Daten übertragen

Auf 73,6 % der besuchten Websites erhalten Tracker unsichere Daten

Reichweite von Trackern, die unsichere Daten senden

Cliqz hat Tracker untersucht. Viele speichern „unsichere“ Daten, anhand derer einzelne Nutzer identifiziert und durchs Web verfolgt werden könnten.



In welchem Umfang Internetnutzung nachverfolgt wird, ist erstaunlich und erschreckend: <https://cliqz.com/lp/xinglp02>

- » <https://support.apple.com/de-de/HT203036>
- » [www.androidpit.de/anonym-surfen-mit-android-inkognito-modus-privatsphaere](http://www.androidpit.de/anonym-surfen-mit-android-inkognito-modus-privatsphaere)

Zahlreiche Informationen und praktische Tipps zum Schutz von Daten und Privatsphäre gibt [www.selbstdatenschutz.info](http://www.selbstdatenschutz.info)

Werden verschiedene Suchmaschinen im Wechsel benutzt, also zum Beispiel Bing, Yahoo, Google und DuckDuckGo, so kann kein Betreiber alle Ihre Suchanfragen sammeln. DuckDuckGo bietet den zusätzlichen Vorteil, keine Daten des Benutzers an die Suchmaschine weiterzureichen: <https://duckduckgo.com>

Auch gibt es noch Entdeckungen zu machen bei Suchmaschinen jenseits von Google: <http://t3n.de/news/google-alternative-474551/>

Ein Großteil der Identifizierbarkeit geht auf die Verwendung von Cookies zurück, kleine Dateien, die vom Webseitenbetreiber auf den Rechnern ihrer Besucher abgelegt werden. Dagegen hilft beispielweise das Add-on Cookie Monster für Firefox, mit dem Cookies selektiv angenommen oder abgelehnt werden können: <https://addons.mozilla.org/de/firefox/addon/cookie-monster/>

Regelmäßiges Löschen von Cookies sollte zur Gewohnheit werden, um das Trackingpotenzial zu reduzieren: [http://praxistipps.chip.de/cookies-loeschen-in-ie-chrome-und-firefox\\_1277](http://praxistipps.chip.de/cookies-loeschen-in-ie-chrome-und-firefox_1277)

Der Flashplayer hat neben zahlreichen Sicherheitsproblemen auch die Möglichkeit, Daten auf dem Rechner von Besuchern abzulegen (Local Shared Object – LSO). Diese werden auch zur Identifikation verwendet, weil sie nicht mit Cookies angezeigt und gelöscht werden. Die

Einstellungen kann man nur auf dieser Webseite vornehmen: [www.macromedia.com/support/documentation/en/flashplayer/help/settings\\_manager03.html](http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager03.html)

Das Add-on Better Privacy für Firefox kann LSOs löschen: <https://addons.mozilla.org/de/firefox/addon/betterprivacy/>

Unter Windows sammeln sich vielerlei Protokolle und auch der Browserverlauf an, die Rückschlüsse auf viele Details der PC-Nutzung zulassen. Diese lassen sich mit kleinen Programmen löschen: [www.welt.de/wirtschaft/webwelt/article135005837/CCleaner-5-So-optimieren-Sie-ihr-Windows-System.html](http://www.welt.de/wirtschaft/webwelt/article135005837/CCleaner-5-So-optimieren-Sie-ihr-Windows-System.html)

Fast alle Dienste verlangen eine Registrierung, um sie nutzen zu können. Dabei wird natürlich das Verhalten des Nutzers protokolliert. Es gibt jedoch auch Alternativen, die sich ohne Registrierung nutzen lassen und somit Datensuren vermeiden. Dateiversand: [www.filedropper.com](http://www.filedropper.com), Mailversand und anonyme(re)s Surfen: <http://anonymouse.org>

Eine Garantie auf Anonymität im Internet gibt es nicht, obwohl diese durch die Meinungsäußerungsfreiheit gegeben sein sollte. Etwas Aufwand reduziert jedoch die Datensuren bereits beträchtlich und kann das Abbild, das Dienstanbieter von uns haben, unschärfer machen oder fragmentieren. Die Bewusstheit für die Beobachtbarkeit im Internet sollte jeder für sich kultivieren und seine eigenen Schlüsse daraus ziehen.

Wie immer gibt es auch diesen Artikel als PDF mit Links zum Anklicken: <http://www.bayerisches-aerzteblatt.de/aktuelles-heft.html>

## Autor

Dr. Marc M. Batschkus,  
 Arzt, Medizinische Informatik,  
 Spezialist für eHealth, eLearning & Mac OS X  
 E-Mail: [mail@batschkus.de](mailto:mail@batschkus.de)