



HAND AUF'S HERZ...

...Wie häufig liest Du Nutzungsbedingungen und Datenschutzrichtlinien von Webseiten, Social Networks, Apps? Und natürlich nutzt Du Google für Recherchen – und findest es praktisch, dass Google oft die richtigen Vorschläge für deine Suchanfrage kennt, kaum, dass Du die ersten Buchstaben eingegeben hast. Du kaufst bestimmt auch mal bei Amazon ein, hast vielleicht einen Facebook-Account und bist Mitglied in der ein oder anderen WhatsApp-Gruppe, richtig?

Wir alle hinterlassen permanent Spuren - ob wir wollen oder nicht!

Wir alle nutzen täglich das Internet – und hinterlassen dabei permanent Spuren. Ganz direkt, durch die Dinge, die wir freiwillig teilen, durch Likes, öffentlich geteilte Wunschzettel auf Amazon etc. pp. Aber auch indirekt durch jeden Klick, jede Suche... und sogar einfach nur dadurch, dass wir unser Handy immer bei uns tragen: technisch kann jede Bewegung, jede Handlung, die wir in und mit digitalen Medien vollziehen, getrackt, gespeichert und potenziell in irgendeiner Art und Weise weiterverwendet werden. Und häufig genug geschieht das auch...

Man kann sich nun fragen: Ist das schlimm? Bei der riesigen Datenmenge, die rund um den Globus in jeder

Sekunde produziert wird, steigt doch eh keiner so richtig durch. Da gehe ich doch in der Masse unter. Und selbst wenn, ich habe ja nichts zu verbergen! Und das bisschen Werbung, das mir angezeigt wird, das ist doch praktisch. Oder ich ignoriere es einfach.

Stellen wir mit der Aussage »Ich habe doch nichts zu verbergen« nicht diejenigen unter Generalverdacht, die ihre Privatsphäre schützen wollen?!

Allerdings sind es gerade die großen Datenmengen, die es immer einfacher machen, auch aus weitgehend anonymisierten Daten und digitalen Spuren auf die Person dahinter zu schließen. Stetig weiterentwickelte Algorithmen ermöglichen eine immer bessere Mustererkennung. Die Persönlichkeitsprofile, die über uns erstellt werden, werden immer genauer und detaillierter.

Und: stellen wir mit der Aussage »Ich habe doch nichts zu verbergen« nicht all diejenigen unter einen unbestimmten Generalverdacht, denen die eigene Privatsphäre wichtig ist? Darüberhinaus: wenn wir allzu freimütig mit unseren Daten umgehen, kann es sein, dass wir ohne zu fragen auch Informationen über Andere öffentlich machen, z.B. über den Zugriff einer App auf unser Adressbuch.

Und ist es nur das Targeting, d.h. das möglichst individuell zugeschnittene Marketing, um das wir uns Gedanken machen müssen? Oder ist es vielleicht auch möglich, dass versucht wird, uns, z.B. in unserer individuellen politischen Entscheidungs- und Willensbildung gezielt zu beeinflussen? Möglich ist es auf jeden Fall!

Unsere Privatsphäre ist ein schützenswertes Gut - wir sollten für unsere Freiheit kämpfen!

Aber heißt das nun, dass wir uns nicht mehr guten Gewissens im Netz bewegen können? Doch, natürlich – denn das Internet ist ein nicht mehr wegzudenkender und überaus praktischer Bestandteil unseres alltäglichen Lebens. Dennoch: Der technische Fortschritt macht es notwendig, dass wir unsere Privatsphäre aktiv schützen! Zum einen können wir technisch einen Missbrauch unserer Daten so schwierig wie möglich machen. Zum anderen müssen wir dafür kämpfen, dass wir auch auf lange Sicht ein Datenschutzrecht behalten, dass unsere Privatsphäre als schützenswertes Gut ernst nimmt – und uns auch weiterhin einen die Freiheit gibt, das Internet so zu nutzen, wie wir das wollen.

Ein paar Informationen, Tipps und Tricks zum Thema findet Ihr in dieser Broschüre!

LINKS UND INFORMATIONEN

AKTUELLES ZUM THEMA DATENSCHUTZ
<https://netzpolitik.org/category/datenschutz>
 WAS PASSIERT MIT MEINEN DATEN? (BSP. SPOTIFY)
<http://www.fluter.de/was-macht-spotify-mit-meinen-daten>

DATENSCHUTZ EINFACH ERKLÄRT
<https://www.youtube.com/watch?v=V5A2JhJug>
 BEISPIELE FÜR ALTERNATIVE MESSENGER
 » Signal
 » Telegram
 » Threema

SICHERER UND ANONYMER MAILPROVIDER
<https://posteo.de/de>
 ZAHLEICHE ALTERNATIVEN ZU GÄNGIGEN APPS
<https://prism-break.org/de/>

Autoren
 CHRISTINA SCHWALBE
 LUCAS JACOBSEN
 Satz
 ALEXANDR SALIENKO
 CHRISTINA SCHWALBE

Universität Hamburg
 Fakultät für Erziehungswissenschaft
 Medienzentrum für Bildung,
 Kommunikation und Service
 Von-Melle-Park 8
 20146 Hamburg
 mz.ew@uni-hamburg.de
 www.ew.uni-hamburg.de/mz



Dieses Werk ist lizenziert unter
 (Ausnahme: Der Comic auf Seite 5
 steht unter einer CC-BY-NC-Lizenz)

STARKES PASSWORT, ABER WIE?



WIE KANN ICH MEINE DATEN SCHÜTZEN?

Schritt 1: Datensammlung erschweren

Sogar, wenn wir keine unserer Daten bewusst hergeben, lassen wir uns im Netz zu 95%iger Sicherheit identifizieren. Wie man seine Daten verschleiern und somit schwerer zugänglich machen kann, erfahrt Ihr hier:

<http://www.giga.de/extra/ratgeber/specials/browser-finger-print-was-ist-das-wie-verhindern-einfach-erklart/>

<https://amiunique.org/tools>

Schritt 2: Verschlüsselung

Im Gegensatz zur Verschleierung von Daten, wo wir dafür sorgen, dass wir weniger ungewollte Informationen über uns im Netz preisgeben, geht es bei der Verschlüsselung von Daten darum, ausgewählte Daten für andere unzugänglich zu machen.

Hier könnt ihr eure Clouds verschlüsseln:
<https://cryptomator.org/de/>

Schritt 3: Anonymisierung

Bei der Anonymisierung wird versucht, seine Aktivitäten im Netz komplett Anonym zu halten, so dass keiner weiß, welche Person hinter dem Bildschirm sitzt.
<https://www.torproject.org/projects/torbrowser.html>.

