

Greiffenberger Notizen

Neues aus Greiffenberg und Umgebung
Nr. 49



Nichts zu verbergen

Wie Google mit unseren Daten umgeht

von Jörg Berkner

„Ich habe ja nichts zu verbergen!“ - man kann geradezu auf diesen Satz warten, wenn das Gespräch in geselliger Runde auf das Thema Datenklau und Datensicherheit kommt. Diese Reaktion ist verständlich, denn der Mensch verdrängt gern, was er glaubt nicht beeinflussen zu können. Aber sie ist auch ein Ausdruck der Hilflosigkeit gegenüber den großen Datensammelfirmen. Natürlich hat *jeder* etwas zu verbergen, wir nennen das üblicherweise Privatsphäre. Jedem von uns werden schon nach kurzem Nachdenken Erlebnisse und Fakten aus dem eigenen Leben einfallen, die er nicht auf eine Postkarte schreiben würde, geschweige denn im Internet veröffentlicht oder in den Händen von Datensammlern sehen möchte.

Nur, wie soll man sich richtig verhalten, wie sich gegen die übergriffige Datensammelei der großen Internet-Konzerne wehren? Ist das überhaupt noch möglich?

Diese Fragen können wir allerdings nicht in zwei Sätzen beantworten, denn die digitale Kommunikation ist in den letzten drei Jahrzehnten umfassend geworden und die Digitalisierung dringt immer mehr in unsere Lebensbereiche ein. Wir wollen also versuchen, etwas Durchblick in das Knäuel unserer digitalen Abhängigkeiten zu bringen um schließlich die Frage zu beantworten: Was tun?

Wie immer im Leben ist es dafür wichtig, die richtigen Fragen zu stellen. Für den Anfang sollen die folgenden genügen:

- Wie entstehen Daten über uns,
- wer sammelt sie und
- warum werden sie gesammelt?



Internet 4.0 – Fortschritt der Technik¹

Wie entstehen Daten über uns?

Die ersten Informationen über uns als Person entstehen schon am Tag unserer Geburt: Mit jedem Lebensjahr werden es dann mehr - Krankenkassen, Ärzte, Schulen, Versicherungen, Einwohnermelde-, Finanz- und sonstige Ämter, Notare, Gerichte und die Unternehmen, für die wir arbeiten, sammeln und speichern Daten über uns. Das gehört zum Leben in einer Gesellschaft dazu und ist nicht verwerflich, solange sie vertraulich behandelt und nicht gegen uns verwendet werden.

Eine ganz neue Dimension hat das Datensammeln aber mit der enormen Verbreitung des Internets bekommen. Hier werden Daten über uns gesammelt, ohne dass wir uns dessen bewusst werden. Mehr noch, es wird gesammelt und ausgewertet, was wir im Internet und in den sozialen Medien ansehen, sagen, tun und teilen und dabei naiver Weise für völlig unbedeutend halten.

¹ Cartoon: GDD / Gresser & Lenz

Wer sammelt diese Daten?

Die kurze Antwort lautet GAFA – die Abkürzung steht für Google, Apple, Facebook und Amazon und benennt die größten Datensammler, aber längst nicht alle. Google steht hier nicht von ungefähr an erster Stelle. Nach aktuellen Untersuchungen benutzen z.B. 98,1% der Nutzer Google für die Internetsuche. Erst mit großem Abstand folgen andere Suchmaschinen, wie Bing (51%), Yahoo!Search (18,7%), DuckDuckGo (16,3%) und Startpage (14,8%).²

GAFA

GAFA ist eine gängige Abkürzung für die großen Datensammler Google³, Amazon, Facebook und Apple. Spätestens seit Einführung von Windows 10 müsste allerdings noch ein „M“ für Microsoft hinzugefügt werden.

Die amerikanische Harvard-Professorin Shoshana Zuboff hat in ihrem Buch „Das Zeitalter des Überwachungskapitalismus“ den unglaublichen Umfang und die Hintergründe der Google-Datensammelei beschrieben, der wir heute ausgesetzt sind.⁴ Sie verfolgt dabei Googles Entwicklung von einem reinen Suchmaschinenbetreiber zum weltweit größten Überwachungskapitalisten. Das führt zur dritten Frage: Warum wird gesammelt?

Google entdeckt die Klick-Ökonomie

Google ist in seinen Anfangsjahren bekannt geworden durch seine Suchmaschine. Der Begriff „Googeln“ wurde zum Synonym für die Suche im Internet, er steht seit 2004 sogar im Duden. Mit einem speziellen Algorithmus⁵ wurde das Internet ständig durchsucht, um schnell und passend Suchergebnisse anzeigen zu können. In den ersten Jahren von Google wurden die Suchfragen der Nutzer allein zur Verbesserung dieses Suchalgorithmus verwendet. Aber es gab ein großes Problem - als reine Suchmaschine war Google nicht profitabel. Das änderte sich erst, als

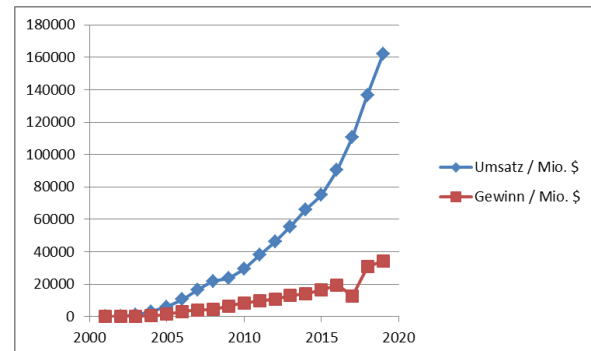
² Andree, Thomsen, Atlas der digitalen Welt [1], S.100, Nettoreichweite, d.h. Anteil der Internetnutzer, die diesen Dienst nutzen, Daten aus Q3/2019.

³ Google gehört zum Konzern Alphabet

⁴ Zuboff, Überwachungskapitalismus [2]

⁵ Page-Rank-Algorithmus

entdeckt wurde, wie wertvoll die Nutzerverhaltensdaten sind. Im Jahr 2000 machte Google noch 15 Mio. \$ Verlust, danach aber stiegen Umsatz und Gewinn exponentiell an.



Umsatz und Gewinn von Google von 2001 bis 2019 in Mio. \$, 2019 wurde beim Umsatz die Grenze von 160 Mrd. \$ überschritten.⁶

Um die Jahrtausendwende machten Google-Wissenschaftler die Entdeckung, dass neben den Suchbegriffen noch viel mehr Eingabedaten der Nutzer anfielen, die sie bis dahin als nutzlos angesehen hatten: Welche Seiten besucht der Nutzer, wie lange verweilt er dort, auf welcher Seite war er vorher, welche Produkte sucht er, was klickt er an, wie groß ist der Abstand zwischen zwei Klicks, kehrt er mehrfach zu einem Produkt zurück usw. Mit speziell dafür entwickelten Programmen wurde es möglich, in diesem Meer von Klick-Daten Verhaltensmuster zu erkennen, die wertvolle Voraussagen zum Nutzer-Verhalten zulassen. Die sogenannte Klick-Ökonomie war geboren.⁷

Dieses Wissen über das Nutzerverhalten, welches Google aus unseren Daten gewinnt, ist goldwert und wird an Internet-Händler verkauft, und zwar in Echtzeit. Google entwickelte dafür basierend auf unseren Verhaltens-Daten Softwareprodukte wie AdWords und AdSense, mit denen Händler auf den Nutzer zugeschnittene Werbung platzieren können. Die Platzierung der für jeden Nutzer individuell ausgewählten Werbung funktioniert mit dieser Software über automatisierte Auktionen von Werbeplätzen in Echtzeit, also in Abhängigkeit davon, was der Nutzer gerade auf der besuchten Web-Seite sieht und macht. In Millisekunden wird entschieden, wer den Werbeplatz bekommt und welche Werbung der Nutzer zu sehen bekommt. Dafür müssen die Händler natürlich bezahlen.

⁶ https://de.wikipedia.org/wiki/Google_LLC #Umsatz_und_Gewinn und Alphabet Annual Report 2019, p. 26 - 30



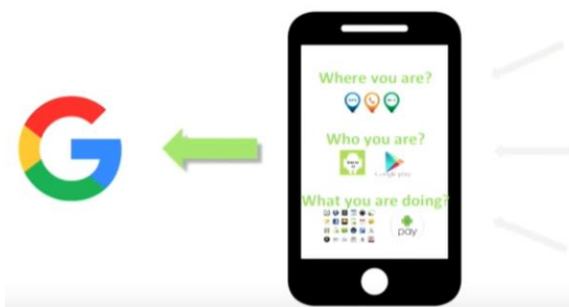
Ihr Kontostand erlaubt keinen Espresso mehr!

Die beschriebenen Prozesse der Datengewinnung, -verdichtung und -verwertung erwiesen sich für Google als extrem profitabel. Um das Wachstum von Umsatz und Gewinn auch weiterhin zu sichern, werden immer mehr neue Nutzer-Verhaltensdaten gebraucht. Deshalb ist Google ständig auf der Suche nach neuen Datenquellen und entwickelt gezielt Produkte, die als Generator für Nutzerdaten dienen können. Beispiele sind Google-Nest, Google Glas und – das wird manch einen überraschen – das weit verbreitete Smartphone-Betriebssystem Android.

Unser Smartphone - die ideale Datenquelle

Ein Problem für die Datensammler besteht in der Zuordnung der Nutzerdaten zu einer konkreten Person, denn oft benutzt der moderne Mensch verschiedene Geräte, um im Internet unterwegs zu sein, und dies auch noch zu verschiedenen Zeiten an verschiedenen Orten. Für die großen Datensammler ist darum das internetfähige Mobiltelefon die beste Datenquelle überhaupt.

Android is a data collection device



Das Smartphone - die ideale Datenquelle⁸

Es liefert eine Vielfalt von Informationen über seinen Besitzer: besuchte Internetseiten, das Surfverhalten auf diesen, Einkäufe, Online-Zahlungen, Kontakte, E-Mails, Bewegungs- und Standortinformationen. Das Smartphone löst also

⁷ Zuboff [2], S. 99

für die Datensammler ein schwieriges Problem: die Zusammenführung der Datenspuren von verschiedenen Aktivitäten eines Nutzers zu einem Profil. Man muss nur dafür sorgen, dass der Nutzer die Datenerfassung zulässt. Das geht am besten, wenn er sie gar nicht erst bemerkt.

Bei Google wurden die Vorteile des Smartphones als Datenquelle schnell erkannt. Schon 2008 begann man deshalb mit der Entwicklung des Smartphone-Betriebssystems *Android*, welches kostenlos an Gerätehersteller lizenziert wurde. Die vorrangige Strategie dahinter war nicht etwa die Absicht, auf dem Smartphone-Markt Gewinne zu realisieren, das war nur ein willkommener Nebeneffekt.⁹ Die strategische Überlegung war, mit diesem Betriebssystem den Zugriff auf die denkbar beste Quelle für Verhaltensdaten von Nutzern zu bekommen.¹⁰



Ein Thermostat von Googles Smart Home-System Nest.¹¹

Eine besondere Rolle spielen dabei die endlosen und unverständlichen Nutzungsbestimmungen der Anbieter von Internetdiensten, von Soft- und Hardware, die mit Absicht zig Seiten lang und mit Verweisen auf kooperierende Firmen und deren ebenso lange Nutzungsbestimmungen versehen sind. Ein Beispiel: Zwei Forscher der Universität London haben die Nutzungsbedingungen von Googles Nest-Thermostat-System untersucht, und festgestellt, dass man zu ihrer vollständigen Prüfung fast 1000 Dokumente lesen und verstehen müsste!¹² Diese unglaubliche Zahl kommt zu Stande, weil in jedem Dokument auf weitere Firmen verwiesen wird, die ebenfalls Nest-Daten verwerten und ihrerseits umfangreiche Bedin-

⁸ Bild: Vortrag von Peter Lord, Oracle, CCA 2018 [6]

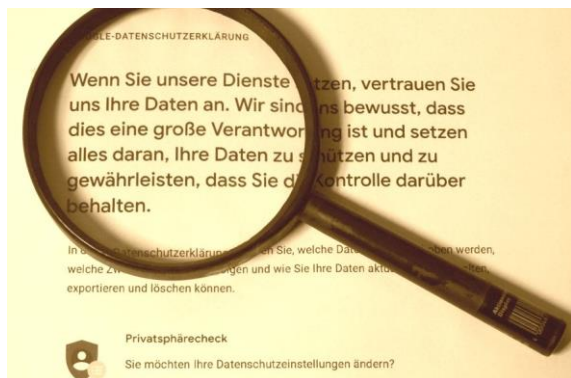
⁹ Die Umsätze mit dem Google Pixel Phone werden im Jahresbericht gar nicht erst gesondert ausgewiesen und mit Google Nest, Pixelbooks und anderen Produkten zusammen unter „others“ geführt. Vgl. dazu Alphabet Annual Report 2019, p. 26

¹⁰ Zuboff [2], S. 160

¹¹ Bild: Wikipedia, public domain

¹² Zuboff [2], S. 21

gungen formuliert haben. So macht man es dem Nutzer unmöglich Verträge zu prüfen und hofft, daß er resigniert und den Bedingungen zustimmt. Auf diese Weise führt Google die jahrhundertalte Rechtsinstitution des Vertrages ad absurdum und verschleiert, wozu der Nutzer eigentlich zustimmt.



Die Google Datenschutzerklärung umfasst als pdf-Datei 33 Seiten und enthält zahlreiche Verweise auf weitere Dokumente (Stand Febr. 2021)

Aber, werden jetzt Google-Anhänger einwenden, jeder kann doch in seinem Google-Konto die Datenschutzeinstellungen suchen und ändern. Damit ist aber schon akzeptiert, dass die Einstellungen als Standard immer zunächst die Daten-Weitergabe erlauben. Das ist entscheidend: Der Nutzer muss erst aktiv werden, um das zu ändern. Richtig wäre es aber umgekehrt – die Standardeinstellung muss auf „Nein“ stehen.

Haus ohne Türen

Veranschaulichen wir uns das an einem (zugespitzten) Beispiel: Eine Baufirma hat für uns ein Eigenheim errichtet, aber wir stellen beim Einzug überrascht fest, dass das Haus weit offen steht, weil alle Türen fehlen. Die Firma erklärt nun, das wäre ein Vorteil: Es sei doch jetzt viel einfacher das Haus zu betreten und zu verlassen, denn das lästige Aufschließen der Türen entfällt. Außerdem stünden ja Türen im Keller und man habe die Möglichkeit, sie selbst einbauen.

Absurd? Natürlich, aber das ist genau die Herangehensweise der Datensammler. Die Nutzerdaten werden erst einmal abgegriffen und verwendet, wer etwas dagegen hat, muss selbst etwas dagegen tun. Es ist die Denkweise der Pioniere des Wilden Westens, übertragen in die neue digitale Welt: Wir nehmen uns, was wir brauchen. Wer das nicht will, kann sich ja wehren. So hatte Google auch kein Problem damit, seit 2004 bei jedem Nutzer seines Gmail-Dienstes den Inhalt

des Posteingangs zu scannen, um dann passende Werbung einzublenden, bis diese Praxis 2017 wegen anhaltender Proteste abgeändert wurde.



Haus ohne Türen: Sinnbild für den unbeschränkter Zugang zu den Daten der Bewohner.¹³

Google kehrt ein fundamentales Prinzip im Zusammenleben unserer Gesellschaft um – die Respektierung der Privatheit und der Persönlichkeit. Wer mein Haus betreten will, muss *vorher* um Erlaubnis bitten. Wer ein Foto von mir machen möchte, muss mich *vorher* fragen. Auch wer meine Daten, meine digitale Identität, auswerten will, muss *vorher* meine Einwilligung einholen.

Weil der Gegenwind beim Datensammeln aber langsam zunimmt, hat Google 2015 reagiert und die Seite „Mein Konto“ eingeführt. Hier kann man Einstellungen zur Nutzung der eigenen Daten verändern. Das oben genannte Prinzip bleibt aber unangetastet. Außerdem stellt sich sofort die Frage, wie viele Nutzer diese Möglichkeit tatsächlich anwenden? Einen Hinweis gibt ein Umfrageergebnis von 2017: Nur 25% der befragten Internetnutzer gaben an, sich aktiv um ihren Datenschutz zu kümmern.¹⁴ Dazu kommt: Auch von jedem, der *kein* Google-Konto hat, werden Daten gesammelt, denn ca. 2 Mio. Apps und Web-Seiten verwenden Programme wie Google Analytics und Google AdSense.¹⁵ Auf 78% aller Internet-Seiten kommen Google-Tracker zum Einsatz, auf 34% solche von Facebook.¹⁶

Wie anonym sind meine Daten?

Nun kann man einwenden: Wen stört die statistische Auswertung der anonymen Klickdaten von mir und Millionen anderen? Da geht es doch gar nicht mehr um die einzelne Person! Sind also anonymisierte Daten unbedenklich? Das ist lei-

¹³ Bild: Wikipedia, public domain

¹⁴ Statista-Umfrage 2017 [4]

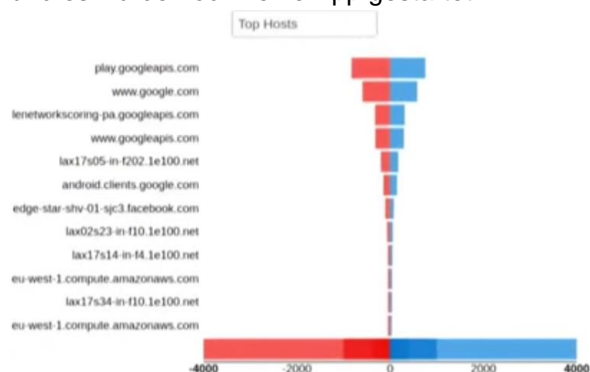
¹⁵ Klein, Vertrackt [5]

der ein Irrtum, denn schon mehrfach wurde nachgewiesen, dass anonymisierte Daten mit wenig Aufwand zu einem Profil verdichtet und leicht einer Person zugeordnet werden können. Besonders wichtig dafür sind die Standortdaten, die entweder durch GPS oder, falls ausgeschaltet, auch durch Triangulation zwischen den Funkzellen ermittelt werden. Android-Handys senden solche passiven Daten ohne unser Zutun an Google.¹⁷ Da jeder Nutzer täglich sein Haus oder seine Wohnung aufsucht, lassen sich mit weiteren, oft frei verfügbaren Informationen schnell seine Adresse und auch seine Name feststellen.

Darüber hinaus vergibt Google für jedes Android-Gerät eine Werbe-ID, also eine eindeutige Kennung, die man nicht abschalten kann. Damit ist es sehr einfach, Nutzer und Profildaten zu verbinden.¹⁸

Ein aufschlussreiches Experiment

2018 führte John Lord, Vice President der Firma Oracle, bei der CCA-Konferenz¹⁹ live ein interessantes Experiment vor. Ein neues, noch nie benutztes Smart Phone wurde eingeschaltet und dann wurden über einen WiFi-Hotspot alle gesendeten und empfangenen Daten aufgezeichnet und analysiert. Das Telefon hatte noch keine SIM-Karte, es war noch kein Nutzer angemeldet und es wurde noch keine App gestartet.



Grafik der Server (Top Hosts), an die das Smartphone während des Experiments Daten sendete. Ganz oben: play.googleapis.com²⁰

Trotzdem sendete es ständig Daten: an Google: über den (analysierten) Bewegungszustand (on

foot, walking, on Bicycle), über die Höheninformation und über alle erreichbaren WiFi-Stationen in der Nähe (Frequenz und Signalstärke).

Allein diese Informationen reichen aus, um Schlussfolgerungen auf den Standort zu ziehen. All dies wird nur vom Android-Betriebssystem veranlasst. Interessanterweise wurden auch Verbindungen zu Facebook-Servern hergestellt. An dieser Stelle erinnern wir uns noch einmal an den berühmten Satz von Googles langjährigem CEO Eric Schmidt: „Wir wissen wo Du bist. Wir wissen wo Du warst. Wir können mehr oder weniger wissen, was Du denkst.“²¹

Vertrauen in Google?

In den letzten Jahren kann man eine steigende kritische Haltung gegenüber den großen Datensammlern erkennen. Auf die Frage, wie stark die Nutzer Firmen wie Google, Facebook oder Amazon vertrauen, antworteten erstaunliche 38,6 % mit „wenig“ und 41,2 % mit „gar nicht“, zusammen rund 80%.



Fast ebenso viele sprechen sich für die Nutzung anderer Anbieter aus: „Ja, auf jeden Fall“ sagen

¹⁶ Zuboff, Überwachungskapitalismus [2], S.163

¹⁷ ZDF WISO: Alexander Pessler Data check: Passive Handy-Daten, Download 3.2.2020

¹⁸ Vertrackt, c't Daten schützen 2020 [5]

¹⁹ Competitive Carriers Association Mobile Carriers Show, 2018 [6]

²⁰ Presentation of Peter Lord at CCA Mobile Carriers Show, 2018 [6]

²¹ Interview mit James Bennet (The Atlantic) beim "Second Annual Washington Ideas Forum" am 1. Oktober 2010, s.a. [3], S.137

52,3%, „Eher ja“ meinen 27,0%. Aber an der Konsequenz mangelt es noch sehr: 27 % geben an, aus Bequemlichkeit nicht nach Alternativen zu suchen und 13% kennen gar keine.²²



Umfrageergebnisse zum Vertrauen in die großen Digitalfirmen, Civey, 2018²³

Nachdenken bei Google

Anfang 2020 veröffentlichte Google in Deutschland in verschiedenen Magazinen eine 36seitige Beilage unter dem viel versprechenden Titel „Digitales Ich. Privates schützen, Chancen nutzen“. Neben der ausführlichen Darstellung von Vorteilen der Digitalisierung gibt es darin auch Beiträge zur Datensicherheit. In einem Interview mit einem Google-Mitarbeiter²⁴ findet sich darin auch eine gewagte Behauptung: „Google würde niemals Daten seiner Nutzer verkaufen. Wir erfassen Daten, damit wir unsere Produkte individuell auf den Nutzer anpassen können, und wir erfassen nur Daten, für die wir auch einen Verwendungszweck haben.“ Wie aber passt diese Aussage mit dem Smartphone-Experiment von Peter Lord zusammen? Mit viel gutem Willen könnte man darin eine Halbwahrheit sehen, tatsächlich aber handelt es sich um eine bewusste Irreführung der Leser. Denn Google verkauft zwar nicht die einfachen Rohdaten seiner Nutzer, aber diese werden aggregiert, kombiniert, ausgewertet und dann in den oben beschriebenen Programmen wie Adwords usw. verwertet, denn nur das bringt den richtig großen Gewinn.

Inzwischen gibt es auch bei Google Kritik an der Firmenphilosophie, gerade haben Angestellte die

²² Civey-Umfrage, 2018 [7]

²³ Civey-Umfrage, 2018 [7]

²⁴ Christoph Sperl, Mitarbeiter im Google Safety Engineering Center München [8], <https://safety.google/engineering-center/>

Gewerkschaft Alphabet Workers Union (AWU) gegründet. Sie streiten allerdings nicht vorrangig für bessere Gehälter, sondern für bessere Werte. Das frühere Firmen-Motto „Don't be evil“ (Sei nicht böse) soll wieder zur Geltung kommen.

Die schleichende Veränderung

Wir hören und lesen immer wieder von Daten-skandalen und von unserer Ausspähung im Netz. Und doch ziehen wir meist keine Konsequenzen daraus. Der Soziologe Harald Welzer erklärt das mit dem sozialpsychologischen Phänomen der „Shifting Baseline“.²⁵ Gemeint ist eine langsame Verschiebung unserer Bewertungsmaßstäbe für das was gut oder schlecht ist, die wir gar nicht mehr wahrnehmen. Reaktionen wie „Da kann man ja doch nichts machen“ und das eingangs erwähnte „Ich habe ja nichts zu verbergen“ sind Ausdruck dieser Verschiebung. Viele sehen sich mit den komplizierten Begriffen der IT-Technologie überfordert und scheuen den Aufwand, in ihrem Web-Browser oder ihrem Smartphone die Datenschutzeinstellungen zu suchen, zu verstehen und zu verändern. Das wird natürlich von den Anbietern ausgenutzt. Oft sind die Einstellmöglichkeiten über verschiedene Seiten und Menüs verstreut und dazu missverständlich bezeichnet. Dafür gibt es sogar einen Begriff: „Deceived by design“ (Getäuscht durch Design). Mit Farbwahl, Anordnung, schlechter Sichtbarkeit und unklarer Bedeutung von Design-Elementen wird unsere Entscheidung beeinflusst.²⁶

Und noch ein anderer Punkt fördert unsere Inaktivität beim Schutz unsere Daten: Die Datensammelei tut nicht weh. Anders als bei einem Schadvirus, der den Rechner oder das Smartphone blockiert, bis Geld gezahlt wird, merken wir vom Datensammeln nichts. Erst wenn die Daten missbraucht werden, wenn z. B. mit einer gestohlenen Identität Waren gekauft und Geld abgehoben wird, wird es richtig unangenehm. Dann ist das Kind aber schon in den Brunnen gefallen. Muss es also erst wehtun, ehe wir uns um unsere Daten kümmern?

Was tun?

Auch wenn Google es gern so hätte – man muss ja nicht alles mit Google-Programmen erledigen. Durch die Nutzung von Alternativen kann die Menge der abgegriffenen Daten stark verringert werden. Für die Internet-Suche eignen sich z.B.

²⁵ Welzer, Die smarte Diktatur [9], S. 29

²⁶ Studie Deceived by Design [10]

die Suchmaschinen startpage.com, duckduckgo.com oder metager.org sehr gut.

Startpage.com

Auch für Google Maps gibt es Alternativen, z.B. den ADAC Routenplaner (maps.adac.de) oder OpenStreetMap (openstreetmap.de). Schließlich kann ich aus eigener Erfahrung als E-Mail-Programm Mozilla Thunderbird und als Internet-Programm Mozilla Firefox mit gutem Gewissen empfehlen (thunderbird.net/de/) bzw. (mozilla.org/de/firefox).



Wer jedoch glaubt, auf Google nicht verzichten zu können, der muss sich wohl oder übel mit den Datenschutzeinstellungen befassen. Die Zeitschrift c't hat im Jahr 2020 in einem Sonderheft praktische Checklisten für einen besseren Datenschutz veröffentlicht, mit deren Hilfe man schnell die richtigen Einstellungen für die verschiedensten Anwendungsbereiche findet. Eine Kurzform der Checklisten kann man unter: <https://ftp.heise.de/ct/listings/2020/20/checkliste2021.pdf> herunterladen. Diese Checklisten gibt es nicht nur für Google, sondern auch für die Themen Windows10, Homeoffice, Android, iOS, Chat, Browser, Facebook, E-Mail, Cloud-Speicher, Gesundheit und Fitness sowie Smart Home.²⁷ Speziell für Google sind unter www.ct.de/wpw5 Hinweise zu finden, wo die richtigen Einstellungen gemacht werden können. Dort gibt es auch noch weitere Vorschläge für Alternativen.

Also, einfach mal ausprobieren!



DuckDuckGo forderte 2011 in San Francisco Google mit dieser Werbung heraus: Google verfolgt Dich – wir nicht.²⁸

²⁷ c't Daten schützen 2020 [11]

²⁸ wired.com [12]

Quellen

- [1] Andree, Martin, Thomsen, Timo: "Atlas der digitalen Welt", Campus, 2020
- [2] Zuboff, Shoshana: „Das Zeitalter des Überwachungskapitalismus“, Campus, 2018
- [3] Bode, Thilo: „Die Diktatur der Konzerne“, S. Fischer Verlag, 2018
- [4] statista.com – Umfrage zum Datenschutz in Deutschland 2017, <https://de.statista.com/statistik/daten/studie/712716/umfrage/umfrage-zum-datenschutz-in-deutschland/>
- [5] Klein, Torsten: „Vertrackt. Wie Google das Leben von Milliarden Menschen erfasst.“, in: c't Sonderheft Daten schützen, 2020, S.6-11
- [6] Presentation of Peter Lord at CCA Mobile Carriers Show, 2018 www.youtube.com/watch?v=VkgMGXKLeK0
- [7] Civey-Umfrage für „Next Conference“ 2018, „Google, Amazon, Facebook: Die Mehrheit der Deutschen misstraut den Digitalkonzernen“, <https://t3n.de/news/google-amazon-facebook-die-mehrheit-der-deutschen-misstraut-den-digitalkonzernen-1110623/> Download 2020-01-30
- [8] Google LLC: „Aufbruch. Digitales Ich“, Anzeigensonderveröffentlichung, Febr. 2020, SZ Scala GmbH
- [9] Welzer, Harald: "Die smarte Diktatur. Der Angriff auf unsere Freiheit.", Fischer Verlag, 2016
- [10] „Deceived by Design, How tech companies use dark patterns to discourage us from exercising our right to privacy“, Studie des Norwegischen Verbraucherrates, 27.6.2018
- [11] c't: "Daten schützen 2020", Sonderheft, Heise Medien GmbH, 21.07.2020
- [12] Singel Ryan: „DuckDuckGo Challenges Google on Privacy“, <https://www.wired.com/2011/01/duckduckgo-google-privacy/>

Impressum

Die Greiffenberger Notizen sind eine private Veröffentlichung auf www.joerg-berkner.de

Alle bisherigen Ausgaben finden Sie auf: www.joerg-berkner.de/GN/Greiffenberger_Notizen.html

Cartoons: Gesellschaft für Datenschutz und Datensicherheit / Gresser & Lenz, mit freundlicher Genehmigung, www.gdd.de/downloads/materialien/cartoons

Logos: Startpage Wiki, gemeinfrei, Thunderbird und Firefox: Mozilla Corporation, CC BY 3.0 bzw. MPL2

Fotos: Jörg Berkner, soweit nicht anders angegeben

Version 2021-02-04