Anonymisieren

Michael Georg Schmidt
Ein Beitrag der studentischen Gruppe ***ITS Us.***
der ***TH Lübeck***

29. August 2023

Zusammenfassung

Dieser Vortrag beschäftigt sich mit der Notwendigkeit von Anonymisierung. Weshalb Anonymisierung für jede/n persönlich und für unsere ganze Gesellschaft unerläßlich wichtig ist.
Alle Einträge im Inhaltsverzeichnis und in den Quellen sind verlinkt. Blaue Texte weisen auf externe Links hin, rote Texte sind innerhalb des Artikels verlinkt.

Inhaltsverzeichnis

1 Anonymisieren - wozu?

Stellen Sie sich vor, Sie informieren sich im Internet über eine Geschlechtsumwandlung. Kurz danach bekommen Sie E-Mails und Post zu diesem Thema – unaufgefordert. Es sprechen Sie Leute auf Ihre Recherche an.
Wie fühlt sich das an?
Nicht gut? Verständlich! Daher ist es gut, wenn man seine Daten anonymisiert.

2 Wie konnte es dazu kommen?

Wenn Sie digital unterwegs sind, hinterlassen Sie Spuren – immer. Unternehmen wie Alphabet und Meta, die Muttergesellschaften von Google, Facebook, Instagram, WhatsApp und Co. sind an Ihren Datenspuren interessiert. Sie sammeln Ihre Daten um hieraus Profile zu erstellen, die sie verkaufen. Die genannten Player sind nicht die Einzigen die das machen. Es gibt tausende kleinere und noch viel größere Unternehmen, die mit Daten handeln. Das größte Unternehmen dürfte wohl ***Acxiom*** sein.

2.1 Ich habe nirgends meinen Namen angegeben

Um erkannt zu werden, müssen Sie nirgends Ihren Namen angeben. Ihr Browser, Ihr Messenger, Ihr E-Mailclient übertragen von sich aus große Mengen an so genannten Metadaten. Das sind Informationen wie

- Welches Betriebssystem kommt zum Einsatz?
- Welche Auflösung hat der Monitor / das Display vor dem die Person sitzt?
- Welche weiteren Programme sind installiert?
- Welche Schriften sind installiert?
- Welche Cookies sind gespeichert?
- Wo befindet sich die Person um die es geht?
- **... und sehr viel mehr Daten.**

„Metadaten sind strukturierte Daten, die Inhaltsdaten beigeordnet sind und etwas über diese aussagen.“ (Prof. Dr. Dorina Gumm, TH Lübeck)

Wie wichtig Metadaten sind, erkennen Sie an der Aussage des ehemaligen Direktors der CIA, später auch Direktor der NSA, ***Michael Vincent Hayden***:
„We kill people based on metadata“.
Diese Aussage hat er im Rahmen einer Podiumsdiskussion an der Johns Hopkins University im Jahr 2014 getroffen.
Wie viele Daten Ihr Browser überträgt, können Sie selber ausprobieren, indem Sie die Site ***browserleaks.com*** aufrufen.
Mit diesen Metadaten sind Sie identifizierbar. Bereits vier davon reichen aus, um eine vermeintlich anonyme Abfrage, einer natürlichen Person zuzuordnen. Das haben ***Yves-Alexandre de Montjoye et al.*** wissenschaftlich nachgewiesen.

3 Was kann ich dagegen tun?

Sie können einiges dagegen tun, dass Sie erkannt werden.

3.1 Anonymisieren

„Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“ (Wikipedia).

3.2 Warum sollte ich meine Daten anonymisieren?

Ihre Daten sollten Sie anonymisieren

- Damit Sie unbeobachtet leben können. Oder finden Sie es gut, wenn irgendwelche Unbekannten genau wissen, was Sie tun, was Sie denken, wen Sie treffen?
  Beispiel:
  Jeffrey D. Burrill war Sekretär der amerikanischen Bischofskonferenz. Er hat – anonym – die App ***grindr*** genutzt. Darüber hat er sich mit homosexuellen Männern verabredet. Grundsätzlich kein Problem. Für einen katholischen Bischof schon. Denn Journalisten der katholischen Wochenzeitung ***The Pillar*** haben von einem Datenhändler anonyme Daten gekauft, die sie deanonymisiert haben. Dabei kam das heraus. Burrill musste zurücktreten.

- Damit Sie keine Verträge angeboten bekommen, die genau an Ihren Lebensumständen orientiert sind, sondern genauso gut sind, wie die für andere auch.
  Beispiel:
  Sie sind sehr sportlich und wollen sich das erste Mal selbst krankenversichern. Statt des günstigen Vertrages den Sie erwarten, bekommen Sie einen ziemlich teuren Tarif angeboten. Das liegt daran, dass Ihr Lieblingssport Kickboxen ist. Damit ist Ihr Verletzungsrisiko hoch. Sie sind also potentiell teuer für die Krankenversicherung.
- Damit Sie eine Stelle auf die Sie sich mit erstklassigen Zeugnissen bewerben auch bekommen.
  Beispiel:
  Die Stelle bekommen Sie nicht – weil Sie Kickboxen machen. Damit ist das Risiko, dass Sie verletzungsbedingt ausfallen zu hoch für den potentiellen Arbeitgeber.
- Damit unsere Demokratie geschützt wird. Damit wir
- die Möglichkeit haben, unsere Meinung zu äußern, ohne dabei beobachtet zu werden,
- uns über Dinge informieren können, ohne dabei beobachtet zu werden oder uns dafür rechtfertigen zu müssen,
- Menschen treffen können, die nicht zur Mitte der Gesellschaft gehören, ohne deswegen gezwungen zu sein, uns zu rechtfertigen,
- unser Leben so führen können, wie wir es mögen,
- reisen können, wohin wir wollen, ohne kritisch beobachtet zu werden
- wohnen können, wie wir es möchten,
- Damit wir Dritten die Möglichkeit nehmen, gezielt und einfach auf uns Einfluss zu nehmen.
- ... und noch vieles mehr, was einer funktionierenden freiheitlichen Demokratie bedarf.
  Beispiel:
  Am 06. Januar 2021 stürmten Vandalen das Kapitol in Washington. Ein unglaublicher Angriff auf die amerikanische Demokratie. Möglich war dieser Angriff nur, weil vorher große Gruppen von Menschen gezielt beeinflusst wurden. Amerikaner sind bekannt dafür, dass sie nicht besonders sorgsam mit ihren persönlichen Daten umgehen. Das hat es ermöglicht, dass Menschen zu großen Gruppen mit ähnlichen Interessen zusammengefasst

wurden. Diese Gruppen wurden über soziale Medien, Fernsehbeiträge und Ähnliches, so beeinflusst, dass es ihnen gar nicht bewusst war, beeinflusst zu werden.
Inzwischen ist bekannt, dass ***Jewgeni Wiktorowitsch Prigoschin***, auch bekannt als der Unternehmer, der hinter der Söldnertruppe Wagner des Ukraine-Kieges stand, die Menschen in den USA beeinflusst hat. Das hat er mit Hilfe einer so genannten Trollfabrik in St. Petersburg gemacht. Das ist eine Firma, die Leute dafür beschäftigt hat, Fake-Accounts in sozialen Medien einzurichten und hierüber Unwahrheiten und gezielte Einflussnahme zu verbreiten. Das kann nur wirken, wenn ausreichend viele Informationen über einzelne Menschen vorliegen. In Deutschland ist dies in diesem Ausmaß noch eher unwahrscheinlich, weil hier das Bewusstsein für Datenschutz deutlich besser als in den USA ist.

4 Wo ist Anonymisierung relevant?

Grundsätzlich ist Anonymisierung überall da relevant, wo wir digital agieren. Das können verschiedene Bereiche sein, wie

- Umfragen
- Social Media
- Telefonieren
- Surfen im Internet

5 Wie gehe ich mit Anonymisierung um?

Es kommt darauf an, in welchem Bereich Sie sich bewegen. Grundsätzlich gibt es einiges, was Sie tun können, um Ihre Daten zu anonymisieren.

5.1 Umfragen

Bei Umfragen sollten Sie ganz genau überlegen

- Wer könnte hinter der Umfrage stecken?
- Wie wichtig ist es Ihnen, dass Ihre Angaben anonym bleiben?

Grenzen der Anonymisierung bei Umfragen
Bei Umfragen müssen Sie davon ausgehen, dass immer klar ist, wer Sie sind.

5.2 Social Media

Bei Social Media kommt es darauf an, welche Social Media Sie benutzen. Wenn Sie sich auf Facebook, Instagram oder TikTok bewegen, haben Sie keine Chance auf Privatsphäre oder Anonymisierung. Hier müssen Sie immer davon ausgehen, dass Sie beobachtet werden, die Anbieter Profile von Ihnen erstellen und diese verkaufen. Bei ***TikTok***, können Sie sogar Gefahr laufen, dass Sie persönlich verfolgt und beobachtet werden.
Grenzen der Anonymisierung bei Social Media
Wie schon beschrieben, können Sie Ihre Privatsphäre bei Social Media nicht schützen. Selbst enge Einstellungen für Privatsphäre schützen Sie nicht davor, ausgekundschaftet zu werden, denn die Anbieter von Social Media leben davon, dass sie die Daten ihrer Mitglieder zu Profilen zusammenfassen und verkaufen. Überlegen Sie daher ganz genau, mit wem Sie wo „befreundet“ sein wollen und schränken Sie Ihre Nutzung von Social Media so weit es möglich ist ein. Eine Ausnahme stellt hier das soziale Netzwerk ***Mastodon*** dar, welches ***dezentral*** organisiert ist und auf Spendenbasis arbeitet. Der ***Landesbeauftragte für Datenschutz und Informationssicherheit Baden Württemberg***, Stefan Brink, nutzt und empfiehlt Mastodon.

5.2.1 Spezialfall Messenger

Bei Messengern haben Sie durchaus die Möglichkeit anonymisiert zu kommunizieren. Dabei kommt es vor allem darauf an, dass der Messenger den Sie nutzen eine ***Ende-zu-Ende-Verschlüsselung (E2EE - End-to-End-Encryption)*** anbietet. Das heißt, dass Ihre Daten auf dem Ausgangsgerät verschlüsselt werden. Das sie über verschlüsselte Leitungen, verschlüsselt übertragen werden. Das bieten einige Messenger an. Nicht allen kann man glauben, dass sie wirklich so handeln.

- ***Telegram*** behauptet, eine E2EE zu haben. Nachweislich werden jedoch alle Daten die Sie bei ***Telegram eintippen in Echtzeit auf deren Server übertragen***, auch, wenn Sie diese Daten anschließend wieder löschen, ohne sie abgeschickt zu haben.
  Telegram kennt keine Anonymität. Ihre Daten werden in jedem Fall, immer und ohne Perspektive der Löschung, gespeichert. Wer hinter Telegram steckt ist unklar. Es gibt wohl zur Zeit kaum einen gefährlicheren Messenger als Telegram.
- ***WhatsApp*** behauptet auch, eine E2EE zu verwenden. Meta, der Konzern hinter WhatsApp nimmt sich das Recht heraus, all Ihre Metadaten zu speichern und zu verarbeiten. Sie verkaufen die Daten nicht, aber behalten sich vor, die Daten an befreundete Unternehmen weiterzugeben – die sie dann verkaufen.
  Grenzen der Anonymisierung bei WhatsApp
  WhatsApp behauptet zwar, dass die mit ihm verfassten Nachrichten E2EE sind, dennoch können Mitarbeiter von WhatsApp ***Ihre Nachrichten unter bestimmten Umständen lesen***. Das ist seltsam, denn eine echte E2EE, bedingt, dass nur der Sender und der Empfänger die Möglichkeit haben, eine Nachricht zu entschlüsseln. Daher sind Zweifel angebracht, dass WhatsApp wirklich eine E2EE verwendet.
  Weiterhin lässt WhatsApp Ihre Metadaten vermarkten. Die Bedeutung von Metadaten sind in ***Punkt 3.2 Warum sollte ich meine Daten anonymisieren*** beschrieben.

- ***Signal*** ist ein Messenger, der Ihnen einen hohen Grad an Anonymisierung bietet. Dieser Messenger hat eine echte E2EE und speichert nach eigenen Angaben nur Ihr Eintrittsdatum (das Datum an dem Sie Signal installiert haben) und das Datum der letzten Nachricht.
  Grenzen der Anonymisierung bei Signal
  Signal könnte die Metadaten Ihrer gesamten Kommunikation verwerten. Sie müssen darauf vertrauen, dass dies nicht geschieht, so wie Signal es vorgibt. Ebenso könnte Signal ein Soziogramm von Ihnen erstellen, denn es kennt Ihre Kontakte. Die Zusage von Signal, vertraulich zu arbeiten, erscheint jedoch glaubhaft. Da Sie Signal nur nutzen können, wenn Sie Ihre Telefonnummer preis geben, ist hiermit ein großer Teil Ihrer Anonymität nicht mehr gegeben.
- ***Threema*** spricht sich mit englischem *Th* am Anfang. Ursprünglich hieß Threema Eeema, was für End-to-End-Encrypted Messaging App stand. Die Betreiber haben schnell gemerkt, dass das etwas umständlich klingt und daraus Threema – *3x E* - gemacht. Threema ist ein Messenger, der in der Schweiz beheimatet ist. Er bietet Ihnen ein hohes Maß an Anonymität, da Sie Threema nutzen können, ohne, dass Sie irgendwelche Kontakte bekanntgeben müssen, oder Ihre Telefonnummer angeben müssten. Bei Threema können Sie mit einer so genannten Threema-ID kommunizieren.
  Grenzen der Anonymisierung bei Threema
  Auch bei Threema sind Sie darauf angewiesen, dass der Anbieter sich so verhält, wie er es verspricht. Da das das Geschäft von Threema ist, es kostet einmalig 5,99€ (Stand April 2023), gehe ich davon aus, dass ich Threema vertrauen kann, und Threema kein Profil von mir erstellt.

5.3 Telefonieren

Ein Aspekt an den die Meisten bei Vertraulichkeit und Anonymität nicht denken, ist das Telefonieren. Telefonanbieter haben die Möglichkeit perfekt Soziogramme zu erstellen, indem sie die Telefonnummern auswerten, mit denen wir kommunizieren. Telefonie ist heute zum allergrößten Teil digital. Das macht es leichter, Profile zu erstellen, als auch Gespräche abzuhören.
Dagegen können Sie sich jedoch wehren, indem Sie beim Telefonieren auf Apps wie Signal oder Threema zurückgreifst. Beide bieten E2EE verschlüsselte Telefonate, auch als Gruppentelefonate, an. Diese Gespräche sind somit erheblich schwerer zu belauschen, als „normale“ Gespräche.

Grenzen der Anonymisierung beim Telefonieren
Hier gilt das Gleiche wie unter 5.2.2 Spezialfall Messenger bereits erwähnt. Sie müssen auch hierbei den Anbietern von Signal und Threema vertrauen.

5.4 Surfen

Am meisten Daten fallen beim Surfen im Internet an. Wie unter ***2.1 Ich habe nirgends meinen Namen angegeben*** erwähnt, können Sie das über die Website ***Browserleaks*** nachvollziehen. Beim Surfen können Sie allerdings auch sehr viel für Ihre Privatsphäre tun, indem Sie Ihre Daten anonymisieren. Dafür gibt es verschiedene Möglichkeiten.

5.4.1 Der richtige Browser

Zum Thema der richtige Browser haben wir zwei Vorträge und dazugehörige Skripte.

- Mein Browser - was verrät die Plaudertasche über mich?
- Mein Browser - wie bringe ich die Plaudertasche zum Schweigen?

5.4.2 Browser die Sie meiden sollten:

- Internet Explorer
- Edge
- Opera
- Vivaldi

Diese Browser schnüffeln Sie umfangreich aus.

5.5 TOR - ein Browser, der Ihnen hilft, ein hohes Maß an Anonymität zu erlangen

Mit dem ***TOR Browser*** können Sie ein hohes Maß an Anonymität erreichen.
Das funktioniert wie folgt. Sie verbinden sich mit einem Server des TOR-Netzwerks, einem so genannten Entry-Node. Dieser Server nimmt Ihre Anfrage an und verschlüsselt sie. Diese verschlüsselte Anfrage "verpackt" er in einen "Mantel", der an einen weiteren Server des Netzwerks geht. Auch diese Anfrage ist verschlüsselt, und es weiß immer nur der jeweils vorherige Server, wer die Anfrage gestellt hat. Kommt Ihre Anfrage beim Exit-Node an, sendet dieser sie ins Internet um die Anfrage auszuführen. Auf dem gleichen Weg kommt die Antwort zu Ihnen zurück.
Das TOR-Netzwerk ist das Netzwerk in dem Sie auch das Darknet finden. Sicherlich haben Sie schon das eine oder andere Mal gehört, dass dort kriminelle Online-Marktplätze ausgehoben worden sind. Das zeigt Ihnen auch die ***Grenzen der Anonymisierung mit TOR*** Es bedarf eines sehr großen Aufwands, um Nutzer im TORnetzwerk zu identifizieren und zurückverfolgen zu können, aber es ist eben nicht unmöglich. Dennoch bietet TOR Ihnen die Möglichkeit sich (relativ) unbeobachtet über alles mögliche zu informieren. Sie haben auch die Möglichkeit anonyme E-Mailadressen über TOR einzurichten. Dazu haben wir einen Vortrag „E-Mailing aber sicher".

Wichtig bei der Nutzung von TOR
Wichtig bei der Nutzung von TOR ist, dass Sie an dem Browser nichts verändern, nachdem Sie ihn geöffnet haben. Nicht die Größe, keine Einstellungen, fügen Sie keine Add-ons hinzu. Benutzen Sie TOR einfach so, wie er kommt. Würden Sie auch nur irgendetwas verändern, wären Sie als Individuum erkennbar.
Der häufigste Fehler den Nutzer von TOR begehen, der zur Deanonymisierung führt, ist, dass sie sich von ihrem Rechner zu TOR direkt verbinden. Das ist nicht gut, weil der Weg von Ihrem Rechner zum Entry-Node schlicht per TLS (Transport Layer Security) verschlüsselt ist. Das heißt aber auch, dass Ihre Anfrage auf dem Weg ins TOR-Netzwerk bis zu 40 Zwischenstationen passiert. An jeder Zwischenstation wird Ihre Anfrage kurz entschlüsselt und im Klartext zwischengespeichert – inklusive der Metadaten. Das birgt das Risiko, erkannt zu werden.

Dieses Problem können Sie umgehen, indem Sie ein so genanntes VPN (Virtuelles Privates Netzwerk) verwenden. Das ist eine Software, die dafür sorgt, dass Ihre Daten auf Ihrem Gerät verschlüsselt, auf

direktem Weg – ohne Zwischenstopp - zum Entrynode gesandt werden und erst dort der Entry-Node sehen kann, was Sie wissen wollen. Ich nutze dafür den Anbieter Proton mit seinem Angebot ***ProtonVPN***. Es gibt eine kostenlose Version dieses VPNs. Auch beim VPN müssen Sie dem Anbieter vertrauen können, denn Ihr gesamter Datenverkehr läuft über dessen Server.

6 Fazit

Es gibt viele Stellen, die Ihre Daten haben wollen, denn sie sind wertvoll. Dagegen, dass Ihre Daten missbraucht werden, können Sie sich wehren.

Oftmals wird Ihnen Anonymisierung versprochen, jedoch ist dies ein so schwammiger Begriff, dass Sie nicht wissen, ob es trotz der Anonymisierung nicht immer noch möglich ist, nachzuvollziehen, wer Sie sind.

Daher müssen Sie sich selber um Anonymisierung kümmern, um unsere freiheitliche Demokratie zu schützen, um sicher zu stellen, dass Sie selber keine Nachteile erleiden.

7 Quellen

1. Acxiom - https://www.acxiom.com/
2. Anonymisieren – Wikipedia - https://de.wikipedia.org/wiki/Anonymisierung_und_Pseudonymisierung
3. Browserleaks – eine Website, die zeigt, welche Daten der Browser überträgt - https://browserleaks.com/
4. de Montjoye, Y.-A., Radaelli, L., Singh, V. K. & Pentland, A.. Science . Unique in the shopping mall:On the reidentifiability ofcredit card metadata. Ausführliche Informationen zu Metadaten. https://science.sciencemag.org/content/sci/347/6221/536.full.pdf
5. Der Landesbeauftragte für Datenschutz und Informationssicherheit Baden Würtemberg - https://www.baden-wuerttemberg.datenschutz.de/barrierefreiheit/
6. Hiller, A., Hakuna Metadata - Warum Metadaten und Browserverläufe mehr über uns verraten als oft vermutet. netzpolitik.org – Erläuterung, weshalb Metadaten so gefährlich für die Anwender sind https://netzpolitik.org/2017/hakuna-metadata-warum-metadaten-und-browserverlaeufe-mehr-ueber-uns-verraten-als-oft-vermutet/
7. ITS Us. - https://www.th-luebeck.de/forschung-und-transfer/kompetenzen/fachgruppen/it-sicherheit/studentische-aktivitaeten/
8. Jewgeni Wiktorowitsch Prigoschin - https://de.wikipedia.org/wiki/Jewgeni_Wiktorowitsch_Prigoschin
9. Johns Hopkins University. The Price of Privacy: Re-Evaluating the NSA, A Debate – Die Podiumsdiskussion in der Michael Vincent Hayden erklärt, dass Amerika Menschen auf Grund von Metadaten tötet (ehemaliger Direktor der CIA, später NSA) https://www.youtube.com/watch?v=kV2HDM86XgI
10. Mastodon - https://joinmastodon.org/de
11. Pillar investigates: USCCB gen sec Burrill resigns after sexual misconduct allegations - https://www.pillarcatholic.com/p/pillar-investigates-usccb-gen-sec
12. Proton(VPN) - https://protonvpn.com/
13. Proton(VPN) kostenlos - https://account.protonvpn.com/signup?plan=free&currency=EUR
14. Signal – der Messenger - https://signal.org/de/#signal

15. Sturm auf das Kapitol in Washington 2021 – Wikipedia - https://de.wikipedia.org/wiki/Sturm_auf_das_Kapitol_in_Washington_2021
16. SWR Wissen - Diese Daten sammelt Tiktok - https://www.swr.de/wissen/daten-spionage-wird-tiktok-in-den-usa-verboten-100.html
17. Telegram-Chat: der sichere Datenschutz-Albtraum – eine Analyse und ein Kommentar, heise security - https://www.heise.de/hintergrund/Telegram-Chat-der-sichere-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html
18. TH Lübeck - https://www.th-luebeck.de/
19. The Pillar - https://www.pillarcatholic.com/
20. TOR Browser - https://www.torproject.org/download/
21. WhatsApp: In diesem Fall kann der Messenger eure Nachrichten lesen – netzwelt - https://www.netzwelt.de/news/193161-whatsapp-diesem-fall-messenger-nachrichten-lesen.html