Samstag, 08. Juni 2024, 15:59 Uhr
~16 Minuten Lesezeit

Verwanzte Welt

Für die Bequemlichkeit, die Smartphones uns bieten, bezahlen wir mit der Preisgabe von Freiheit. Die Geräte spionieren uns nicht nur aus, sie formen auch unser Bewusstsein.

von Tom-Oliver Regenauer
Foto: PeopleImages.com - Yuri A/Shutterstock.com

Was ist uns lieber — Freiheit oder Gängelung? Verfügbarkeitsstress oder Entspannung? Ein Rest von Intimsphäre oder totale Transparenz? Informelle Selbstbestimmung oder das Gefühl, für kommerzielle Zwecke nur benutzt zu werden? Sich sicher zu fühlen oder ständigen Angriffen auf unseren Geist ausgesetzt zu sein? Die Antwort auf all diese Fragen sollte einfach sein. Dennoch trifft die Mehrheit der Menschen bei diesen Entscheidungen Tag für Tag die für sie jeweils schädliche Wahl. Das Smartphone ist zum Tyrannen im Taschenformat geworden. Für viele ist es ein Suchtfaktor, und den wenigen, die noch leichten

Herzens darauf verzichten könnten, wird das Gerät zunehmend durch strukturelle Zwänge aufgedrängt. Im selben Maß, wie das Smartphone „unentbehrlich" geworden ist, wachsen die Gefahren und Zumutungen, die mit seiner Benutzung verbunden sind. Programmierer arbeiten auf Hochtouren an Anwendungen, die uns zunehmend nicht nur ausspionieren, sondern unseren Geist auch im Interesse der herrschenden Narrative zu deformieren versuchen. Die von Apple und Google konfigurierten Geräte sind weitaus mehr als nur „nützliche Werkzeuge" — es sind Wanzen, Überwachungskameras, Datenkraken und Waffen zur psychologischen Kriegsführung in einem.

„Die Gefahr, dass der Computer so wird wie der Mensch, ist nicht so *groß wie die Gefahr, dass der Mensch so wird wie der Computer*" (Konrad Zuse).

Die meisten Menschen hegen einen vagen Verdacht. Viele haben das ein oder andere Indiz wahrgenommen, das belegt, das ein solcher Verdacht durchaus begründet sein könnte. Trotzdem schaffen es die wenigsten, ihr Verhalten objektiv zu analysieren und einmal verinnerlichte Verhaltensweisen zu ändern. Gewohnheiten und Routinen sind schwer loszuwerden. Vor allem, wenn diese sich zu Sucht oder Zwang entwickeln. Das passiert nicht nur bei Alkohol und Drogen, sondern in geradezu epidemischer Weise bei etwas, das ich bevorzugt „Taschenspion" nenne: dem Smartphone.

Während die exzessive Nutzung des Geräts in praktisch allen Lebenslagen fraglos zur sozialschädlichen Unart — um nicht zu

sagen Plage oder Seuche — avanciert ist, markiert der Suchtfaktor des kontinuierlich potenter werdenden Begleiters nicht einmal das größte Problem. Denn Abhängigkeiten lassen sich überwinden, wenn auch müh- und langsam; dass die Geräte zur lückenlosen Observation, Manipulation und Transformation der Gesellschaft genutzt werden aber nicht. Denn sie haben sich längst zu tief in die sozioökonomischen Strukturen unserer Zeit gefressen. Einem Großteil der Bevölkerung erscheint der Alltag ohne Smartphone kaum mehr organisierbar. Ob Kommunikation, Nachrichten, Wettervorhersage, Routenplaner, Zahlungen, Zwei-Faktor-Authentifizierung, Fotosammlung, Videostreaming oder Musikarchiv — der mobile Begleiter hilft.

Doch das irreführend positiv und progressiv geprägte Lifestyle-Image des nützlichen Allroundtalents täuscht über dessen sprichwörtlich böse Absichten hinweg. Diese offenbaren sich bei einem Blick auf seine Entwicklung, die dahinterstehenden Konzernstrukturen, ein paar erschreckende Zahlen zu seinen Effekten auf Mensch und Gesellschaft und vor allem auf das, was Smartphones mit Android/Google- oder iOS/Apple-Betriebssystem ganz ohne Zutun oder Wissen des Nutzers treiben.

Zur **Kontextualisierung** (https://explodingtopics.com/blog/mobile-internet-traffic): Über 60 Prozent des gesamten Internetverkehrs sowie 55 Prozent der weltweiten Webseitenzugriffe finden mittlerweile über Mobiltelefone statt (Stand: April 2024). 98 Prozent der Geräte laufen entweder auf Android oder iOS. 92,3 Prozent aller Internetnutzer greifen von ihrem Taschencomputer aus auf das Internet zu. **6,92 Milliarden** (https://www.zippia.com/advice/smartphone-usage-statistics/) Menschen nennen ein solches Gerät derzeit ihr eigen. Das sind Ende 2023 gut 86 Prozent der Weltbevölkerung, die damit, je nach Region, zwischen zwei und knapp sechs **Stunden** (https://explodingtopics.com/blog/smartphone-usage-stats) pro Tag verbringen. Der alarmierende globale **Durchschnitt**

(https://explodingtopics.com/blog/screen-time-stats) für Menschen im Alter von 16 bis 64 Jahren liegt aktuell bei sechs Stunden und 58 Minuten Bildschirmzeit pro Tag. Weit über **hundert Mal** (https://www.der-bank-blog.de/smartphone-adiction/nachdenkliches/29112/) greift man in diesem Zeitraum nach dem Gerät. Tendenz steigend. **35,2 Prozent** (https://www.bankmycell.com/blog/average-screen-time-on-iphone-android) der Nutzungsdauer verbringen iPhone- und Android-Kunden auf Social Media (Stand: 2021). Zum Telefonieren wurden Smartphones schon seit **2012** (https://www.mobile-zeitgeist.com/studie-smartphones-werden-kaum-noch-zum-telefonieren-genutzt/) kaum noch genutzt. „Smartphone-Penetration", wie man die Marktdurchdringung im **Vertriebsjargon** (https://marketsplash.com/smartphone-statistik/) der Telekommunikationsbranche bezeichnet, scheint in Anbetracht dieser Zahlen eine zunehmend zutreffende Beschreibung für die allgemeinen Entwicklungen darzustellen. Denn das Gerät vergewaltigt das Gehirn.

Trotzdem hat das Handy die Welt im Sturm erobert. Zuerst war es die Begeisterung für das Neue, die Freude am mobilen Telefonieren. Am Spielzeug selbst. Es hatte was von Amateurfunk. Oder Gameboy. Dann kam die SMS. Dicht gefolgt von mobiler E-Mail und der Möglichkeit, nun auch unterwegs ins Internet gehen zu können. Dann folgte das erste iPhone.

> ***Was dieser technische Fortschritt seit 2007 mit einem im Kern sozialen Wesen angestellt hat, sehen wir heute an Bushaltestellen, Restaurant-Tischen, auf Schulhöfen oder bei gemeinsam einsamen Gruppen von Display-Junkies. Die Auswirkungen sind verheerend. Der spielerisch-leichte Flair des Handfunk-Feelings ging rasch verloren. Was das Gerät heute primär auslöst, sind Stress, Druck, Verwirrung, Zwänge und Ängste.***

Selbst eine oberflächliche Suche fördert sofort **sechs**

(https://www.menshealth.de/behandlung/erste-hilfe-fuer-typische-handy-krankheiten/) bis **neun** (https://www.onmeda.de/krankheiten/galerie-handykrankheiten-id215804/) „medizinische Errungenschaften", sprich Zivilisationskrankheiten zutage, die auf unsachgemäße Nutzung des Smartphones zurückzuführen sind. Von der Smartphone-Akne und Video-Schulter bis hin zum Handy-Nacken, **PVS** (Phantom Vibration Syndrome), FOMO (Fear of missing out), PtSS (Post-textliches Stress-Syndrom) oder MAIDS, dem „Mobile and Internet Dependency Syndrome". Das unreflektierte Nutzungsverhalten, das Distraktionsdiktat der Plattformökonomie, **verändert** (https://mitsloan.mit.edu/ideas-made-to-matter/study-social-media-use-linked-to-decline-mental-health) unser **Denken** (https://www.sciencedaily.com/releases/2017/06/170623133039.htm), die Physis, Gehirnkapazität, Augen und unsere emotionalen wie sozialen Fähigkeiten. Von der „mentalen Gesundheitskrise", die längst mehr nicht nur bei **Teenagern** (https://www.nbcnews.com/health/health-news/social-media-mental-health-anxiety-depression-teens-surgeon-general-rcna85575) durch intensive **Social-Media-Nutzung** (https://mitsloan.mit.edu/ideas-made-to-matter/study-social-media-use-linked-to-decline-mental-health) ausgelöst wird, gar nicht erst zu sprechen. Es dürfte im Lichte nackter Zahlen und sich abzeichnender Langzeiteffekte also unstrittig sein, dass der vermeintlich praktische Alltagshelfer die Spezies Mensch evolutionär nicht wirklich vorangebracht hat.

> ***Im Rausch permanenter Erreichbarkeit geht leider unter, dass Smartphones uns nicht nur massiven physischen und sozialen Schaden zufügen. Nicht umsonst bezeichne ich sie meist als Waffe. Oder Wanze. Denn Wissen ist Macht — und niemand weiß so viel über den Menschen der Postmoderne wie Google oder Apple.***

Die Konzerne kennen nicht nur alle unsere **Kontakte**

(https://www.washingtonpost.com/technology/2021/07/15/turn-off-contact-sharing/), Bewegungsdaten, Songs, Fotos, Videos, Bankverbindungen, Kontostände und E-Mail-Anhänge, sondern auch unsere Suchanfragen, politischen Ansichten, Sorgen, sexuellen Präferenzen, vertraulichen Nachrichten und intimen Gespräche. Diese Informationen zeichnen nicht nur ein detailliertes Bild vom sozialen Netzwerk jedes Nutzers, sondern auch ein psychologisches Profil, das exakter kaum sein könnte. Über **72 Millionen** (https://appdevelopermagazine.com/72m-data-points-collected-on-children-in-spite-of-coppa/) Datenpunkte sammeln Anbieter für Digitalwerbung in den USA pro Kind bis zu dessen 13. Lebensjahr. Facebook hortet mindestens **52.000** (https://www.komando.com/social-media/facebooks-52000-data-points-on-each-person-reveal-something-shocking-about-its-future/489188/) Einträge je Nutzer. Das harmloseste Ergebnis dieser Datensammlung ist zielgerichtete Werbung, die uns auf Basis von Daten und Nutzungsverhalten auf Plattformen und Webseiten angezeigt wird.

Deutlich gravierender sind die Auswirkungen durch Datenmissbrauch — siehe Cambridge Analytica **Skandal** (https://www.businessinsider.com/facebook-87-million-peoples-data-taken-in-cambridge-analytica-scandal-2018-4) —, mentale Manipulation, elektronische Ausweise, digitale Währungen, algorithmisierte Zensur, Sozialkreditsysteme, CO_2-Budgetierung und Geofencing. Alles Projekte, die ohne Smartphone überhaupt nicht möglich wären. Wer permanent seinen Standort an eine Zentrale übermittelt, ist leicht zu kontrollieren. So werden bereits heute viele Inhalte, die in der Schweiz oder anderen Nicht-EU-Ländern angezeigt werden, in EU-Staaten unterdrückt. Auch manch ein Musiktitel lässt sich nicht mehr abspielen, wenn man auf Reisen ist. „In Ihrer Region nicht verfügbar“, heißt es da. Geofencing-Exklusion light.

Smartphones **überwachen**

(https://www.comparitech.com/blog/vpn-privacy/stop-mobile-phone-tracking/) und dokumentieren die **Position** (https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html) ihres Besitzers natürlich auch, wenn alle GPS-Funktionen deaktiviert sind oder das Gerät komplett ausgeschaltet ist, wie ein **Artikel** (https://slate.com/technology/2013/07/nsa-can-reportedly-track-cellphones-even-when-they-re-turned-off.html) zu NSA-Überwachungstechniken von 2013 oder ein **Bericht** (https://www.princeton.edu/news/2017/11/29/phones-vulnerable-location-tracking-even-when-gps-services) der Princeton University von 2017 zeigen. Das optionale Abschalten von Standort- und Ortungsdiensten oder der Hintergrundaktualisierung in den Smartphone-**Menüs** (https://www.theverge.com/21401280/android-101-location-tracking-history-stop-how-to) bezieht sich nur auf Dienst- und Drittanbieter-Apps. Wobei viele davon unbeeindruckt trotzdem Daten übertragen. **Verkauft** (https://www.aclu.org/news/immigrants-rights/the-u-s-government-is-secretly-using-cell-phone-location-data-to-track-us-were-suing) werden solche Lokationsdaten bevorzugt an Regierungen und Geheimdienste.

Und die Ortungsdienste von Google und Apple lassen sich weder abschalten, noch ist klar, was mit den Daten geschieht. So war beispielsweise meine gesamte Reiseroute kreuz und quer durch Kuba auf den Meter genau bei Google Maps dokumentiert, obwohl ich alle Tracking-Funktionen deaktiviert hatte und sich auf der Insel mit dem Smartphone keine Datenverbindung herstellen lässt, wenn man sich nicht gerade in der Nähe eines Hotel-Hotspots befindet und lokal erhältliche Guthabenkarten für Daten freischaltet. Dieser Programmatik folgend ist es ein Leichtes, digitales Geld oder moderne **PKW** (https://privacyacademy.com/modern-cars-are-designed-to-control-you-2/) demnächst so zu programmieren, dass sie nur in einem vordefinierten Radius funktionieren. So wird

das Smartgrid zum unsichtbaren Käfig.

Welche Ziele der digital-finanzielle Komplex des Korporatismus verfolgt, zeigt sich exemplarisch an den jüngsten Entwicklungen für Android-Smartphones. Beispiel **Google Play Protect** (https://techcrunch.com/2023/11/04/google-play-android-real-time-app-scanning-sideload-apps/), eine Betriebssystemsoftware, die vor „schädlichen", oder „unbekannten" Drittanbieter-Apps warnen, sie scannen und deren Installation verhindern soll. Vorgeblich zur Sicherheit des Nutzers. Es braucht jedoch nicht viel Fantasie, um sich vorzustellen, dass auch unliebsame Applikationen von Odysee, Rumble, *RT*, *Al Jazeera* oder anonyme Krypto-Wallets rasch auf der Liste schädlicher Software landen und so nicht mehr verwendbar sind.

Apple machte 2021 Schlagzeilen mit der Bekanntgabe, „**Client Side Scanning** (https://mitsloan.mit.edu/ideas-made-to-matter/study-social-media-use-linked-to-decline-mental-health)" auf iPhones und iPads installieren zu wollen. Diese **Erweiterung** (https://www.lawfaremedia.org/article/apple-client-side-scanning-system) sollte es dem Tech-Konzern ermöglichen, sämtliche Fotos zu scannen, die auf iCloud hochgeladen werden. Damit sollte die Verbreitung von Kinderpornografie — CSAM (Child Sexual Abuse Material) — erschwert werden. Das **Internet Architecture Board** (https://de.wikipedia.org/wiki/Internet_Architecture_Board) (IAB) warnte damals eindringlich vor diesem skandalösen Paradigmenwechsel in puncto Privatsphäre und Datenverschlüsselung. Nach einigem Tumult nahm Apple offiziell Abstand von diesem Vorhaben. Installiert wurde die Software allerdings trotzdem. Das Programm befindet sich also heute auf jedem Apple-Gerät mit aktuellem Betriebssystem. Es sei jedoch nicht aktiv, teilen Apple, die Faktencheck-Industrie und diverse **Tech-Blogger** (https://eclecticlight.co/2023/01/18/is-apple-checking-images-we-view-in-the-finder/) mit.

Das ist allerdings nicht korrekt, wie man anhand der Ausführungen des Cybersicherheitsexperten **Rob Braxman** (https://www.youtube.com/watch?v=WTGY4kJRXu0) erkennen kann. Die Funktion ist nur gut getarnt. Bei genauerer Betrachtung wird klar: Jedes Foto, das man mit einem iPhone, iPad oder Mac aufnimmt, wird lokal gescannt. Wie sonst sollte das Gerät Gesichter identifizieren und für spezielle Alben vorschlagen können. Dabei wird jedes Bild mit sogenannten **Neural Hashes** (https://towardsdatascience.com/apples-neuralhash-how-it-works-and-ways-to-break-it-577d1edc9838) versehen, mit eindeutigen Identifikatoren, die beim Upload in die Cloud übertragen und katalogisiert werden. Privatsphäre für Fotos gibt es nicht mehr. Denn auch wenn die Cloud-Dienste deaktiviert sind, übertragen Apple-Geräte die Transkripte der Neural-Hash-Datenbank nachts heimlich an die Zentrale. Und löschen lassen sich Bilder in der Cloud auch nicht so einfach. Klickt man im Kontextmenü eines Fotos auf „Delete“, wird das Foto nicht wirklich gelöscht, sondern nur in der User-Ansicht ausgeblendet. Wie lange Apple und Google die Daten auf ihren Servern belassen, ist nicht bekannt. Vermutlich lange. Denn wie ein **Versuch** (https://www.copytrans.net/support/how-to-restore-permanently-deleted-photos-and-videos-from-icloud/) von „CopyTrans“ zeigt, lassen sich aus der iCloud auch Fotos herunterladen, die vermeintlich bereits vor Jahren gelöscht wurden.

Google geht noch einen Schritt weiter. Wie das „Medium für digitale Freiheitsrechte“ **Netzpolitik.org** (https://netzpolitik.org/2024/client-side-scanning-google-will-vor-telefonbetrug-warnen/#!) am 16. Mai 2024 ausführt, plant das Unternehmen, künftig alle Anrufe seiner Nutzer zu scannen — und zu speichern —, um seine Kunden so vor Telefonbetrügern warnen zu können. Vorratsdatenspeicherung war gestern. Mittlerweile arbeiten neben den Tech-Konzernen selbstverständlich auch die transatlantisch bewegten Überwachungszirkel in **EU** (https://www.internetsociety.org/resources/doc/2023/client-

side-scanning/), Großbritannien und den USA an Gesetzen, die Client Side Scanning und anlasslose Totalüberwachung legalisieren. Auch wenn derartige Unterfangen das Recht auf den Schutz persönlicher Daten oder die Unschuldsvermutung ad absurdum führen und Projekte wie die sogenannte **Chatkontrolle** (https://www.patrick-breyer.de/en/posts/messaging-and-chat-control/) nach allgemeinem Rechtsverständnis **illegal** (https://www.infosecurity-magazine.com/news/eus-clientside-scanning-plans/) sind.

Doch schlimmer geht immer. Smartphones, die sich mit Gesichtserkennungssoftware wie „Face ID" entsperren lassen — als wäre der an polizeidienstliche Erfassung erinnernde Fingerabdruck nicht schon genug gewesen —, fertigen alle fünf **Sekunden** (https://techthelead.com/tiktok-user-shows-how-iphone-takes-infrared-pictures-of-you-every-five-seconds/) ein **Infrarotbild** (https://www.itechpost.com/articles/105677/20210518/iphone-spying-taking-invisible-photos-disable-face-id-infrared-camera.htm) von ihrer Umgebung an. Selbst dann, wenn der Bildschirm gesperrt oder verdeckt ist. Nach Angaben von Apple ist das nötig, um das Gerät zügig per Blick auf den Bildschirm entsperren zu können. Die von Face ID angefertigten Fotos werden in mathematische Strukturen umgewandelt und auf dem Telefon abgelegt. Einem Gerät, das jede **Nacht** (https://archive.ph/BQTcB) gegen drei Uhr unaufgefordert nicht einsehbare Datenpakete „nach Hause" schickt.

> ***Die Kameras moderner Smartphones können aber noch ganz andere Dinge. Sie folgen zum Beispiel dem Blick des Besitzers, um dessen Handlungen antizipieren oder Befehle empfangen zu können. Analysieren seine Mimik. „Aufmerksamkeitssensible Funktionen", nennt das die Firma mit dem Apfel-Logo. Wem bei der immer öfter biometrisch gehandhabten Einreisekontrolle an Flughäfen mulmig zumute ist, sollte demnach wohl kein Smartphone nutzen.***

Der Taschenspion hört natürlich auch zu. Und zwar **permanent** (https://nordvpn.com/de/blog/is-my-phone-listening-to-me/). Wie sonst sollte „Siri“ wissen, wann man etwas von ihr will. Doch auch hier wiegeln „**Experten** (https://www.abendblatt.de/ratgeber/article233448559/Passgenaue-Handywerbung-Hoert-mich-mein-Smartphone-ab.html)“ und leitmedialer Komplex vehement ab und **behaupten** (https://www.giga.de/artikel/werbung-auf-dem-smartphone-hoert-das-handy-mit/), es sei reiner Zufall, dass Werbeanzeigen und Social-Media-Inhalte exakt das widerspiegeln, was im Umfeld des Gerätes in den letzten Stunden besprochen wurde. ***USA Today*** *(https://eu.usatoday.com/story/tech/columnist/2019/12/19/your-smartphone-mobile-device-may-recording-everything-you-say/4403829002/)* räumt in diesem Kontext zwar ein, dass das Telefon zuhöre, diese Daten aber nur lokal verarbeitet würden und keine Sprachaufzeichnungen an Apple, Google oder Amazon übertragen würden. Und das ist sogar korrekt. Denn die Datenmenge wäre zu groß. Stattdessen übertragen die Smartphones Textdateien mit Transkripten, die heute jeder sehen kann, wenn er mit iMessage eine Voicemail aufnimmt und diese umgehend als Text erscheint. Diesen Aspekt sparen die Faktenchecks beflissentlich aus.

Zudem werden die KI-basierten **Anwendungen** (https://pubmed.ncbi.nlm.nih.gov/37047862/) „zur Vermeidung häuslicher Gewalt“ oder präventiver „Gefahrenabwehr“, von denen eine im März 2023 veröffentlichte **Studie** (https://www.mdpi.com/1660-4601/20/7/5246) 136 Stück untersuchte, nur dann wie in Aussicht gestellt funktionieren, nämlich autonom, wenn das Smartphone seine Kameras, Mikrofone und Bewegungssensoren permanent nutzt, um seine Umgebung zu überwachen.

> ***Dabei stellt das einzelne Gerät künftig nicht mehr das größte Problem für freiheitsaffine Zeitgenossen dar.***

> ***Denn die Taschenspione überwachen seit geraumer Zeit nicht mehr nur ihren jeweiligen Besitzer, sondern auch dessen gesamtes Umfeld.***

Dazu kommunizieren die Geräte untereinander, tauschen Informationen wie IMEI-Nummern, IP-Adressen und Kontaktdaten aus. **iPhones** (https://www.maclife.de/news/ios-135-verwaltest-covid-19-benachrichtigungen-am-iphone-100116709.html) bieten diese Funktion seit September 2020 (iOS 13.7) flächendeckend über das **Betriebssystem** (https://netzpolitik.org/2020/update-bei-google-und-apple-kontaktverfolgung-soll-bald-auch-ohne-app-klappen/) an. Die über Bluetooth Low Energy (**BLE** (https://www.youtube.com/watch?v=K6HCgBzhibU)) gesammelten Informationen bildeten die Grundlage für die Contact-Tracing-Apps während der Coronakrise. Auch die deutsche Corona-Warn-App nutzte den intransparenten Datenpool. Dafür konnte das Programm über eine Schnittstelle alle Begegnungen der vergangenen 14 Tage auslesen. Ende 2020 entwickelten bereits über **20 Länder** (https://www.spiegel.de/netzwelt/apps/apple-und-google-ermoeglichen-kontaktverfolgung-ohne-app-a-b6286907-62da-4040-be18-7869a0dec57c) Tracking-Applikationen, um die von Big Tech gesammelten Bewegungs- und Begegnungsdaten auslesen und in ihren COVID-Apps darstellen zu können.

Meint: iPhones zeichnen seit knapp vier Jahren jeden Kontakt mit einem anderen iPhone auf und bilden daraus Netzwerkkarten zu Bewegungen und Begegnungen ihrer Besitzer. Im Menü des Smartphones lässt sich diese Funktion zwar deaktivieren – anzunehmen, das Gerät sammle deshalb nicht trotzdem die entsprechenden Daten, ist allerdings naiv. Nach Angaben von Apple sollten diese Informationen übrigens nur lokal gespeichert und nach 14 Tagen automatisch gelöscht werden. Was von solchen Statements zu halten ist, zeigt das vorgängig angeführte Beispiel mit den vermeintlich gelöschten, aber auch nach Jahren wiederherstellbaren iCloud-Fotos.

Google (https://www.zeit.de/digital/2020-09/kontaktverfolgung-apple-google-corona-warn-app-coronavirus) zog natürlich nach und implementierte eine ähnliche Datenkrake. So zeichnen auch Android-Geräte seit Ende 2020 jede Begegnung mit anderen Android-Geräten auf. Damit entstanden zwei riesige **Mesh-Netzwerke** (https://www.bluetooth.com/de/learn-about-bluetooth/feature-enhancements/mesh/mesh-faq/), in denen Maschinen ohne Zutun ihres Besitzers untereinander kommunizieren. In Deutschland verwenden 66,1 Prozent der Smartphone-Nutzer Android – 33,2 Prozent iOS von Apple (**Stand** (https://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland/): März 2024). Damit sind 99,3 Prozent der Bevölkerung kartografiert. Denn seit gut einem Monat verstehen sich die beiden bisher getrennt voneinander spionierenden Betriebssysteme nun auch **gegenseitig** (https://www.youtube.com/watch?v=9xPjIfJI5Jk).

> ***Das läutet nicht nur klammheimlich einen Paradigmenwechsel in Sachen Totalüberwachung ein, ein solches Mesh-Netzwerk schafft darüber hinaus die Grundlage für die Militarisierung der Smartphone-Infrastruktur, weil dieses Netzwerk nicht nur Daten sammeln und senden, sondern auch Befehle empfangen kann.***

So könnte auf Knopfdruck für 99,3 Prozent der Bevölkerung Malware installiert, ein Blackout simuliert oder eine bestimmte Funkfrequenz generiert werden. Diese könnte — wie in meinem **Text** (https://www.regenauer.press/die-sechste-dimension) „Die sechste Dimension“ beschrieben — Nanopartikel und Smartdust zu bestimmten Reaktionen anregen.

In diesem Kontext ist bemerkenswert, dass das iPhone mitnichten auf einen genialen Erfinder zurückzuführen ist — auch wenn sich

Steve Jobs gerne als solcher gerierte —, sondern auf **Militärtechnologie** (https://nintil.com/mazzucato-and-the-iphone-i/). Jobs hat sie nur clever verwendet und vermarktet. Mariana Mazzucato widmete dieser Geschichte ein ganzes Kapitel ihres 2013 publizierten **Buches** (https://en.wikipedia.org/wiki/The_Entrepreneurial_State) „The Entrepreneurial State". Auf 261 Seiten zeigt die Autorin, dass viele der gemeinhin als privatwirtschaftliche Meisterleistung gefeierten Innovationen unserer Zeit eigentlich auf einen interventionistischen Staat zurückzuführen sind. Batterien, Sensoren, Chips, **Siri** (https://www.theatlantic.com/technology/archive/2011/10/darpa-project-s-powering-new-iphone-4s/337134/), Touchscreen — allesamt finanziert und entwickelt von **US-Regierung** (https://thebreakthrough.org/issues/energy/the-iphone-and-the-invisible-hand-of-government) und US-Militär. Eine 2014 von **Business Insider** (https://www.businessinsider.com/the-us-military-is-responsible-for-almost-all-the-technology-in-your-iphone-2014-10) veröffentlichte Grafik verdeutlicht das Ausmaß. Noch 2012 warnte die **DARPA** (https://www.wired.com/2012/02/darpa-iphone/) selbst davor, dass Mobiltelefone bei flächendeckender Verbreitung eine ideale Waffe für verdeckte Angriffe auf die Bevölkerung darstellen.

Google existiert gleichsam nur dank **Forschungsbudgets** (https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance), die von **CIA** (https://medium.com/insurge-intelligence/how-the-cia-made-google-e836451a959e) und NSA zur Entwicklung von Massenüberwachungswerkzeugen zur Verfügung gestellt wurden. Ein firmeninternes **Video** (https://www.theverge.com/2018/5/17/17344250/google-x-selfish-ledger-video-data-privacy) aus dem Jahr 2016 verdeutlicht die Vision von Google, mit „totaler Datensammlung die Gesellschaft verändern" zu können. Wie von Yasha Levine in seinem 2018 publizierten **Buch** (http://surveillancevalley.com/blog/google-

has-been-a-military-contractor-from-the-very-beginning) „Surveillance Valley“ dargelegt, gilt das aber nicht nur für Google, sondern für alle Big-Tech-Konzerne. Selbst bei **CBS *News*** *(https://www.cbsnews.com/news/social-media-is-a-tool-of-the-cia-seriously/)* konnte man 2011 nachlesen, wie intensiv **In-Q-Tel** (https://de.wikipedia.org/wiki/In-Q-Tel), das Investmentvehikel der CIA, bei der Gründung von Google, Facebook, Twitter und Co. mitmischte und wie der Geheimdienst die Unternehmen seither für seine Zwecke missbraucht. Überschrift des CBS-Artikels: „Social Media is a tool of the CIA. Seriously.“ Übersetzt: Soziale Medien sind ein Werkzeug der CIA. Ernsthaft.

Dass man dieser permanenten Smartphone-Überwachung durch Google und Apple auch durch die Verwendung verschlüsselter Messenger-Dienste nicht mehr entkommt, veranschaulicht das unlängst von **Microsoft** (https://learn.microsoft.com/en-us/windows/ai/apis/recall) vorgestellte KI-Dienstprogramm **Recall** (https://www.forbes.com/sites/thomasbrewster/2024/05/28/microsoft-recall-feature-is-always-watching/). Es soll demnächst für Windows ausgerollt werden und dem Benutzer bei der Suche nach Dateien helfen. Dafür macht Recall alle paar Sekunden Screenshots und zeichnet damit alles auf, was auf dem Computer geschieht. Die umgehend Sturm laufenden Datenschützer versuchte Microsoft-CEO Satya Nadella damit zu beruhigen, dass die **Daten** (https://support.microsoft.com/en-us/windows/privacy-and-control-over-your-recall-experience-d404f672-7647-41e5-886c-a3c59680af15) nur lokal gespeichert würden, verschlüsselt seien und nach drei Monaten gelöscht werden sollen. Wenig beruhigend. Denn verschafft sich ein Hacker Zugriff auf einen Computer, muss er nur Recall aufrufen, um Zugang zu Passwörtern oder anderen sensiblen Daten zu erhalten. Ob die Daten nur lokal gespeichert und nach drei Monaten gelöscht werden, ist ebenfalls fraglich. Vor allem aber zeigt ein Programm wie Recall, dass auch technisch sichere Messenger ganz simpel überwacht werden können. Dazu muss man

deren Nachrichten nicht auf dem Server abfangen und entschlüsseln, sondern einfach nur durchgängig auf dem Smartphone fotografieren und zur Übertragung in Textdateien umwandeln.

> ***Zusammenfassend muss man konstatieren: Wer seine Privatsphäre schützen möchte, sollte sein Smartphone abschalten. Oder abschaffen. Denn die von Apple und Google konfigurierten Geräte sind Wanzen, Überwachungskameras, Datenkraken und Waffen zur psychologischen Kriegsführung – keine nützlichen Werkzeuge.***

In diese Kategorie fallen eher die sogenannten Dumb-Phones, mit denen man eigentlich nur telefonieren und SMS versenden kann. Die an die frühen 2000er erinnernden Geräte belästigen den Besitzer weder mit unzähligen unnötigen Applikationen noch mit nie enden wollenden Benachrichtigungen. Keine Dopamin-Shots. Keine Updates. Zudem führen die Geräte kein heimliches Eigenleben. Wenn sie aus sind, sind sie aus. Meist lässt sich sogar der Akku herausnehmen. Darüber hinaus melden solch rustikale Handys nicht permanent den eigenen Standort an eine Zentrale. Diese Argumente scheinen mehr und mehr Menschen zu überzeugen. Das 2017 neu aufgelegte Nokia 3310 verkaufte sich **2023** (https://www.rnd.de/digital/dumbphone-statt-smartphone-die-generation-z-aendert-ihr-handy-verhalten-AAS4DXJALRAZJHIQ54F2MJTPZQ.html) bereits doppelt so oft wie im Vorjahr. Ich selbst nutze seit Längerem wieder ein **Nokia 8210** (https://www.hmd.com/en_int/nokia-8210-4g?sku=16LIBG21A01). Kosten: Circa **70 Euro** (https://geizhals.de/nokia-8210-4g-v106527.html). Mein Smartphone checke ich je nach Bedarf zwei oder drei Mal am Tag. Die restliche Zeit bleibt es auf Flugmodus oder stummgeschaltet an einem fixen Ort. Kommunikation und Aufgaben, die ich zuvor über das Smartphone abgewickelt habe, verlagere ich wieder zurück auf den PC. Die unmittelbaren Auswirkungen dieses Vorgehens auf Tagesablauf und Lebensqualität

sind beachtlich. Befreiend.

Wer nicht auf ein Smartphone verzichten will oder kann, sollte sich nach **Alternativen** (https://murena.com/what-smartphone-without-google/) zu Google und Apple umschauen. Das iPhone fällt dabei aus, da sich das iOS-Betriebssystem nicht verändern oder ersetzen lässt. Android kann allerdings **angepasst** (https://www.theverge.com/2022/5/31/23144917/murena-one-smartphone-degoogle-android) und ohne Google-Dienste genutzt werden. Zudem lassen sich **Smartphone-Alternativen** (https://vivaldi.com/blog/technology/smartphones-5-alternatives-to-apple-google-and-samsung/) auch mit anderen Betriebssystemen wie GrapheneOS betreiben, die die Privatsphäre des Nutzers respektieren – solange man auch seine Apps nicht mehr aus dem Google Play Store, sondern zum Beispiel von **F-Droid** (https://f-droid.org/), **Aurora** (https://www.chip.de/downloads/Aurora-Store-APK-Android-App_183135643.html) oder **APKPure** (https://apkpure.com/de/) herunterlädt.

Als Endgerät bietet sich in unseren Breiten beispielsweise ein **Murena** (https://murena.com/shop/smartphones/brand-new/murena-fairphone-5/) Fairphone oder **Volla Phone** (https://volla.online/de/) an. In den USA ein **Above Phone** (https://abovephone.com/). Das Volla Phone wird ab Werk optional mit zwei Betriebssystemen ausgeliefert, einer Eigenentwicklung sowie GrapheneOS. Damit hat man Kontrolle über die eigenen Daten. Und nach einer kurzen Einarbeitungsphase stellt auch der Verzicht auf Google-Dienste kein Problem mehr dar — denn für praktisch jede Google-App gibt es eine überwachungsfreie Open-Source-Alternative. Tipps, Tools, Tutorials und weiterführende Informationen zum Schutz der Privatsphäre auf PC oder Telefon finden sich unter anderem bei **Rob Braxman** (https://brax.me/home/rob) oder im **Shop** (https://privacyacademy.com/privacy-shop/) der „Privacy

Academy“.

> ***Will man im Mediazän nicht Sklave seiner Geräte sein, muss man sich aktiv mit diesen Themen auseinandersetzen, seine Routinen ändern. Was auch immer man dahingehend gedenkt zu tun, man sollte es jetzt tun.***

Man muss sich diesem Netzwerk der Totalüberwachung entziehen, die Matrix verlassen, solange es noch geht. Denn die verführerische Bequemlichkeit der Observationsökonomie hat einen hohen Preis: die Freiheit. Und Smartphones sammeln längst mehr Daten über ihre Besitzer, als ein Geheimdienst es mit konventionellen Mitteln je könnte.

Tom-Oliver Regenauer, Jahrgang 1978, war nach betriebswirtschaftlicher Ausbildung in verschiedenen Branchen und Rollen tätig, unter anderem als Betriebsleiter, Unternehmens- und Management-Berater sowie internationaler Projektmanager mit Einsätzen in über 20 Ländern. Seit Mitte der 90er-Jahre ist er zudem als Musikproduzent und Texter aktiv und betreibt ein unabhängiges Plattenlabel. Der in Deutschland geborene Autor lebt seit 2009 in der Schweiz. Zuletzt erschien von ihm „Homo Demens — Texte zu Zeitenwende, Technokratie und Korporatismus“. Weitere Informationen unter **regenauer.press** (https://www.regenauer.press/).