Donnerstag, 13. Februar 2025, 15:00 Uhr
~21 Minuten Lesezeit

Private Datenkultur

Die Angriffe auf unsere digitale Selbstbestimmung häufen sich — wir sollten endlich damit anfangen, uns zu verteidigen.

von Hakeem Anwar
Foto: Patdanai/Shutterstock.com

Die Gesellschaft verlässt sich mittlerweile so sehr auf Big Tech, dass sie vergessen hat, wie man grundlegende Dinge erledigt. Wie man sich Telefonnummern merkt. Oder den Weg durch eine

fremde Stadt. Den Zugriff auf das iCloud- oder Google-Konto zu verlieren, ist, als würde man sein letztes Hemd einbüßen. Im Windschatten dieser Finten wird das Gefüge der Gesellschaft neu zugeschnitten, um sich jenen Kräften anzupassen, die von Massenüberwachung profitieren. Einschließlich unserer Regierungen. Private Datenkultur ist eine Denkweise, die das Ziel hat, so viel Privatsphäre und Kontrolle über die persönlichen Daten zu haben wie möglich. Angesichts eines immer weiter wachsenden Überwachungsstaates müssen wir dringend Verantwortung für die Technologie übernehmen, die wir nutzen — indem wir unser Nutzungsverhalten ernst- und dauerhaft den Gegebenheiten anpassen. Daher folgend eine Analyse der größten Bedrohungen für die Privatsphäre. Und ein paar Hinweise, wie man sie gegen Big Tech und Staat verteidigen kann. Übersetzt von Tom-Oliver Regenauer.

Die Deutschen lieben ihre Privatsphäre. Zumindest bisher. Als Amerikaner wünschte ich mir, die Bewohner anderer Länder hätten die gleiche Einstellung. Aber es ist klar, dass die meisten Menschen von betrügerischen Technologieunternehmen ausgetrickst wurden. Besagte Unternehmen ködern uns mit Apps, Diensten und „Annehmlichkeiten“, die wir eigentlich nicht brauchen. Die Gesellschaft verlässt sich mittlerweile so sehr auf Big Tech, dass sie vergessen hat, wie man grundlegende Dinge erledigt. Wie man sich Telefonnummern merkt. Oder den Weg durch eine fremde Stadt. Den Zugriff auf das iCloud- oder Google-Konto zu verlieren, ist, als würde man sein letztes Hemd einbüßen. Im Windschatten dieser Finten wird das Gefüge der Gesellschaft neu zugeschnitten, um sich

jenen Kräften anzupassen, die von Massenüberwachung profitieren. Einschließlich unserer Regierungen.

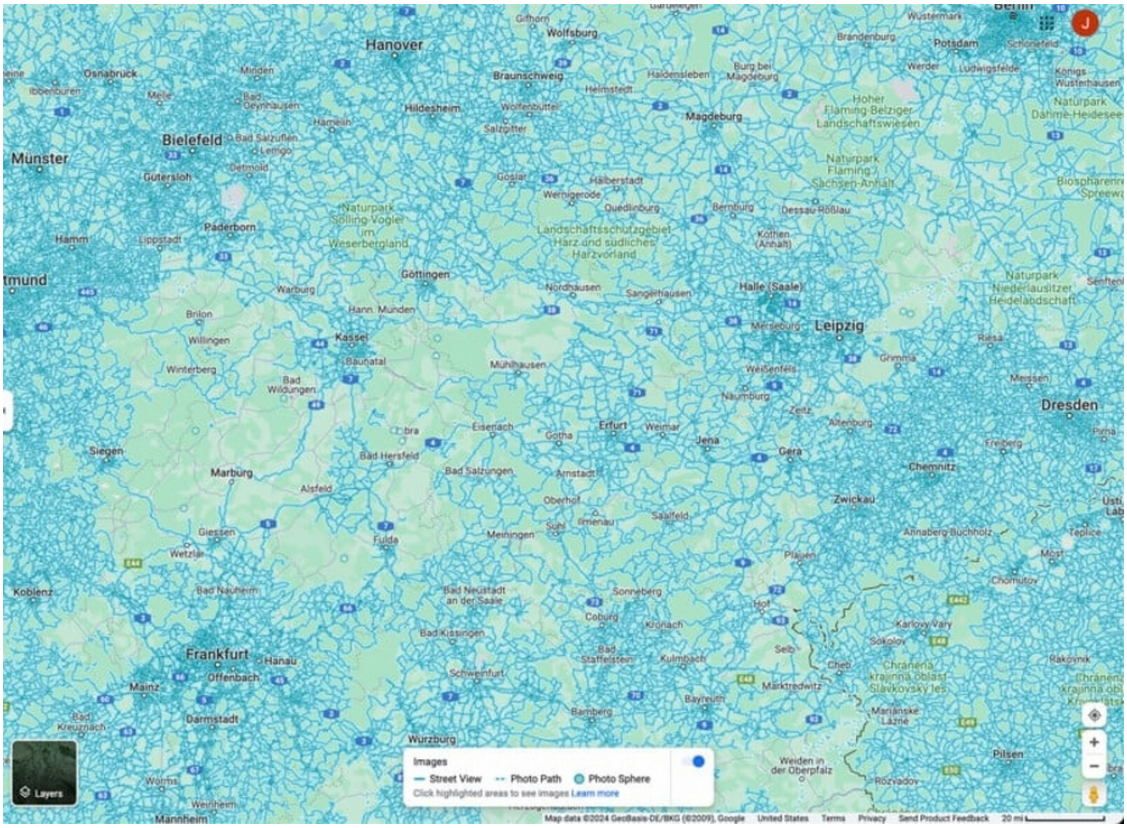
Private Datenkultur ist eine Denkweise, die das Ziel hat, so viel Privatsphäre und Kontrolle über die persönlichen Daten zu haben wie möglich. Angesichts eines immer weiter wachsenden Überwachungsstaates müssen wir dringend Verantwortung für die Technologie übernehmen, die wir nutzen — indem wir unser Nutzungsverhalten ernst- und dauerhaft den Gegebenheiten anpassen. Daher folgend eine Analyse der größten Bedrohungen für die Privatsphäre. Und ein paar Hinweise, wie man sie gegen Big Tech und Staat verteidigen kann. Werfen wir dazu zuerst einen Blick auf die Geschichte des auch in Deutschlands einstmals lauten Widerstands gegen Google Street View.

Alles ist kartografiert

Google Street View startete im Jahr 2007 und schickte ganze Fahrzeugflotten mit 360-Grad-Kameras los, um Panoramabilder von Straßen auf der ganzen Welt aufzunehmen. Diese Fahrzeuge kartografierten nicht nur Straßen und Gebäude, sondern auch WLAN-Netze. Doch Deutschland war eines der wenigen Ländern weltweit, das sich der lückenlosen Überwachung durch Google widersetzte.

Als Google 2010 ankündigte, **zwanzig** (https://www.sueddeutsche.de/wirtschaft/google-street-view-in-deutschland-20-staedte-online-1.1025313) der größten deutschen Städte kartografieren zu wollen, herrschte große Empörung. Während ein Gericht Google recht gab und das Vorgehen für legal erklärte, nahmen manche Bürger die Sache selbst in die Hand. Sie zerstörten Googles Street-View-Fahrzeuge und drohten manch einem der Fahrer. Auch wenn Gewalt natürlich grundsätzlich

abzulehnen ist, ist verständlich, warum Menschen so reagieren und zur Selbstjustiz greifen. Denn solche Kartografie-Programme sind invasiv und übergriffig. Nachdem seitens Staat und Justiz jedoch keine Unterstützung zu erwarten war und der öffentliche Aufschrei – wie so oft — bald in der Echokammer allgemeiner Bequemlichkeit verhallte, setzte Google Street View seinen Betrieb praktisch ungehindert fort. Heute ist ein Großteil des Landes kartografiert, fotografiert und virtuell zugänglich.



Geolokalisierungsdatenbanken

Eine geheime Datenbank, von der manch einer schon gehört haben mag, ist Googles **Sensorvault** (https://en.wikipedia.org/wiki/Sensorvault) — ein System, das die Standortdaten aller Benutzer von Google Maps oder anderen Google Standortdiensten in einer zentralen Geolokalisierungsdatenbank sammelt — dauerhaft.

> ***Strafverfolgungsbehörden können sogenannte Geofence-Durchsuchungsbefehle anfordern, um auf diese Daten zuzugreifen. Die Anwendung dieser speziellen Durchsuchungsbefehle hat in den vergangenen Jahren natürlich exponentiell zugenommen, da die Daten es den Behörden unglaublich einfach machen, potenzielle Verdächtige zu finden.***

Dazu müssen sie lediglich ein bestimmtes Datum oder eine bestimmte Uhrzeit sowie einen Bereich auf der Karte angeben — schon erhalten sie Daten zu allen Telefonen, die Googles Standortdienste in diesem Bereich nutzten und nutzen.

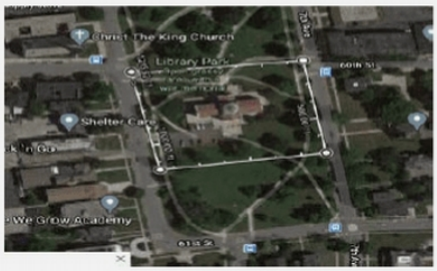
Als dieses Vorgehen von der ***New York Times*** *(https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html?partner=rss&emc=rss)* aufgedeckt wurde, sorgte dies für massive Empörung. Google revidierte daraufhin seine Standortverlaufsrichtlinien und behauptete, dass der Standortverlauf von Google Maps fortan und standardmäßig nur noch auf dem Gerät verbleibe. Es ist zum heutigen Zeitpunkt unklar, ob Sensorvault noch existiert, Google solchen Anfragen von Behörden noch nachkommt und welche Standortdaten Google über seine Location Services überhaupt sammelt. Anzunehmen, das Unternehmen hätte das Datensammeln tatsächlich eingestellt, erscheint allerdings reichlich naiv.

Allein im Jahr 2020 erhielt Google 11.554 Anfragen für Geofence-Haftbefehle. Andere Unternehmen wie Apple, Snapchat, Lyft und Uber, die ebenfalls Geolokalisierungsdaten verwalten, erhalten natürlich auch Geofence-Haftbefehle von den Strafverfolgungsbehörden — auch wenn die Behörden davon ausgehen müssen, dass im Gegensatz zu Sensorvault nur minimale Datenmengen verfügbar sind. Fakt ist: Jede App, die Zugriff auf Geolokalisierung hat, kann eine Karte der historischen Bewegungen erstellen. Daher sollte man sehr vorsichtig sein, wem man seine Geolokalisierungsdaten anvertraut.

(2) identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

- Date: August 25, 2020
- Time Period: 01:00 AM to 03:00 AM (CST)
- Target Location: Geographical area identified as:
  42.580802, -87.820086; 42.580940, -87.818942;
  42.580243, -87.818733; 42.580146, -87.819945
  Also approximately depicted using the following image:

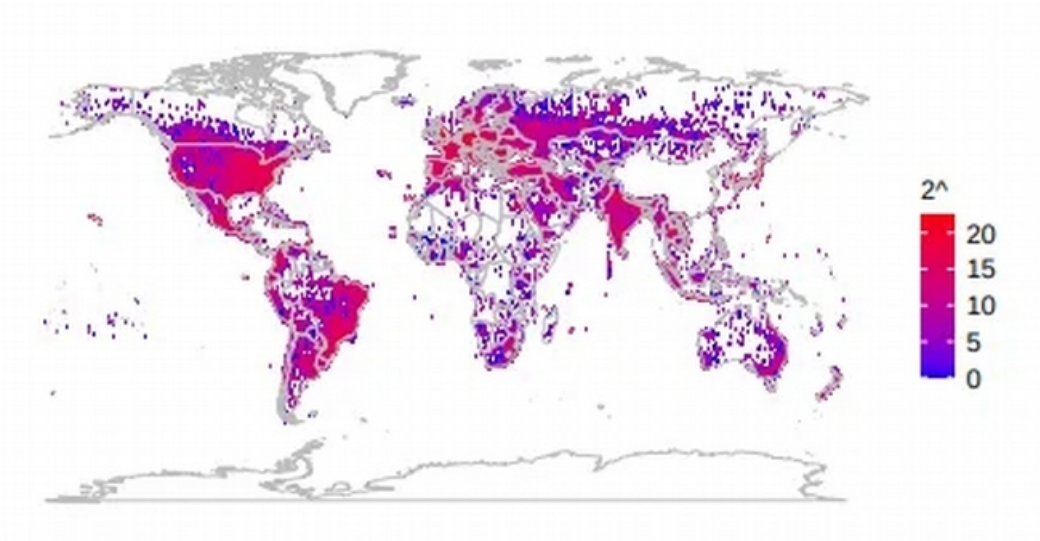


Google is further ordered to disclose the above information to the Government within 10 days of the issuance of this warrant.

WLAN-Überwachung

Haben Sie sich jemals gefragt, woher Google und Apple so genaue Daten über Ihre Position haben? Jedes dieser Unternehmen kann Ihren physischen Standort jederzeit bis auf sechs Meter genau feststellen, weil sie WLAN-Positionierungssysteme (WPS) entwickelt haben, die die Standorte nahegelegener WLAN-Netzwerke verwenden. Das bedeutet natürlich, dass Google und Apple die

Daten sehr vieler WLAN-Netzwerke sammeln mussten. Wie viele Netzwerke das sind? Forschern an der Universität von Maryland **gelang** (https://www.security-insider.de/apple-wps-datenschutzprobleme-forscher-decken-risiken-auf-a-cf3d8671dd2896d3ccd7c823f823ab87/) es, Apples WPS-System zu verwenden, um sich ein Bild von der tatsächlichen Anzahl zu machen. Als die Wissenschaftler ihren eigenen Standort auf Apples WPS-Datenbank abfragten, antwortete diese mit 400 nahegelegenen WiFi-Netzwerken und deren genauen Standorten. Nach wiederholten Standortabfragen — basierend auf fingierten und jeweils unterschiedlichen Positionen — sammelten sie schockierende zwei Milliarden WiFi-Netzwerke und deren Standorte. Diese Anzahl genügt, um jedes bewohnte Gebiet auf dem Planeten nahezu lückenlose zu kartografieren.



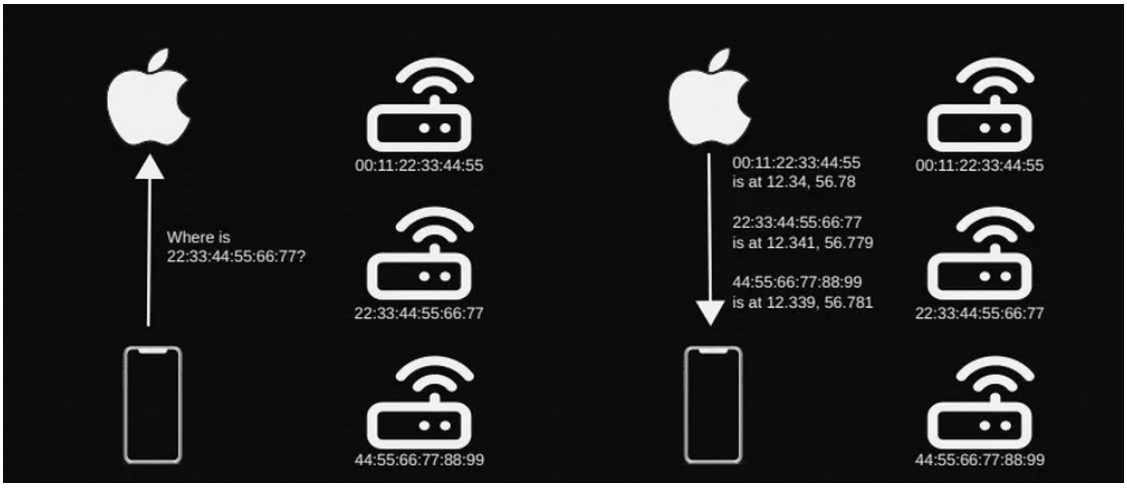
> ***Durch die Überwachung dieses Systems in verschiedenen Gebieten und über vordefinierte Zeiträume war es den Forschern aus Maryland möglich, Soldaten aufzuspüren, die vor der Mobilisierung in der Ukraine oder der Zerstörung im Gazastreifen geflohen waren — nur durch Veränderungen der aufgezeichneten Bewegungsmuster in aktiven WLAN-Netzwerken.***

Natürlich ist nicht nur Apple auf diesem Gebiet aktiv. Auch Google sammelt WLAN-Netzwerke, seit Google Street View mit Daten

gefüttert wird. Sprich, seit 2007.

Zusätzlich zu den automatisch erfassbaren Daten verlässt sich dieses Überwachungsnetzwerk auf Datensätze, die Smartphone-Nutzer unwissentlich und permanent zur Verfügung stellen. Sendet ein Smartphone seinen Standort an Google oder Apple, überträgt es gleichzeitig alle in der näheren Umgebung verfügbaren WLAN-Netzwerkkennungen an die Cloud – inklusive deren Signalstärke. Anschließend verwendet das WPS diese Netzwerk- und Signaldaten, um den endgültigen Standort einer Person zu identifizieren. Auf diese Weise erstellen und aktualisieren die Unternehmen eine riesige Datenbank mit WLAN-Zugangspunkten, die mit jeder Standortanfrage aktualisiert wird.

Mit dieser Datenbank kann der Standort von Einzelpersonen, Gruppen, Gebäuden und allen Entitäten ermittelt werden, die im Lauf der Zeit und auf der ganzen Welt mit einem WLAN-Netzwerk verbunden waren oder sind. Ironischerweise schlägt Apple selbst vor, die Endung „_nomap“ am Ende der häuslichen WLAN-Kennung anzuhängen, um zu vermeiden, dass diese in der Datenbank des Konzerns auftauchen — was natürlich dazu führt, dass solch gut informierte Widerständler in Netzwerkkarten auffallen.



Das Grundproblem rührt daher, dass die meisten WLAN-Netzwerke permanente Kennungen haben, die als BSSIDs (Basic Service Set Identifier) bezeichnet werden. Apple- und Google-Telefone

verwenden dieses WLAN-Positionierungssystem natürlich. Tatsächlich ist es aber die Standardmethode, um Geolokalisierung innerhalb einer lokalisierbaren App zu verwenden.

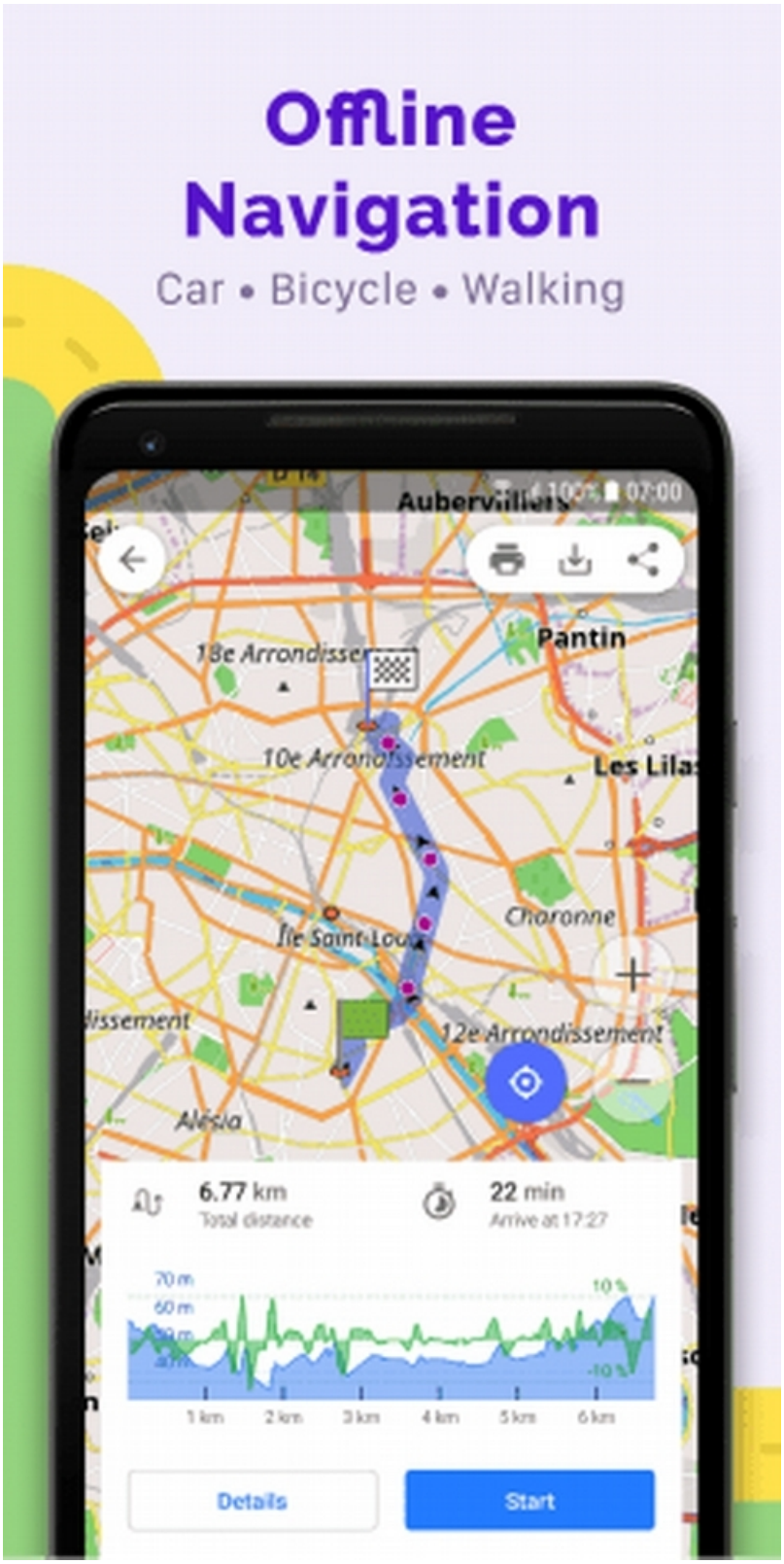
> ***Die einzige Möglichkeit, nicht Teil dieses Überwachungsnetzwerks zu sein, besteht darin, ein Telefon ohne Standortdienste von Google oder Apple zu verwenden. Und das geht derzeit nur mit einem Telefon, das auf Google-Dienste gänzlich verzichtet.***

Standortdiensten ein Schnippchen schlagen

Man stelle sich vor, es gäbe eine Karte aller lokal relevanten Punkte, die nicht nur die hiesigen Sehenswürdigkeiten, Restaurants oder Geschäfte enthält, sondern auch die Lieblingsplätze der besten Freunde, die eigenen Laufrouten oder Gebiete, in denen man gern Pilze sammelt und wandern geht. Eine Karte also, die man selbst gestalten kann. Ohne Abhängigkeit von Dritten. Genau das bietet die Kartenplattform **OpenStreetMaps** (https://www.openstreetmap.org/#map=8/46.825/8.224), die kostenlos als Open-Source-Lösung am PC und für Android-basierende mobile Betriebssysteme verwendet werden kann.

OpenStreetMaps ist ein von der weltweiten Nutzergemeinschaft betriebenes Kartenprojekt, das Daten für Karten und Sehenswürdigkeiten per Crowd-Sourcing sammelt. Jeder kann mithilfe einer App auf dem Telefon und am Computer dazu beitragen und kostenfrei über die Dienste verfügen. **OsmAnd** (https://osmand.net/) ist eine mobile Navigations-App, die OpenStreetMaps-Kartendaten verwendet und es Benutzern ermöglicht, Kartenabschnitte oder ganze Länder direkt auf das Telefon herunterzuladen. Sobald die Karten lokal auf dem Telefon gespeichert sind, ist keine Verbindung zum Internet mehr

erforderlich, um zwischen zwei Punkten zu navigieren. Das macht OsmAnd zu einer perfekten App, wenn kein Internetzugang verfügbar ist oder man sich dem überstaatlichen Überwachungsregime nicht bei jeder Routenplanung freiwillig offenbaren möchte.



Wenn sich immer mehr Menschen entscheiden, diesen Weg zu

gehen, anstatt Big Tech mit Nutzerdaten zu füttern, wären die OpenStreetMap-Karten in kürzester Zeit genauso aussagefähig wie die Datenkraken von Google oder Apple. Mit wachsender Nutzerzahl wächst der Nutzen solcher Lösungen. Individuelle Karten könnten schon bald all die Informationen enthalten, die für den Leser und sein persönliches Umfeld relevant sind und dann sogar im .GPX-Format exportiert und mit Menschen geteilt werden, denen man vertraut.

Ein weiteres Werkzeug, das von OpenStreetMaps unterstützt wird, ist **FacilMaps** (https://facilmap.org/#11/47.3682/8.5671/Lima) — eine Anwendung, die den kollaborativen Kartierungsprozess signifikant vereinfacht. Denn FacilMaps erlaubt es, Karten zu erstellen, die man gemeinsam mit anderen gestaltet beziehungsweise befüllt. Das ist nicht nur für Familien, Vereine oder Unternehmen nützlich, sondern auch für die Bürgerrechtsbewegung. Wir zum Beispiel haben FacilMaps verwendet, um Watch-Partys für unser lösungsorientiertes Event **The People's Reset** (https://thegreaterreset.org/) international zu teilen. Applikationen wie OsmAnd oder FacilMaps findet man übrigens in einem Open-Source-App-Store namens **F-Droid** (https://f-droid.org/en/).

Der Big-Tech-Computer ist kein Freund

Wer in den Laden geht und einen Computer kaufen möchte, hat zwei Möglichkeiten: Microsofts Windows oder Apples macOS. Und beide Betriebssysteme sind eine Zumutung in puncto Datenschutz und Privatsphäre. Denn diese Systeme sind proprietär, was bedeutet, dass ihr Code nicht öffentlich zugänglich ist. Das bedeutet auch, dass es schwierig ist, Konzernangaben hinsichtlich der Privatsphäre dieser Systeme zu überprüfen. Marketing- und Werbeslogans haben in der Regel wenig mit der Realität zu tun.

Denn auch wenn es bei beiden Systemen anpassbare Datenschutzeinstellungen gibt, sind hinter den Kulissen zusätzliche Tracking-Mechanismen am Werk.

Sowohl Microsoft als auch Apple tauchen im **PRISM** (https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data)-Programm auf, von dem die Welt durch den ehemaligen NSA-Mitarbeiter Edward Snowden erfuhr. Eine durchgesickerte Präsentation deutete darauf hin, dass die National Security Agency (NSA, Auslandsnachrichtendienst der USA) Daten direkt von diesen und anderen großen Technologieunternehmen bezieht. Während PRISM ein geheimes Programm ist, geben die beiden Unternehmen natürlich auch freiwillig Daten an Strafverfolgungsbehörden weiter. Sogar ohne Gerichtsbeschluss. Laut Apples Transparenzbericht für Deutschland gingen von Januar bis Juni 2023 10.113 Geräteanfragen von der Regierung ein. Dabei wurden Gerätekennungen wie die IMEI- oder Seriennummer angefordert. Apple stellte die Daten in 64 Prozent der Fälle zur Verfügung. Gemäß Microsofts Transparenzbericht erhielt das Unternehmen aus Deutschland 27.242 Anfragen zu Verbraucherdaten für Microsoft-Dienste. Davon wurden 63,5 Prozent bedient.

Telemetrie in Windows 11

Im Jahr 2023 kam heraus, dass Windows 11 Verbindungen zu mehreren Drittanbietern herstellt, wenn der Computer eingeschaltet wird. Der YouTube-Kanal TPCSC verwendete einen Netzwerkverkehrsanalysator, um festzustellen, dass Windows 11 unter anderem Konnektivität zu Onlinediensten wie MSN, Bing, Steam (einer Spieleplattform), McAfee (AntiVirus) und ScorecardResearch herstellte — ein riesiger Daten-Aggregator für Drittanbieter, der Benutzer über ihre verschiedenen Geräte und das

Internet hinweg verfolgt. Dabei ist zu beachten, dass dies geschieht, sobald der Computer eingeschaltet wird. Ganz ohne dass der Benutzer irgendetwas damit gemacht hätte. Es bedarf wenig Fantasie, um sich vorzustellen, wie umfangreich die Telemetrie bei der Benutzung von Windows- oder Apple-Rechnern ist.

Einer der ärgerlichsten Aspekte bei der Verwendung von Windows-Computern sind die erzwungenen Updates. Zum Leidwesen aller zwingt Microsoft seine Benutzer, Software-Updates zu installieren — selbst wenn das Arbeitsprozesse unterbricht, ein Spieleprogramm läuft oder eine Live-Präsentation vor Hunderten von Menschen stattfindet. Sprich, der Computer wird neu gestartet und ist nicht einsatzbereit, bis die Updates installiert sind. Und das kann manchmal ziemlich lange dauern.

> ***Wer einen Windows-Computer verwendet, hat letztlich keine Kontrolle darüber, was das Gerät macht. Und schon das nächste Update könnte wieder neue obligatorische Überwachungswerkzeuge ausliefern, denen man sich nicht verweigern kann.***

Windows Recall

2024 kündigte Microsoft eine neue Funktion namens **Recall** (https://www.ndtv.com/feature/microsofts-new-recall-feature-sparks-spying-concerns-elon-musk-links-it-to-black-mirror-5710761) an, die alle paar Sekunden Schnappschüsse des Bildschirms macht und mithilfe von künstlicher Intelligenz (KI) eine Textzusammenfassung der Aktivitäten erstellt. Das soll dem Nutzer nach **Angaben** (https://support.microsoft.com/en-us/windows/retrace-your-steps-with-recall-aa03f8a0-a78b-4b3e-b0a1-2eb8ac48701c) des Konzerns ermöglichen, in der Zeit zurückzureisen und nach etwas zu suchen. Microsofts Planung sah vor, diese Funktion einzuführen, ohne dass sie abgeschaltet werden

kann. Doch als das Vorgehen öffentlich wurde, wies ein Sicherheitsingenieur darauf hin, dass alle Zusammenfassungen der Benutzeraktivitäten ohne jegliche Verschlüsselung auf der Festplatte gespeichert sind. Das bedeutet, dass Angreifer im Falle eines Hacks über den gesamten Nutzungsverlauf des Besitzers verfügen könnten. Glaubt man Microsoft, sind diese Zusammenfassungen nur lokal gespeichert und werden nicht an die Cloud des Unternehmens übertragen. Aber sind solche Versprechen vertrauenswürdig?

Die Recall-Funktion wurde den Benutzern ohne grundlegenden Datenschutz aufgezwungen. Erst nachdem der Gegenwind zu heftig wurde, gab Microsoft nach und machte Recall zu einer Opt-in-Funktion. Dennoch ist die Situation aufschlussreich, wenn es um die Prioritäten von Microsoft geht. Zusätzlich zu Recall verfügen Microsoft-Computer über eine Aktivitätsverlaufskomponente, die den Verlauf standardmäßig an Microsoft sendet. Dies ist nur eine von vielen Windows-Funktionen, die dem Anspruch auf Schutz der persönlichen Daten diametral entgegenstehen.

Apple scannt Fotos

Vor gut vier Jahren wies der Sicherheitsforscher Jeffrey Paul nach, dass macOS alle lokal gespeicherten Fotos automatisch scannt. Dies geschieht, ohne den Benutzer darüber zu nachrichtigen. Oder dessen Einverständnis. Selbst dann, wenn der Computer nicht mit der iCloud gekoppelt ist und die Apple-Foto-App nicht verwendet wird. Paul zeigte außerdem, dass Apple jedes auf dem Heimcomputer laufende Programm protokolliert und die Nutzungsdaten unverschlüsselt über das Internet an die Cloud des Konzerns überträgt. Das bedeutet, dass Apple weiß, wann jemand zu Hause und wann jemand bei der Arbeit oder auf Reisen ist. Apple weiß, welche Apps man bei der Arbeit öffnet und wie oft. Apple

weiß, wann welche Software bei wem und in welchem WLAN-Netzwerk verwendet wird. Und Apple weiß auch, wenn man auf einer Reise in einer anderen Stadt den Tor-Browser in einem Hotel nutzt. Apple weiß alles. Da diese Daten offen und ohne Verschlüsselung über das Internet übertragen werden, sind die betreffenden Informationen für jeden verfügbar, der Zugriff auf das Netzwerk hat — beispielsweise einen Internetdienstanbieter oder den Staat.

Die Lösung: Verwendung eines freien Betriebssystems. Für jeden, der seine Privatsphäre und Freiheit schätzt, ist die Wahl klar. Das Linux-Betriebssystem ist die beste Option. Zig Millionen von Anwendern arbeiten bereits mit Linux und bringen die Mainstream-Monopole damit in Bedrängnis. Linux ist eine Gemeinschaftsentwicklung. Anstatt von einem Unternehmen proprietär aufgesetzt zu werden, wurde das System offen entwickelt, indem der **Linux-Kernel** (https://www.redhat.com/de/topics/linux/what-is-the-linux-kernel) des Entwicklers **Linus Torvalds** (https://de.wikipedia.org/wiki/Linus_Torvalds) mit dem Betriebssystemcode des **GNU-Projekts** (https://www.gnu.org/home.en.html) kombiniert wurde. Beide Komponenten sind Open Source, was bedeutet, dass sie von jedem untersucht, geändert und geteilt werden können. Dies führte zur Entstehung verschiedener Arten von Linux-Betriebssystemen, aus denen man heutzutage wählen kann. Diese Betriebssysteme können auf den meisten Geräten problemlos betrieben werden. Ausnahme: Apple-Computer neueren Datums. Linux-Systeme unterstützen alle grundlegenden Hardwarefunktionen, die Computerbenutzer erwarten und benötigen.

Die Unterstützung für Linux-Software hat große Fortschritte gemacht. Waren früher viele Programme, die auf herkömmlichen Rechnern liefen, nicht kompatibel, wird mittlerweile die überwiegende Mehrheit der Apps unterstützt. Darunter zum

Beispiel auch Mainstream-Apps wie Zoom oder Spotify — von deren Verwendung ich allerdings grundsätzlich abrate. Die Installation von Linux mittels eines USB-Laufwerks ist relativ einfach. Man sollte allerdings nicht vergessen, dass die Installation alle Daten des alten Systems löscht – außer man betreibt Linux in einer **virtuellen Maschine** (https://www.computerwoche.de/article/2859321/fuenf-beliebte-virtualisierer-fuer-linux-im-vergleich-2.html) auf dem bestehenden System. Für den allgemeinen Anwender empfehlen sich unter anderem Linux-basierte Betriebssysteme wie **PopOS** (https://pop.system76.com/), **Linux Mint** (https://linuxmint.com/) oder **KDE Neon** (https://neon.kde.org/). Auf meiner Homepage habe ich diesbezüglich ein paar weiterführende Informationen zusammengestellt.

Aus der Not eine Tugend machen

Als Datenschützer und **Aktivist** (https://thegreaterreset.org/speakers/hakeem-anwar/) war es mir ein Anliegen, mich nicht nur über Probleme zu beschweren, sondern auch Lösungen dafür zu entwickeln. So entstand vor ein paar Jahren aus persönlicher Motivation, Fachwissen und den Zuwendungen von Freunden meine Firma **Above** (http://www.abovephone.com/). Heute entwickelt und konfiguriert unser kleines Team Laptops, Smartphones und Software — Produkte, die Datenschutz in den Fokus stellen und deshalb von vielen namenhaften Investigativjournalisten verwendet werden. Unser **Privacy Laptop** (https://abovephone.com/book/) arbeitet mit AboveOS, einem von uns entwickelten Betriebssystem, das auf einer erweiterten Version von Linux namens **Arch Linux** (https://archlinux.org/) basiert. Wir haben das System bewusst so konzipiert, dass es zeitgemäß, aber benutzerfreundlich ist. Denn nicht wenige Computernutzer haben Angst, ihre gewohnte Arbeitsumgebung zu verändern. Obwohl die Argumente klar gegen

die weitere Verwendung proprietärer Betriebssysteme wie Windows und macOS sprechen. Denn wer mit diesen Systemen arbeitet, besitzt seinen Computer nicht wirklich, sondern gehört Big Tech. Mitsamt all seiner Daten.

Der Taschenspion

Die Wahrung der Privatsphäre auf dem Smartphone erscheint sogar noch wichtiger als der Schutz der Daten auf dem Computer. Denn der steht meist zu Hause — während Telefone uns begleiten, wenn wir bei der Arbeit, bei Freunden oder auf Reisen sind. Sie hören, sehen und wissen alles. Ein Smartphone ist ein Mobilfunkgerät, das mit GPS, einer Kamera, einem Mikrofon und unzähligen Sensoren ausgestattet ist. Und es gibt mehr als sieben Milliarden Geräte weltweit — also nahezu eines pro Person. Schockierende 98 Prozent dieser Smartphones laufen auf einem von nur zwei Betriebssystemen: Android (Google) oder iOS (Apple). Die Datenmengen, über die diese beiden Unternehmen verfügen, ist unvorstellbar. Es ist nicht übertrieben zu behaupten, dass die Konzerne ihre Kunden besser kennen als diese sich selbst. Dabei sollte man aufgrund ihrer unrühmlichen Historie gerade diesen beiden Unternehmen keinerlei Daten anvertrauen.

Das Tracking auf Smartphones kann in drei Ebenen unterteilt werden: Betriebssystem, Apps und Telekommunikation. Durch eine unabhängige **Studie** (https://irishtechnews.ie/trinity-study-privacy-concerns-about-apple-google/) von Forschern am Trinity College in Irland wurde festgestellt, dass sich Google- und Apple-Telefone durchschnittlich alle fünf Minuten mit „Zuhause“ verbinden. Dabei senden sie eindeutige Gerätekennungen wie die IMEI-Nummer (Mobile Equipment ID), IMSI (Mobile Subscriber Identity) und Werbe-IDs. All das kann verwendet werden, um einer Person digital zu folgen. Selbst wenn sich deren Geräte oder

Nummern ändern. Die Werbe-IDs werden darüber hinaus genutzt, um Personen über verschiedene Geräte hinweg zu identifizieren und ihnen beim Surfen im Internet oder bei der Nutzung sozialer Medien synchronisierte Werbeinhalte aufzudrängen.

Die Studie aus Irland wies nach, dass es für den Benutzer absolut keine Möglichkeit gibt, auf diese im Hintergrund laufenden Prozesse Einfluss zu nehmen. Die wenigen Datenschutzeinstellungen, die auf den Geräten angeboten werden, wirken sich kaum auf dessen Tracking-Funktionen aus. Das bereits erwähnte Problem mit proprietärer Technologie: Niemand kann sagen, was im Inneren der Geräte wirklich vor sich geht. Schlimmer noch: Die zentralisierten Softwaredienste, die auf jedem Big-Tech-Telefon installiert sind, können durch Käufe im App Store und Integrationen mit dem Betriebssystem leicht mit der Identität des Benutzers verknüpft werden. Verschiedene Kernfunktionen des Telefons, ob Telefonbuch oder Tastatur, generieren Protokolle, die auch an Google und Apple zurückgesendet werden.

Eine andere Studie, die von mehreren Hochschulen gemeinsam durchgeführt wurde, analysierte das Ausmaß des Trackings über Mainstream-Apps, die der durchschnittliche Nutzer herunterlädt. Dabei konzentrierten sich die Forscher auf das Google-Ökosystem und den Google Play Store. Jede App auf Google Play, also Programme, die in der Regel weit über eine Million Mal heruntergeladen werden, enthielt durchschnittlich fünf Tracking-Programme. Diese Tracker sind Codepakete der Analyse- oder Werbeunternehmen von Drittanbietern, die von den Entwicklern der Apps in deren Software integriert werden.

Das Problem ist also, dass all diese Unternehmen Zugriff die detaillierten Nutzungsdaten jeder Person haben. Wenn einer beliebigen App aus dem Play Store Berechtigungen erteilt werden, zum Beispiel der Zugriff auf das Telefonbuch, verfügen besagte Tracker ebenfalls über diese Berechtigungen. Ohne dass der

Besitzer des Telefons etwas davon weiß. Natürlich bleibt auch hier im Dunkeln, was genau in den an Dritte übermittelten Nutzerprotokollen steht, weil sowohl der Code für die Apps im Google Play Store als auch der Code für die Tracker proprietär und damit nicht nachprüfbar ist. Gemäß Branchenanalysten besitzt Alphabet, Googles Muttergesellschaft, sechzehn der zwanzig größten Analyse- und Werbeunternehmen. Den Rest kann man sich denken.

Funknetzanbieter sind auch keine Freunde

Die dritte Ebene des Smartphone-Trackings erfolgt über die Mobilfunkinfrastruktur. Auch wenn die im Rahmen des Artikels erwähnten Analysen und Gesetze primär die Verhältnisse in den Vereinigten Staaten ins Auge fassen, sei an dieser Stelle darauf hingewiesen, dass die Mobilfunkinfrastruktur auf der ganzen Welt praktisch die gleiche ist. Sprich, in Deutschland und Europa ist man mit den gleichen Problemen hinsichtlich Privatsphäre und Datenschutz konfrontiert.

Was bedeutet das? Nehmen wir **CALEA** (https://ndcac.fbi.gov/calea) 1994 (Communications Assistance in Law Enforcement Act), ein US-Bundesgesetz, das alle Telekommunikationsanbieter verpflichtete, Daten bei Bedarf für Ermittlungen herauszugeben. Ergebnis: Keine über das Mobilfunknetz gesendete Kommunikation ist jemals wirklich privat.

> ***Jeder einzelne Telefonanruf und jede einzelne Textnachricht ist für den Mobilfunkbetreiber und damit auch alle Organisationen sichtbar ist, mit denen dieser zusammenarbeitet.***

Telekommunikationsunternehmen speichern „Anrufdatensätze“, die einen Telefonanruf, eine SMS und sogar eine Datensitzung beschreiben können. Dazu gehören Zeitstempel, der Sendemast, dem der Telefonbenutzer am nächsten ist, Absender- und Empfängerrufnummern et cetera. Diese Anrufdatensätze werden den Strafverfolgungsbehörden oder Geheimdiensten zur Verfügung gestellt, sobald diese im Rahmen von Ermittlungen eine gerichtliche Genehmigung vorlegen. Oft genug wahrscheinlich auch ohne dieses Prozedere. Das haben uns die Erfahrungen der Vergangenheit gelehrt. Denn alle Telekommunikationsunternehmen haben dezidierte Teams, die sich ausschließlich mit der Erfüllung dieser Anfragen befassen.

In den Vereinigten Staaten arbeitete zum Beispiel AT&T mit der NSA zusammen, um die Überwachung der Mobilfunkkommunikation zu optimieren. In Zusammenarbeit mit der Drug Enforcement Agency (DEA, Drogenbekämpfungsbehörde) entwickelte AT&T das Projekt **HEMISPHERE** (https://www.eff.org/cases/hemisphere), das seit 2008 jährlich vierzig Milliarden Anrufdetails sammelte. Diese Daten konnten durchsucht und verknüpft werden, um Drogendealer zu finden, die Geräte neueren Datums mieden und sich stattdessen sogenannte Burner Phones (Wegwerftelefone) zulegten.

> ***Wer seine Privatsphäre auf dem Smartphone schützen möchte, muss einen ganzheitlichen Ansatz verfolgen. Das funktioniert am besten mit einem Gerät, das den Mainstream-Optionen in nichts nachsteht und dem Nutzer alle Funktionen bietet, die er auch zuvor hatte.***

Google-freie Betriebssysteme bauen auf der Open-Source-Grundlage des Android-Betriebssystems von Google auf. Die Entwickler entfernen die Spionagewerkzeuge von Google und fügen dafür eigene Funktionen hinzu. Vor allem im Bereich Datenschutz.

GrapheneOS (https://grapheneos.org/) ist ein solches

Betriebssystem. Das entsprechende Entwicklerteam hat hervorragende Arbeit beim Aufsetzen eines sicheren und privaten Systems geleistet. Denn es bietet Benutzern neben Hoheit über die eigenen Daten und ihre Kommunikation sogar Funktionen, die auf einem Mainstream-Telefon gar nicht verfügbar sind. Aus diesem Grund habe auch ich mich vor ein paar Jahren dazu entschieden, GrapheneOS zur Grundlage meiner eigenen Entwicklungen zu machen. So entstand das Above Phone. Ein Gerät, das auch für Laien ohne zusätzliche Kenntnisse sofort einsatzbereit ist und einen extrem hohen Sicherheitsstandard bietet. Inklusive aller Apps, die man von einem Smartphone erwartet — nur eben Open Source. Ohne Überwachung.

GrapheneOS stellt standardmäßig keinerlei Verbindungen zu Google her. Es werden keine Daten an irgendeine Cloud übertragen. Das haben wir selbst noch einmal überprüft, als wir auf dieser Basis unser AboveOS-Betriebssystem entwickelt haben. Das bedeutet, dass es weder Werbung noch neugierige Standortdienste und WLAN-Tracking gibt. Stattdessen aber eine permanente VPN-Verbindung, die die eigene Identität schützt. Wer unbedingt auf Big-Tech-Dienste zugreifen muss, zum Beispiel für die Arbeit, kann diese auf einem isolierten Profil installieren, das von Rest des Smartphones abgeschirmt ist. Das ist weitaus sicherer als die Verwendung von Outlook, Google Maps oder Spotify auf einem herkömmlichen Gerät. Denn als Nutzer hat man vollständige Kontrolle über alle Funktionen des Betriebssystems.

GrapheneOS bietet erweiterte Berechtigungen, die es erlauben, Apps den Zugriff auf Internet, Kontakte oder Fotos zu verwehren beziehungsweise diese im Einzelfall zu steuern. Weiterhin bietet das System „Kill Switches“, also globale Schalter für Mikrofon, Standort und Kamera, die die betreffenden Funktionen auf Ebene des Betriebssystems, und damit verlässlich, deaktivieren. Installiert man Big-Tech-Apps, können diese in hermetisch abgeschirmten „Sandboxes“ betrieben und damit von den Nutzerdaten getrennt

werden.

Über Kataloge wie F-Droid lassen sich alle benötigten Apps anonym herunterladen. Open Source, was bedeutet, dass der Quellcode transparent ist. Und kostenlos. Die Applikationen aus diesem Store haben keine versteckten Tracker — und in vielen Fällen können sie verwendet werden, ohne sich mit dem Internet verbinden zu müssen. Wer dennoch Big-Tech-Programme wie WhatsApp benötigt, kann diese anonym über den **Aurora** (https://discuss.grapheneos.org/d/4109-how-do-i-get-the-aurora-store)-Katalog beziehen und auf einem isolierten Profil installieren.

Darüber hinaus würde ich Menschen, die Wert auf Datenschutz legen, empfehlen, auf internetbasierte Kommunikation anstelle von normalen Telefonanrufen und Textnachrichten umzusteigen. Internetbasierte Kommunikation kann Ende-zu-Ende-verschlüsselt werden. Meint, dass der Mobilfunkanbieter die Inhalte weder sehen noch aufzeichnen kann. Zusätzlich kann der eigene Internetverkehr mit einem VPN verschlüsselt werden. Dieses Vorgehen bietet deutlich mehr Privatsphäre als die offiziellen Lösungen.

Über den Dingen stehen

Wer die im Rahmen dieses Textes zusammengestellten Informationen hilfreich fand, ist vielleicht auch bereit, selbst aktiv zu werden und sich dem permanenten Überwachungsapparat zu entziehen — und deshalb herzlich eingeladen, sich auf meiner **Webseite** (https://takebackourtech.org/) umzuschauen, wo ich regelmäßig Artikel und kostenlose Webinare zum Thema Kommunikationstechnologie veröffentliche.

Auch über einen Besuch auf unserer **Above Webseite**

(https://abovephone.com/manova) würde ich mich freuen, denn mein Team und ich entwickeln Lösungen, die nicht nur Journalisten und Aktivisten, sondern jedem freiheitsliebenden Menschen helfen, sich vor einem immer aggressiver handelnden System zu schützen. Wir bieten diese Lösungen nicht an, um damit reich, sondern um mit allen gemeinsam freier zu werden.

Ob Smartphones, Laptops oder Software — Kommunikationswerkzeuge sind einer der Bereiche im Leben, die mit wenig Aufwand den eigenen Sicherheitsbedürfnissen angepasst werden können. Man muss es nur tun. Und wenn ich bei diesem Schritt ein wenig helfen kann, freue ich mich darüber. Denn bisher hat ihn noch niemand bereut.

Für Fragen, Anregungen oder Feedback zu diesem Text stehe ich jederzeit gerne über das **Kontaktformular** (https://takebackourtech.org/connect/) auf meiner Webseite oder die Kontaktinformationen der **Above Agency** (https://abovephone.com/support/) zur Verfügung.

Hakeem Anwar ist Softwareentwickler, Bürgerrechtsaktivist und Unternehmer. Er lebt in den Vereinigten Staaten. Seit 2020 engagiert er sich für die freiheitliche Bewegung, Datenschutz und einen offenen Debattenraum. Mit seinen Entwicklungen im Bereich der Open-Source-Kommunikationstechnologie unterstützt er eine Vielzahl renommierter Investigativjournalisten. Darüber hinaus ist er ein gefragter Redner bei internationalen Veranstaltungen in den Bereichen IT-Sicherheit, Krypto und Agorismus.