Ein Medienverbund enthüllt, wie dubiose Geschäftemacher riesige Datensammlungen über arglose Bürger feilbieten und die Werbeindustrie dankbar zugreift. Den Stoff liefern ihnen Entwickler von Apps, mit denen sich Handynutzer mithin punktgenau lokalisieren lassen – etwa solche, die den nächsten Schneeschauer nicht abwarten können. Interessant kann das auch für andere Akteure sein: Polizei, Geheimdienste, Militärs, Stalker, Erpresser. Die Liste ließe sich fortführen – lieber nicht. Von **Ralf Wurzbacher**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/250120-Digitaler-Wetteronkel-NDS.mp3

Podcast: Play in new window | Download

Du hast Dich im Wald verlaufen und findest nicht mehr raus? Kein Ding: Deine Wetter-App weiß genau Bescheid, wo du bist. Und hat es auch schon weitererzählt: dem Online-Outdoorshop, dem Verlag für Wanderführer, der Datingplattform, vielleicht ja der US-Armee oder dem BND, mitunter dem Triebtäter, der Dir seit Wochen nachstellt. Willkommen im digitalen Märchenland, das leider viel zu wahr ist, um schön zu sein. Es sind verstörende Erkenntnisse, die ein Rechercheverbund aus *Netzpolitik.org*, dem *Bayerischen Rundfunk (BR)* und fünf Medienpartnern aus Norwegen, Schweden, der Schweiz, den Niederlanden und den USA am Mittwoch der Vorwoche publik gemacht hat.

Ihnen wurde ein riesiger Datensatz zugespielt, dessen Auswertung offenbart: Abermillionen arglose Nutzer von Smartphones sind alltäglich einer umfassenden Massenüberwachung ausgeliefert. Vornehmlich Werbetreibende folgen ihnen buchstäblich auf Schritt und Tritt. Auch Fahnder, Geheimdienste und Kriminelle können ihre Spur aufnehmen. Aber Gesetze und Regeln greifen bei dem schlimmen Treiben ins Leere, selbst Beteiligte blicken nicht durch, wo die Grenzen zwischen legal und illegal verlaufen. Datenschützer warnen vor einem „enormen Kontrollverlust“.

Schnappschuss von Zigmillionen

Das fragliche Material haben die Journalisten von einem Datenbroker erhalten. Davon gebe es weltweit Tausende, die zusammen ein „schier undurchschaubares Geflecht“ bildeten, schreibt *Netzpolitik.org*. Ihr Geschäft ist das Sammeln und Handeln mit hochsensiblen und intimen Informationen über Menschen, die beim Surfen und Kommunizieren im Internet haufenweise streng Vertrauliches über sich preisgeben. Und sie hinterlassen Fußabdrücke,

Positionsdaten, mit denen sich exakte Bewegungsprofile erstellen lassen.

Um Letzteres geht es im Wesentlichen bei dem Paket aus dem Hause Datasys, einer Firma mit Sitz in Florida, die bis vor Kurzem noch unter dem Namen Datastream Group auftrat. Datiert auf den 2. Juli 2024 sind in ihm 380 Millionen Standortdaten aus 137 Ländern verschnürt, übermittelt durch rund 40.000 unterschiedliche Apps, also kleine Computerprogramme auf iOS- oder Android-betriebenen Handys. Die Dimensionen der Machenschaften sind schwindelerregend: Der monströse Fundus ist in Wirklichkeit nur eine Kostprobe des Anbieters, eine „Gratisvorschau", die „Lust auf ein Monatsabo mit tagesaktuellen Daten machen" sollte. Faktisch handelt es sich bloß um einen Schnappschuss, wie er im globalen Maßstab stündlich vielleicht tausendfach den Besitzer wechselt. Zu den Standortdaten gehören sogenannte Mobile Advertising IDs. Solche Werbekennungen funktionierten wie „Nummernschilder" und machten Nutzer „eindeutig erkennbar". Zu finden seien auch Infos über das verwendete Handymodell und den Netzbetreiber, etwa Vodafone oder die Telekom.

Schluss mit Privatleben

Der *Westdeutsche Rundfunk (WDR)* hat Beispiele aufgezählt, was sich mit all dem anstellen lässt. Es ließen sich etwa „regelmäßige Bewegungsmuster zwischen Wohn- und Arbeitsort" rekonstruieren oder wiederkehrende Aufenthalte in Restaurants, Fitnessstudios oder Kinos. Kontakte zu Kliniken und Apotheken könnten Rückschlüsse auf den Gesundheitszustand der Betroffenen ermöglichen. Durch Verknüpfung mit weiteren Datenquellen entstehe so „ein nahezu vollständiges Bild des Lebens einer Person".

Netzpolitik.org hatte schon im vergangenen Sommer einen umfangreichen Datensatz aus identischer Quelle analysiert – Datenbroker Files – und Beängstigendes zutage gefördert. Stalker könnten ihren Opfern auflauern. Wer in sicherheitsrelevanten Bereichen arbeitet, kann erpressbar werden. Zum Beispiel offenbarten die Standortdaten „Besuche in Bordellen, Suchtkliniken oder Gefängnissen". Mit dem neuen Material, das wohlgemerkt nur einen Tag abdeckt, gelang es den Rechercheuren nun sogar, die Wohnadressen zweier Nutzer ausfindig zu machen. Über eine Person brachten sie noch mehr in Erfahrung: „Sie lebte (…) in einem Einfamilienhaus, besuchte ein nahe gelegenes Krankenhaus und eine Spezialklinik in einer bayerischen Großstadt." Was erst kann ein Mensch für und von sich behalten, wenn er eine Woche, einen Monat oder noch länger auf dem Radar ist?

Metergenaue Ortung

Wer sind die „Spanner" und warum tun sie das? Los geht es mit den Apps, die die Daten

erheben. Dazu zählen sehr gängige Anwendungen: Wetter-Apps, Fitness- und Gesundheits-Apps, Navigations-, Social-Media- und Gebets-Apps. Dazu kommen solche für Spiele, Dating, Shopping, Nachrichten und Bildung. Nicht wenige davon sind sehr verbreitet und wurden bereits millionenfach heruntergeladen, auch hierzulande. Namentlich genannt werden Tinder, Grindr, Candy Crush Saga sowie Upday vom Axel-Springer-Konzern, web.de, gmx.de, Focus Online, Kleinanzeigen, FlightRadar24, Hornet, WordBit und Kik. Letzteres ist ein US-Messengerdienst. Mit den entsprechenden Daten spürten norwegische Journalisten eine Person auf, die das schockte: „Ich finde das beängstigend und möchte nicht, dass irgendjemand ständig weiß, wo ich bin und was ich mache."

Es gibt Programme, die den Aufenthaltsort ihrer User mit einer Genauigkeit von unter einem Meter bestimmen. Dazu zählen Angebote der WetterOnline GmbH – ein Schwerpunkt der Recherche –, für die bis dato mehr als 100 Millionen Downloads verzeichnet sind. Allein „Wetter Online mit Regenradar" für Android lief auf knapp 34.000 der an besagtem 2. Juli 2024 in Deutschland georteten 795.000 Handys. Die Produkte der Gesellschaft zählen auch zu den deutschen Apps, die die meisten Positionsdaten ausspucken und an Dritte weiterreichen. Dabei handelt es sich erklärtermaßen um „Werbepartner", aktuell mehr als 830 an der Zahl. Darunter befinden sich Branchenriesen wie Google und die Microsoft-Tochter Xandr. Diese Vorgänge sind zumindest auf dem Papier rechtmäßig. Laut Eintrag im Google Play Store darf WetterOnline den genauen Standort zwecks Werbung und Marketing teilen.

Einer zahlt, alle greifen zu

Aber wie kann es angehen, dass der Ouput in die Hände gieriger Datenhändler gelangt, die die Inhalte einsammeln, aufbereiten und als umfangreiche Datensätze weiterverkaufen? Darauf gab das Bonner Unternehmen nach wiederholten Kontaktversuchen keine Antwort. So lief dies bei vielen der Anfragen. Die Datingplattform Hornet ließ immerhin verlauten: „Wir können die Möglichkeit nicht vollständig ausschließen, dass Werbenetzwerke von Drittanbietern Daten ohne unsere Kenntnis oder Zustimmung weitergegeben haben könnten."

Warum nicht? Weil die Wege der Daten „selbst für Insider verschlungen" seien, heißt es bei *Netzpolitik.org*. Der Knackpunkt ist demnach ein System namens Real Time Bidding (RTB), das darüber entscheidet, welche Werbung von welchem Unternehmen auf dem Handy eines Users erscheint. Das geschieht im Rahmen von Auktionen, die vollautomatisiert und in Millisekunden vonstatten gehen. Dabei senden die Apps Infopakte mit sogenannten Bidstream-Daten – darunter die Advertiser ID und die IP-Adresse der Nutzer – an Plattformen aus, die sie wiederum an eine Vielzahl an Firmen weiterleiten. „Dann bieten die

Unternehmen Mikro-Centbeträge, um unsere Aufmerksamkeit zu bekommen. Der Meistbietende darf seine Werbung ausspielen“, erläutern die Journalisten. „Aber unsere Daten haben alle bekommen.“ In der Masse der Beteiligten reiche es, wenn nur einer die Daten abzwacke, um daraus Pakete für Databroker zu schnüren. „Weder die App-Anbieter noch die Nutzer bekommen das direkt mit.“

650.000 Schubladen

Schöne neue Welt!? Im Kosmos der Werbestrategen sind Menschen nur Konsumentenvieh, das sie in Boxen pferchen und mit den passenden Botschaften anfixen. Mit dem Internet haben sich die Möglichkeiten revolutioniert. Auf Basis wiederholter Datensammlungen werden potenzielle Kunden diversen Segmenten zugeteilt, etwa „fragile Senioren“ „Shopping-versessene Mütter“, um die Zielgenauigkeit der Botschaften zu erhöhen. 2023 enthüllte *Netzpolitik.org*, wie die Branche ihre Kundschaft in „650.000 unterschiedliche Segmente steckt“. Viele dieser Schubladen basierten auf Standorten: „Menschen, die in die Kirche gehen oder in Sexshops, die in wohlhabenden Vierteln wohnen oder auf dem Land.“

Die neuen Befunde zeigten, „dass sich der globale Online-Werbemarkt jeglicher Kontrolle entzogen hat“, befand Michaela Schröder vom Verbraucherzentrale Bundesverband (vzbv). „Skrupellose Datenhändler sammeln und verbreiten hochsensible Informationen über Menschen, während Webseiten und Apps diese rechtswidrigen Praktiken überhaupt erst ermöglichen und die Aufsichtsbehörden völlig überfordert zu sein scheinen.“ Der vzbv fordert Konsequenzen auf europäischer Ebene. Es sei längst überfällig, dass die Europäische Kommission die Verbraucher wirksam schütze und einen Vorschlag vorlege, personalisierte Werbung zu verbieten – etwa über den angekündigten Digital Fairness Act, so Schröder.

Lobby blockiert Regulierung

Tatsächlich war ein entsprechender Anlauf im Rahmen der sogenannten ePrivacy-Verordnung im Jahr 2023 am Widerstand durch Lobbyisten gescheitert. Und dass sich die Politik alsbald eines Besseren besinnt, erscheint bei den bestehenden Kräfteverhältnissen ziemlich abwegig. Aber ganz schutzlos sind die Verbraucher trotzdem nicht. Es gibt eine Reihe an technischen Kniffen, mit denen sich die Ortungsfunktionen von Smartphones, Tablets und PCs abschalten beziehungsweise umgehen lassen.

Wer voll auf Nummer sicher gehen will, dass ihm Konzerne, Schnüffler und Kriminelle nicht auf die Pelle rücken, sagt am besten gleich ganz Tschüss zum Handy. Das schult auch Orientierung und Instinkte. Dann kann man auch nicht verloren gehen.

Titelbild: AlinStock/shutterstock.com