Standortbestimmung

Veröffentlicht von: N8Waechteram: 15. Januar 2019

Den Meisten Nutzern von Schlau- und Wischtelefonen dürfte unbekannt sein, in welchem Ausmaß Daten ihres Mobiltelefons von verschiedenen Unternehmen abgegriffen und gespeichert werden, um sie mittels Algorithmen zu analysieren und Profile allerlei Arten zu erstellen.

Im Bereich der Sozialen Medien mag dies durchaus bekannt sein, wird der Nutzer doch aufgefordert, den AGBs zuzustimmen, in welchen offen zugegeben wird, dass alle Daten gespeichert und "an Dritte" verkauft werden, damit etwaige Werbung den vermeintlichen Interessen gemäß die mögliche Kundschaft erreicht.

Einer der größten und langjährigen Spieler im Weltnetz-Werbemarkt ist Google und das Unternehmen wird keineswegs umsonst als "Datenkrake" bezeichnet. Jede Suche wird gespeichert und der Analyse zugeführt – ein vollautomatischer Vorgang, welcher der Profilbildung für entsprechende IP-Adressen dient.

Ob es eine soeben gebuchte Reise mit der Deutschen Bahn ist, eine Suche nach irgendeiner Versicherung, ein Einkauf bei Amazon oder sonstige spezifische Eingaben in der Google-Suchmaske, innerhalb kurzer Zeit wird entsprechend verwandte Werbung auf besuchten Netzseiten angezeigt. Solange der Nutzer mit seinem Google-Konto angemeldet im Netz unterwegs ist, wird alles gespeichert.

Weniger bekannt dürfte Nutzern von als "Smartphone" getarnten, transportablen Wanzen sein, dass auch die in vielen Geräten eingebaute Sprachsteuerung gerne lauscht und die abgehörten Informationen, über Spracherkennungsprogramme in Textdateien umgewandelt, der entsprechenden Datenbank hinzufügt. Zu Vielen fehlt es an Aufmerksamkeit einen Zusammenhang zu erkennen, wenn man sich mit einem Freund über etwas unterhalten hat und wenig später auf Internetseiten eingeblendeter Werbung ausgesetzt wird, welche nur allzu passend scheint. Doch ein "Zufall" kann hier ausgeschlossen werden.

Jedoch werden von den zahlreichen Anwendungen auf Mobiltelefonen nicht nur Beiträge auf Sozialen Medien oder Suchanfragen zur Profilerstellung genutzt. Wie die US-Seite Motherboard unlängst berichtete, wird der Standort des Gerätes nicht nur ständig überwacht und aufgezeichnet, sondern ist die Standortbestimmung auch ein überaus einträgliches Geschäft.

Jedes angeschaltete Mobiltelefon steht in Verbindung zu den in der Nähe befindlichen Mobilfunkverteilern. Folglich weiß der entsprechende Anbieter nicht nur, wie Anrufe, Textnachrichten und Zugriffe auf das Internet weitergeleitet werden, sondern der Standort des Gerätes lässt sich mittels der jeweiligen Entfernung der Sendemasten auch recht genau bestimmen.

Joseph Cox von Motherboard ging der Frage nach, ob ein x-beliebiges Mobiltelefon ausschließlich anhand der Telefonnummer auffindbar ist und traf sich zu diesem Zweck mit einem "Kopfgeldjäger":

„Er hatte angeboten, den Standort eines Telefons für mich herauszufinden, indem ein zwielichtiger, übersehener Dienst benuzt wird, welcher nicht für die Polizei, sondern für Privatleute und Unternehmen gedacht ist.

Bewaffnet nur mit der Nummer und ein paar hundert Dollar sagte er, er könne den derzeitigen Standort fast aller Telefone in den Vereinigten Staaten herausfinden.“

Gegen $ 300 gab der “Kopfgeldjäger“ die Nummer an eine Kontaktperson weiter und wenig später kam ein Bildschirmfoto von Google Maps, auf welchem Queens, ein Stadtteil von New York City, zu sehen war und zudem ein blauer Kreis, welcher den Standort des Telefons auf wenige hundert Meter genau markierte.

Cox betont, dass der “Kopfgeldjäger“ hierfür ausschließlich die Telefonnummer benötigte und keinerlei Vorwissen um den Standort des Telefons hatte. Die Quelle für die Standortbestimmung in Echtzeit seien die Telekommunikationsunternehmen selbst, so heißt es. In diesem Fall T-Mobile, jedoch funktioniere dies auch mit den US-Anbietern AT&T und Sprint.

„Die Nachforschungen von Motherboard zeigen, wie ungeschützt mobile Netzwerke und die darin generierten Daten wirklich sind. Sie sind offen für die Überwachung durch normale Bürger, Stalker und Kriminelle […].

Die Untersuchung zeigt ebenfalls, dass eine Vielzahl von Unternehmen auf Standortdaten eines Mobiltelefons zugreifen können und dass die Informationen von Mobilanbietern an ein breites Spektrum kleinerer Spieler weitergegeben wird, welche nicht unbedingt die richtigen Sicherheitsmaßnahmen einsetzen, um diese Daten zu schützen.“

Die Standortbestimmung lief in diesem Fall über das Unternehmen Microbilt und auf Anfrage von Motherboard wurde dem Bericht nach eine Preisliste zugesandt, auf welcher die einzelnen Angebote aufgelistet werden:

Identity Verification

(Select all services currently planned for use and/or testing)

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6
	1-250	251-1,000	1,001-5,000	5,001-10,000	10,001-20,000	20,001 +
Mobile Device Verification *						
- **Mobile Device Account Verification** [1] ☐	$0.25	$0.23	$0.20	$0.18	$0.17	$0.16
- **Mobile Device Account & Location Verification** [2] ☐	$4.95	$4.46	$3.96	$3.56	$3.32	$3.22
- **Mobile Device Account & Location Verification Monitoring (per device)** [3] ☐	$12.95	$11.66	$10.36	$9.32	$8.68	$8.42
- **Mobile Device Verification Report** ☐	Included with Monitoring					

* All items are governed by FCRA guidelines. Charges are assessed for inquiries returning a “Hit” and “No Hit” result for all verification products.
1 Verifies the submitted information against the mobile carrier billing account information.
2 Verifies the submitted information against the mobile carrier billing account information & attempts to identify the mobile device location.
3 Verifies the submitted information against the mobile carrier billing account information & attempts to identify the mobile device location with subsequent location monitoring.

2. User's intended use of the above service(s) is: _____.

Demnach lässt sich der aktuelle Standort einer Mobilfunknummer für $ 4,95 feststellen

und für $ 12.95 gar Bewegungen überwachen. Dass die Preise mit der Anzahl der überwachten Geräte günstiger werden, spricht eine ganz eigene Sprache. Und dass der Mittelsmann satte $ 300 berechnete, zeigt überdeutlich auf, wie lukrativ diese Art von Geschäft augenscheinlich ist.

Dass Amazons Alexa immer zuhört und dieses und vergleichbare Geräte somit im leichtgläubigen Einverständnis installierte Wanzen innerhalb der eigenen vier Wände sind, ist mittlerweile kein Geheimnis mehr. Ebenso wenig ist es ein Geheimnis, dass tatsächlich jede Eingabe auf allen mit dem Weltnetz verbundenen Geräten aufgezeichnet, analysiert und dem persönlichen Profil hinzugefügt wird, wie auch "Online-Streaming" oder Tonaufzeichnungen.

Das zu Amazon gehörende Unternehmen Ring geht jedoch noch einen Schritt weiter. Ring ermöglicht den direkten Zugriff auf Überwachungskameras, beispielsweise im eigenen Haus oder auf dem Gründstück, und The Intercept berichtet, dass der Echtzeitzugriff mittels Mobiltelefon oder Tablet keineswegs ausschließlich dem berechtigten Nutzer dieser Technik vorbehalten ist:

„Laut einer Quelle stellte Ring seit 2016 seiner in der Ukraine ansässigen Forschungs- und Entwicklungsgruppe praktisch uneingeschränkten Zugriff zu einem Ordner auf Amazons S3-Cloud zur Verfügung, welcher jedes Video enthielt, welches jemals weltweit von einer Ring-Kamera erstellt wurde. […] Diese Kunden-Videodateien herunterzuladen und zu teilen hätte wenig mehr als einen Klick bedurft. […]

Zu dem Zeitpunkt, als der Zugriff in der Ukraine zur Verfügung gestellt wurde, waren die Videodateien unverschlüsselt […]. Die Gruppe in der Ukraine wurde auch mit einer entsprechenden Datenbank versorgt, welche jede einzelne Videodatei mit einem bestimmten Kunden von Ring in Verbindung brachte."

Auch wenn es nach wie vor Menschen gibt, die der Überzeugung sind, ein "Tor-Browser" oder "VPN" würde sie tatsächlich unsichtbar machen, so machen derartige Hilfsmittel und Werkzeuge es jenen Leuten, welche wirklich jeden Schritt verfolgen wollen, bestenfalls ein wenig schwieriger. Anonymität ist im heutigen Technikzeitalter eine überwiegende Illusion.

Auf dem Zuse-Rechner wird jeder Klick und jede Tasteneingabe verfolgt. Mobile Wanzen trägt heute fast jeder mit sich herum. Soziale Medien verkaufen alle greifbare Daten, Telefonanbieter auch Standortdaten. Alexa und dergleichen hören unsere Wohnungen ab und Ring speichert alle Videoaufnahmen unverschlüsselt in einer "Cloud". Spracherkennung, Gesichtserkennung, Standortermittlung, Profilerstellung – "Jason Bourne" ist längst da und der "Große Bruder" hat zumindest die Möglichkeiten, immer mitzuhören.

Der einzige Weg, sich dieser Überwachungswelt zumindest zeitweise ein Stück weit zu entziehen, ist das Zurücklassen aller Geräte und die Zuflucht in der Natur. Doch Vorsicht bei seltsamen Geräuschen am Himmel: Es könnte eine Drohne sein.

Alles läuft nach Plan …

Der Nachtwächter

***