Wie Ihre Fritteuse und andere Haushaltsgeräte zu Datensammler werden

Haben Sie beim Kauf Ihrer schicken Fritteuse gedacht, es geht nur um perfekt knusprige Zwiebelringe? Tatsächlich könnte sie Ihre Daten auf einem Silbertablett an die globalen Tech-Giganten liefern.

Die britische Verbraucherschutzorganisation Which? hat die dunkle Seite der „smarten“ Geräte enthüllt: Ihre Fritteuse könnte nicht nur Ihre Kalorien im Blick haben, sondern auch tief in Ihr Privatleben eintauchen.

Die Bequemlichkeit eines Wi-Fi-fähigen Küchengeräts kommt mit einer ordentlichen Portion Überwachung daher, und Fritteusen sind nur die Vorspeise in diesem Bankett von invasiven intelligenten Geräten.

Alexa, warum benötigt meine Heißluftfritteuse mein Geburtsdatum?

Bei einem Test von Produkten aus vier Kategorien – Heißluftfritteusen, Smartwatches, smarte Lautsprecher und intelligente Fernseher – enthüllte die britische Verbraucherschutzorganisation „Which?“ einen regelrechten Albtraum des Datensammelns. Besonders absurd: Eine Heißluftfritteuse verlangte tatsächlich die Erlaubnis, das Telefon der Nutzer abzuhören. Ja, richtig gelesen – Audioaufzeichnung, weil eine Fritteuse offenbar unbedingt mitlauschen muss, wenn Sie sich gerade über das perfekte Gewürz beraten.

Ein anderes Gerät von Xiaomi ging noch einen Schritt weiter und verknüpfte seine App mit dem „Who is Who“ der Daten-Tracker, darunter Facebook, TikToks Pangle und Tencent. Brauchen Sie eine Minute, um das zu begreifen? Nehmen Sie sich Zeit, denn Ihre Unentschlossenheit wird bereits protokolliert. Auch die Friteusen von Aigostar und Xiaomi übermitteln Ihre persönlichen Daten an Server in China. Dies wurde in ihren Datenschutzhinweisen offengelegt, denn Transparenz bedeutet nichts, wenn sie in juristischem Fachjargon vergraben ist, den Sie nie lesen.

Das wirft die offensichtliche Frage auf: Wozu benötigt man eine Fritteuse, die gleichzeitig als Datensauger dient? Spoiler: Sie brauchen sie nicht. Aber sie verkaufen Ihre Gewohnheiten, Vorlieben und sogar Ihr Geschlecht und Geburtsdatum für Marketingzwecke und möglicherweise

für die globale Datenherrschaft.

Intelligente Lautsprecher und dumme Entscheidungen

Die Untersuchung ergab, dass die intelligenten Lautsprecher von Amazon Echo einen flüchtigen Hoffnungsschimmer bieten: Sie können einige Aufforderungen zur Datenfreigabe während der Einrichtung überspringen. Aber machen Sie es sich nicht zu gemütlich. Um das Gerät zu verwenden, benötigen Sie immer noch ein Amazon- oder Google-Konto, was vorhersehbar dafür sorgt, dass das Mutterschiff einen ständigen Strom Ihrer Daten erhält.

Der Bose Home Portable-Lautsprecher versuchte, den Datenschutz-Heiligen zu spielen, indem er von vornherein um minimale Erlaubnis bat. Doch unter der Oberfläche verbirgt sich ein Rattennest von Trackern, darunter Facebook und Google. Bose, so scheint es, hat die Kunst perfektioniert, tugendhaft zu erscheinen und gleichzeitig Ihre Daten zu horten wie ein Schnäppchen am schwarzen Freitag.

Smartwatches: Der Narc am Handgelenk

Sie denken darüber nach, Ihr Handgelenk aufzurüsten? Denken Sie anders. Zwei preiswerte Smartwatches, die auf Amazon verkauft werden, Kuzil und WeurGhy, wurden als nahezu identische Produkte entlarvt, die kaum funktionieren, es sei denn, Sie geben Ihre Zustimmung zum Datenschutz ab. Ohne diese Zustimmung, herzlichen Glückwunsch, haben Sie eine dumme Uhr gekauft, die nur die Zeit anzeigt.

Die Ultimate-Smartwatch von Huawei geht noch einen Schritt weiter und fordert neun „riskante“ Telefonberechtigungen an, die ihr uneingeschränkten Zugriff auf Ihre Dateien, Ihren Standort, Ihre Audiodaten und sogar einen Blick auf Ihre anderen Apps gewähren. Wenn Sie sich jetzt eine Smartwatch umschnallen, klingt das eher nach einem Onboarding von Big Brother als nach einem Upgrade Ihrer Technik.

Fernsehgeräte: Sie beobachten, wie Sie sie beobachten

Dann gibt es noch die Smart-TVs. Hisense und Samsung verlangen bei der Einrichtung unter dem Vorwand der „Inhaltslokalisierung“ eine Postleitzahl. Samsung besteht darauf, dass dies optional

ist, obwohl Which? fand das Gegenteil heraus. Die TV-App von Samsung verlangte dagegen acht Berechtigungen, darunter die Möglichkeit, alle installierten Apps einzusehen. Das ist richtig: Ihr Fernseher macht sich Notizen über Ihre App-Bibliothek, während Sie Ihre Lieblingssendungen ansehen.

Selbst Hisense, das keine Verbindung zu Trackern herstellte, nutzte die Standortdaten in großem Umfang. LG und Samsung verknüpften ihre Fernseher mit den üblichen Verdächtigen – Facebook, Google und anderen Marketing-Haien -, denn warum sollte man sich einen Film ansehen, ohne sich gleichzeitig in einen solchen zu verwandeln?

Das große Bild: Überwachung durch Design

Der Redakteur von Which?, Harry Rose, fasst es mit erschreckender Klarheit zusammen: „Hersteller von intelligenten Technologien und die Firmen, mit denen sie zusammenarbeiten, sind derzeit in der Lage, scheinbar rücksichtslos Daten von Verbrauchern zu sammeln, und dies geschieht oft mit wenig oder gar keiner Transparenz.“ Übersetzung: Ihre Geräte sind schwarze Löcher für den Datenschutz, und nein, Ihre Zustimmung gilt nicht als informiert, wenn sie unter Schichten von Jargon begraben ist.

Das britische Information Commissioner’s Office plant, bis 2025 neue Leitlinien für intelligente Produkte zu erlassen. Aber solange diese Regeln nicht mit Zähnen – und einem ernsthaften internationalen Schutz – versehen sind, wird der Überwachungszirkus die Aufsichtsbehörden weiter umtreiben.

Wenn Sie also das nächste Mal ein Küchengerät, ein Wearable oder sogar einen Fernseher kaufen, fragen Sie sich: Müssen Sie wirklich Ihre Privatsphäre für das Versprechen einer „intelligenten“ Technologie opfern? Oder ist es an der Zeit, der Überwachungswirtschaft ein Gerät nach dem anderen zu entziehen?

Das Internet der Dinge beobachtet Sie: Wie „intelligent“ zu einem Synonym für Überwachung wurde

Der Traum von einer vollständig vernetzten Welt liegt schon lange vor uns, eine futuristische Utopie, in der Ihr Kühlschrank Milch bestellt, bevor sie ausgeht, Ihr Licht gedimmt wird, wenn Sie bettfertig sind, und Ihre Fritteuse genau weiß, wie Sie Ihre Zwiebelringe mögen. Doch während das Internet der Dinge (IoT) Bequemlichkeit und Effizienz verspricht, baut es im Stillen ein Überwachungsimperium auf, in dem Sie – und nicht das Gerät – das Produkt sind.

Von intelligenten Lautsprechern bis zu Zahnbürsten sind mit dem Internet verbundene Geräte allgegenwärtig und haben sich in unser tägliches Leben integriert. Doch hinter dem glänzenden Äußeren verbirgt sich eine dunklere Wahrheit: Diese Geräte sind datenhungrige Spione, die oft weit mehr Informationen sammeln, als sie für ihre Funktion benötigen. Und mit der Ausdehnung dieses Ökosystems nimmt auch das Ausmaß der Aushöhlung der Privatsphäre zu – für die Verbraucher bedeutet das einerseits Bequemlichkeit und andererseits einen massiven Vertrauensbruch.

Die Verführung durch intelligente Geräte

IoT-Geräte sind so konzipiert, dass sie sich unverzichtbar anfühlen. Sie sparen Zeit, verringern den Aufwand und liefern den süchtig machenden Dopamin-Kick der Automatisierung. Was kann man nicht daran lieben, Alexa zu bitten, das Licht einzuschalten, oder sich von seiner Smartwatch daran erinnern zu lassen, sich nach Stunden am Schreibtisch zu strecken?

Doch der Komfort hat seinen Preis, und dieser Preis sind oft Ihre Daten. Wenn Ihre Geräte ständig mit dem Internet verbunden sind, führen sie nicht nur Ihre Befehle aus, sondern laden auch riesige Mengen an Informationen über Sie hoch. Ihre Gewohnheiten, Vorlieben, Ihr Standort und sogar private Gespräche werden akribisch aufgezeichnet, verpackt und an den Meistbietenden verkauft.

Es geht nicht nur darum, welche Daten gesammelt werden, sondern auch darum, wie viele. IoT-Geräte sammeln oft Informationen, die weit über das hinausgehen, was für ihre Funktion notwendig ist. Man denke nur an Heißluftfritteusen, die Zugriff auf das Mikrofon verlangen, an Smart-TVs, die Ihre Postleitzahl abfragen, oder an Smartwatches, die nicht richtig funktionieren, wenn Sie nicht Ihren genauen Standort und die Nutzung von Apps preisgeben.

Diese Daten werden nicht nur zur Verbesserung von Produkten verwendet. Sie werden in ein ausgeklügeltes Netz von Datenmaklern, Werbetreibenden und Tech-Giganten eingespeist, die damit unheimlich genaue Profile von Ihnen erstellen. Diese Profile können Ihre politische Meinung beeinflussen, Ihr Verhalten manipulieren und sogar Ihren Zugang zu Dienstleistungen bestimmen.

Und das Erschreckendste daran? Vieles davon geschieht mit wenig oder gar keiner Transparenz. Die Datenschutzrichtlinien von IoT-Unternehmen sind oft labyrinthisch und voller juristischer Formulierungen, die verschleiern, wie eingreifend ihre Praktiken sind. Nur wenige Menschen lesen sie, und noch weniger verstehen die Auswirkungen wirklich.

So verlockend die Annehmlichkeiten von Geräten mit Internetanschluss auch sein mögen, es ist klar, dass diese Geräte erhebliche Risiken für den Datenschutz mit sich bringen. Es ist immer am besten, sie nach Möglichkeit ganz zu vermeiden. Wenn das nicht möglich ist, gibt es glücklicherweise Maßnahmen, die Sie ergreifen können, um diese Risiken zu minimieren und die Kontrolle über Ihre persönlichen Daten zurückzugewinnen.

1. Lesen und verstehen Sie die Datenschutzrichtlinien

Datenschutzrichtlinien mögen trocken und voller Fachjargon sein, aber sie sind Ihre erste Verteidigungslinie. Informieren Sie sich vor dem Kauf eines Geräts, welche Daten es sammelt, wie sie verwendet und ob sie an Dritte weitergegeben werden. Wenn die Richtlinien zu sehr in die Privatsphäre eingreifen – oder schlimmer noch: vage sind -, sollten Sie sich zweimal überlegen, ob Sie das Gerät in Ihr Zuhause holen.

2. Datenschutzeinstellungen anpassen

Wenn Sie ein Smart-Gerät gekauft haben, sollten Sie sich nicht mit den Standardeinstellungen zufrieden geben. Nehmen Sie sich die Zeit, die Datenschutzeinstellungen zu durchforsten und alle unnötigen Funktionen zur Datenweitergabe zu deaktivieren. Bei einigen Geräten können Sie sogar bestimmte Datenerfassungsprozesse deaktivieren, aber diese Optionen sind oft tief in den Menüs verborgen. Suchen Sie sie heraus.

3. Unnötige Funktionen deaktivieren

Ein Smart-TV oder eine Heißluftfritteuse müssen sich nicht wie ein Spionage-Agent verhalten. Wenn er ohne zwingenden Grund Zugriff auf ein Mikrofon, eine Kamera oder GPS verlangt, sollten Sie diese Berechtigungen deaktivieren. Bei den meisten Geräten können Sie diese Funktionen entweder über die zugehörige App oder direkt in den Einstellungen Ihres Telefons steuern.

4. Internet-Konnektivität einschränken

Nicht jedes intelligente Gerät benötigt einen ständigen Internetzugang, um zu funktionieren. Eine Heißluftfritteuse zum Beispiel benötigt kein Wi-Fi, um Essen zu frittieren. Wenn Sie solche Geräte nach Möglichkeit offline halten, reduzieren Sie die Datenmenge, die sie an Hersteller und Dritte übertragen können, erheblich.

5. Sichern Sie Ihr Heimnetzwerk

Ihre Geräte sind nur so sicher wie Ihr Netzwerk. Schützen Sie Ihr Heim-Wi-Fi durch:

- Verwenden Sie ein sicheres, eindeutiges Passwort.
- Aktivieren der Zwei-Faktor-Authentifizierung auf Ihrem Router, falls verfügbar.
- Einrichten eines Gastnetzwerks für die Geräte von Besuchern.
- Regelmäßige Aktualisierung der Firmware Ihres Routers, um Sicherheitslücken zu schließen.

- Für zusätzliche Sicherheit sollten Sie ein virtuelles privates Netzwerk (VPN) verwenden, um die IP-Adresse Ihres Hauses zu verbergen und Ihren Internetverkehr zu verschlüsseln.

6. Halten Sie die Gerätefirmware auf dem neuesten Stand

Die Hersteller veröffentlichen häufig Firmware-Updates, um Fehler zu beheben und Sicherheitslücken zu schließen. Aktivieren Sie nach Möglichkeit automatische Updates oder planen Sie regelmäßige Überprüfungen, um sicherzustellen, dass Ihre Geräte über den neuesten Schutz vor neuen Bedrohungen verfügen.

7. Informieren Sie sich über Datenpraktiken

Wissen ist Macht. Folgen Sie vertrauenswürdigen Verbraucherschutzgruppen, um über Datenpraktiken und Datenschutzrisiken im Zusammenhang mit intelligenten Geräten auf dem Laufenden zu bleiben. Wenn Sie diese Themen verstehen, können Sie fundierte Kaufentscheidungen treffen und unnötige Risiken vermeiden.

8. Unterstützung strengerer Datenschutzbestimmungen

Individuelle Maßnahmen sind wichtig, aber um das Problem an der Wurzel zu packen, sind systemische Veränderungen erforderlich. Setzen Sie sich für solide Datenschutzgesetze ein, die Transparenz fordern, das Sammeln von Daten begrenzen und Verstöße streng bestrafen. Unterstützen Sie Organisationen und Politiker, die dem Verbraucherschutz Priorität einräumen.

9. Wählen Sie nicht-intelligente Alternativen

Nicht jedes Gerät muss mit dem Internet verbunden sein, um seinen Zweck zu erfüllen. Eine herkömmliche Kaffeemaschine, ein stummer Fernseher oder ein mechanischer Thermostat funktionieren oft genauso gut – wenn nicht sogar besser -, ohne in Ihre Privatsphäre einzudringen. Der einfachste und effektivste Weg, die Ausbeutung von Daten zu vermeiden, ist es, analog zu arbeiten.

10. Entscheiden Sie sich für Tools, die den Datenschutz berücksichtigen

Wenn Sie ein intelligentes Gerät verwenden müssen, suchen Sie nach datenschutzfreundlichen Alternativen. Zum Beispiel:

- Verwenden Sie Apps, die die Gerätekontrolle ohne unnötige Datenberechtigungen zusammenfassen.
- Erkunden Sie Open-Source-Plattformen, bei denen der Schutz der Privatsphäre der Nutzer im Vordergrund steht.
- Vermeiden Sie Apps, die mit bekannten Unternehmen verbunden sind, die Daten sammeln, wie Facebook oder TikTok.

Quelle: How Your Air Fryer and Other Household Appliances Became Data Miners

Revision #1
Created 2024-12-07 15:08:55 UTC by willi
Updated 2024-12-07 15:09:43 UTC by willi