Schützen Sie Ihre Privatsphäre in einer Welt der digitalen Überwachung

- Wie Google Ihr gesamtes Leben erfasst
- Wie mobile Apps Sie ständig verfolgen
- 5 einfache Schritte, um sich und Ihre Familie zu schützen

murena
choose freedom

Zusammenfassung

Im heutigen digitalen Zeitalter ist der Schutz der Privatsphäre zu einem der wichtigsten Themen für Einzelpersonen und Gesellschaften geworden. Die Geräte, auf die wir uns verlassen – insbesondere unsere Smartphones – sammeln eine immense Menge an persönlichen und beruflichen Daten, oft ohne unser vollständiges Verständnis oder unsere echte Zustimmung.

Technologiegiganten wie Google und Apple sowie eine Vielzahl mobiler Anwendungen haben Zugriff auf intime Details unseres Lebens, und die Methoden, mit denen sie uns verfolgen, stellen erhebliche Bedrohungen für unsere Privatsphäre und Sicherheit dar.

Dieses Dokument untersucht, in welchem Umfang Unternehmen wie Google und Apple Benutzerdaten sammeln, wie mobile Apps Benutzer über Werbung und Echtzeitauktionen verfolgen und welche möglichen Konsequenzen solche Praktiken haben können.
Es bietet auch einfache Schritte, um sich vor digitaler Überwachung zu schützen.

Wie Google Benutzerdaten sammelt und verwendet

Google, eines der weltweit größten Technologieunternehmen, hat sein Imperium aufgebaut, indem es „kostenlose“ Dienste wie Gmail, Google Search, YouTube und Google Maps anbietet und dabei enorme Gewinne aus Werbung erzielt. Diese Dienste haben jedoch erhebliche Kosten für die Privatsphäre der Nutzer.

Wie Google Ihre Daten sammelt:

- Standortverfolgung
- Such- und Browserverlauf
- Persönliche Kommunikation
- Google-Apps und Android

11,6 MB/Tag/Nutzer

Die Menge Ihrer persönlichen Daten, die Google von Android-Smartphones sammelt.

Quelle: Digital Content Next – Prof. Douglas C. Schmidt, Vanderbilt University, August 2018.

Wie Google Benutzerdaten sammelt und verwendet

Standortverfolgung

Google verfolgt Ihren Standort, selbst wenn Sie Google Maps nicht verwenden. Es sammelt Echtzeitdaten von Android-Geräten und kann Ihren Standort über IP-Adressen, Wi-Fi-Netzwerke und Bluetooth-Verbindungen ermitteln.

Wie Google Benutzerdaten sammelt und verwendet

Such- und Browserverlauf

Jede Suche, die Sie über Google Search durchführen, und jede Website, die Sie über Google Chrome besuchen, wird verfolgt und protokolliert. Dadurch kann Google ein detailliertes Profil Ihrer Interessen, Gewohnheiten und Verhaltensweisen erstellen.

Wie Google Benutzerdaten sammelt und verwendet

Persönliche Kommunikation

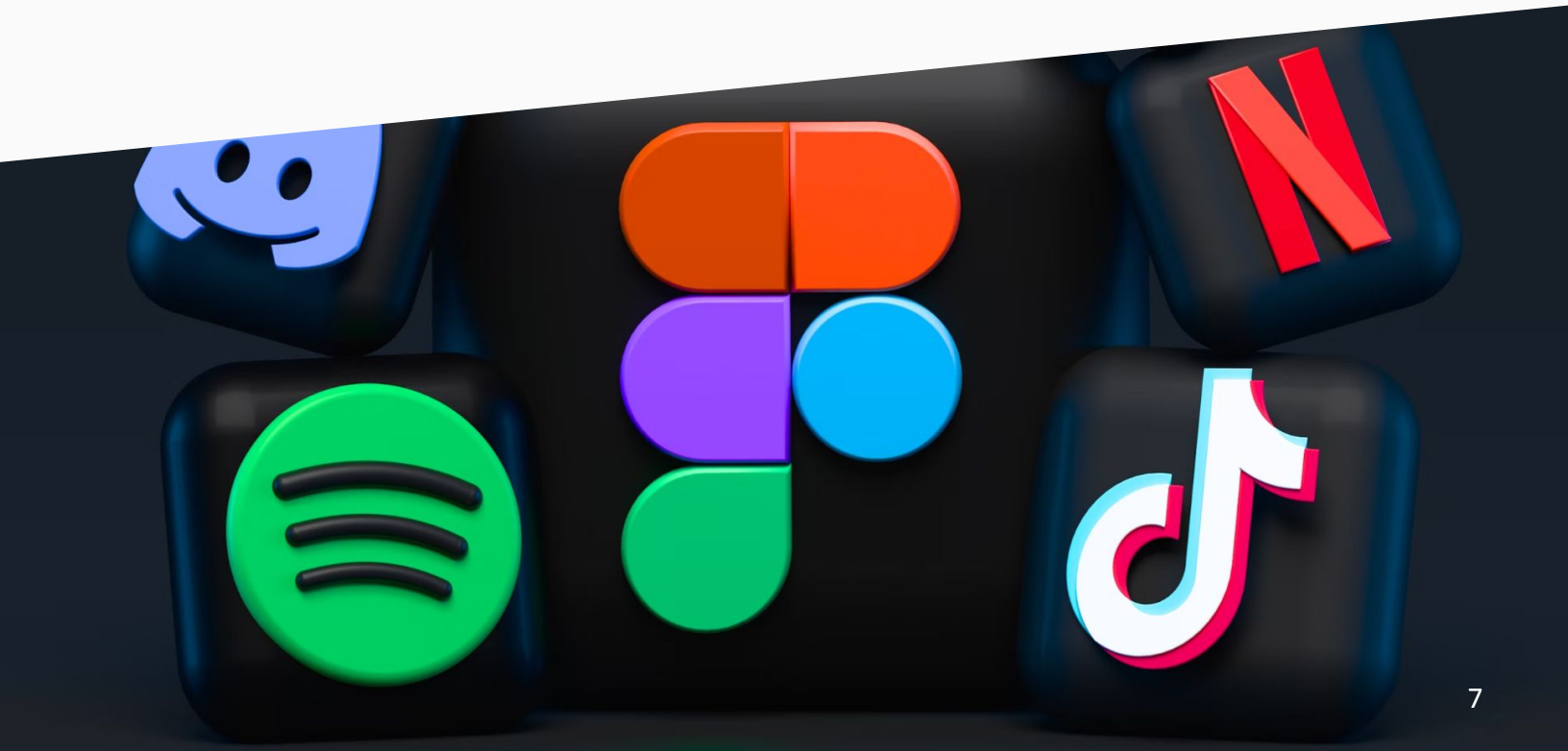
Wenn Sie Gmail oder Google Drive verwenden, können die Inhalte Ihrer E-Mails und Dokumente von den Algorithmen von Google gescannt und analysiert werden, um die Werbezielgruppen zu verbessern. Google sammelt auch Textnachrichten- und Anrufdaten von Android-Nutzern ohne Zustimmung.

Quelle: "What Data Do The Google Dialer and Messages Apps On Android Send to Google?", Prof. Douglas Leith, Trinity College, Dublin, 2022.

Wie Google Benutzerdaten sammelt und verwendet

Google-Apps und Android

Die meisten Android-Telefone sind in das Google-Ökosystem eingebunden, was bedeutet, dass jede Interaktion mit Ihrem Telefon (wie das Öffnen von Apps, die Nutzung der Kamera oder Sprachbefehle) gesammelt werden kann.
Die Google Play-Dienste verfolgen, wie und wann Sie Apps und Websites nutzen, wodurch Google Zugriff auf umfassende Verhaltensdaten erhält.



Apples Ansatz zur Datenerfassung

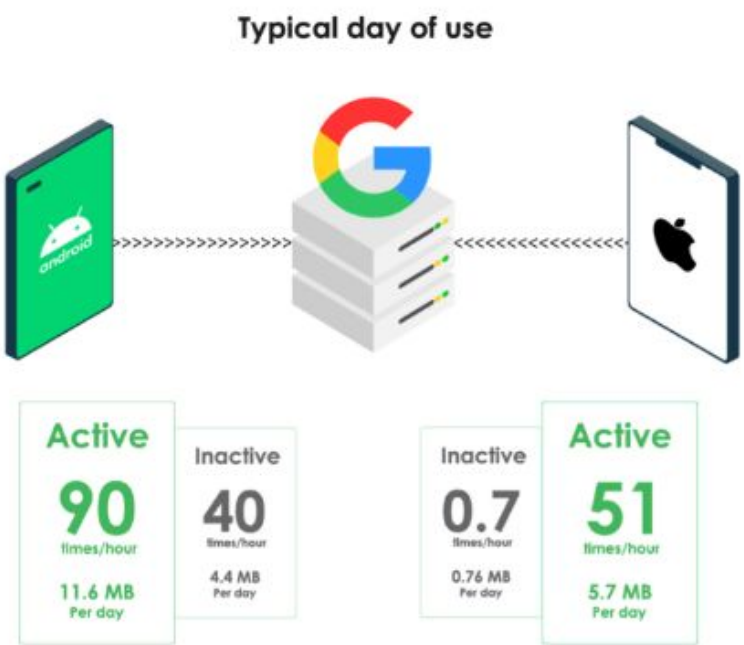
Obwohl Apple sich als privatsphärenorientierteres Unternehmen vermarktet, beteiligt es sich ebenfalls an einer bedeutenden Datenerfassung. Apple sammelt zwar nicht so viele Daten passiv wie Google, sammelt jedoch Informationen über seine Dienste wie den App Store, iCloud und Apple Health.

Apple erhält auch mehr als 25 Milliarden Dollar pro Jahr von Google, um Google Search zur Standardsuchmaschine für iOS-Geräte zu machen.

Gesammelte Datenmengen:

- Ein Android-Telefon im Leerlauf übermittelt täglich zwischen 4,4 MB und 11,6 MB persönliche Daten an Google.
- Ein Apple-Gerät sendet täglich zwischen 0,76 MB und 5,7 MB Daten an Google.

Quelle: Bericht der Vanderbilt University.



Folgen der Datenerfassung durch Google und Apple

Die massive Datenerfassung durch Google und Apple ermöglicht es diesen Unternehmen, äußerst detaillierte Profile von Einzelpersonen zu erstellen, einschließlich ihres Standortverlaufs, ihrer Suchverläufe, Kommunikationsgewohnheiten und Online-Einkäufe. Dies wirft erhebliche Bedenken hinsichtlich der Privatsphäre auf:

- **Überwachungswirtschaft:** Mit solch umfassenden Daten kann Google (und ähnliche Technologieunternehmen) unsere Online-Erfahrungen gestalten, den Inhalt einschränken, den wir sehen, und unsere Entscheidungen beeinflussen, sei es beim Einkaufen, bei politischen Präferenzen oder im täglichen Leben.

- **Verhaltensmanipulation:** Mit seinen präzisen Einblicken in das Benutzerverhalten kann Google seine Daten nutzen, um nicht nur die Werbung zu beeinflussen, die Benutzer sehen, sondern möglicherweise auch, was sie denken oder fühlen, was ernsthafte Risiken für die Autonomie birgt.

- **Datenverletzungen:** Je mehr Daten ein Unternehmen sammelt, desto attraktiver wird es für Hacker. Datenverletzungen bei Unternehmen wie Google können dazu führen, dass persönliche Informationen offengelegt werden.

Wie mobile Apps Werbung und Echtzeitauktionen nutzen, um Benutzer zu verfolgen

Neben Google und Apple beteiligen sich viele mobile Anwendungen weltweit an invasiven Verfolgungspraktiken, oft ohne dass die Benutzer vollständig informiert sind. Wie Apps Benutzer verfolgen:

- **Werbe-IDs:** Mobile Geräte verfügen über eindeutige Kennungen, wie Apples IDFA (Identifier for Advertisers) oder Googles Advertising ID, die es Apps ermöglichen, Benutzer plattformübergreifend zu verfolgen. Diese IDs werden verwendet, um gezielte Werbung zu schalten.

- **Echtzeitauktionen (RTB):** RTB ist ein automatisiertes Auktionssystem, bei dem Werbetreibende in Echtzeit bieten, um Anzeigen an bestimmte Benutzer zu schalten. Wenn Sie eine App oder Website öffnen, erhalten Werbetreibende sofort Informationen über Sie – wie Ihren Standort, Ihr Gerät und Ihr vorheriges Verhalten – und geben Gebote ab, um Anzeigen zu schalten. Dieser Prozess findet Millionen Mal pro Sekunde statt.

Folgen der Verfolgung durch mobile Apps und Echtzeitauktionen

Die durch mobile Apps und Echtzeitauktionen gesammelten Daten stellen erhebliche Bedrohungen für die Privatsphäre der Benutzer dar:

- **Gezielte Manipulation:** Die über RTB gesammelten Daten ermöglichen es Werbetreibenden, hochgradig gezielte und personalisierte Anzeigen zu erstellen. Während dies die Relevanz von Anzeigen verbessern kann, ermöglicht es Werbetreibenden (oder politischen Gruppen) auch, das Verhalten der Benutzer durch die Bereitstellung von spezifischen, emotional aufgeladenen Inhalten zu manipulieren.

- **Ständige Überwachung:** Apps können Ihren Standort, Ihre App-Nutzung und Ihr Browsing-Verhalten in Echtzeit verfolgen, oft ohne Ihre Zustimmung. Dies führt zu einer ständigen Überwachung Ihres digitalen Lebens.

- **Datenmakler und Erosion der Privatsphäre:** Die über RTB gesammelten Daten werden häufig mit Drittanbietern geteilt, die umfassende Profile von Benutzern erstellen können. Diese Datenmakler verkaufen Ihre Daten an Werbetreibende, Regierungen oder andere Stellen, was Ihre Privatsphäre weiter untergräbt.

Tipps zum Schutz vor digitaler Überwachung

Glücklicherweise gibt es mehrere Schritte, die Sie unternehmen können, um sich vor digitaler Überwachung zu schützen:

- **Standortverfolgung deaktivieren:** Deaktivieren Sie die Standortdienste für Apps, die sie nicht benötigen, und verwenden Sie ein VPN, um Ihre IP-Adresse zu maskieren.
- **Werbe-Tracker blockieren:** Verwenden Sie Browsererweiterungen, die sich auf den Datenschutz konzentrieren. Deaktivieren Sie Werbe-IDs auf Android und iOS. Das Blockieren von Trackern in Apps und im Web ist auch eine Standardfunktion in /e/OS.
- **App-Berechtigungen minimieren:** Überprüfen Sie regelmäßig die App-Berechtigungen und widerrufen Sie den Zugriff auf Daten, die für die Kernfunktionen der App nicht erforderlich sind.
- **Verwenden Sie alternative Apps:** Ersetzen Sie so viele Google-Apps und -Dienste wie möglich, insbesondere Gmail und Google-Suche.
- **End-to-End-Verschlüsselung verwenden:** Entscheiden Sie sich für Messaging-Apps wie Signal, Matrix/Element oder Threema, die End-to-End-Verschlüsselung bieten und sicherstellen, dass Ihre Kommunikation privat bleibt. Verwenden Sie E-Mail-Dienste, die vollständige End-to-End-Verschlüsselung wie ProtonMail bieten.
- **Erwägen Sie datenschutzorientierte Geräte:** Murena-Smartphones mit /e/OS sind so konzipiert, dass sie Ihre Privatsphäre schützen, indem sie die Tracking-Mechanismen von Google und Werbe-Tracker vermeiden.

Sicherheit ist NICHT gleich Privatsphäre!

In der heutigen digitalen Landschaft gibt es oft Verwirrung zwischen Sicherheit und Privatsphäre. Obwohl beide wichtig sind, dienen sie unterschiedlichen Zwecken:

- Sicherheit konzentriert sich darauf, Systeme und Daten vor unbefugtem Zugriff zu schützen.
- Privatsphäre zielt darauf ab, die Sammlung und Weitergabe personenbezogener Daten von Anfang an zu begrenzen.

Ein Gerät kann sicher sein und dennoch Ihre Privatsphäre gefährden, da Sicherheit keine Datenerfassung oder Überwachung durch den Systeminhaber verhindert.

Beispiele:

- **Pegasus-Spyware auf iPhones:** Trotz des Rufs von iPhones als sicher wurden Schwachstellen von Pegasus ausgenutzt, um hochrangige Ziele wie einen europäischen Präsidenten und Aktivisten ohne Benutzereingriff zu hacken.
- **Hacking durch russische Geheimdienste:** Während des Krim-Konflikts wurden Smartphones ukrainischer Soldaten gehackt, wodurch Gegner ihre Bewegungen verfolgen und Kommunikation abfangen konnten, trotz der Verwendung militärischer Verschlüsselung.
- **EncroChat und kriminelle Netzwerke:** Verschlüsselte Telefone, die von kriminellen Netzwerken wie EncroChat verwendet wurden, wurden von europäischen Strafverfolgungsbehörden gehackt, was zur Verhaftung vieler Krimineller führte, obwohl die Telefone als "unhackbar" galten.

Wie Murena und /e/OS die Privatsphäre der Benutzer schützen

Im Gegensatz zu den großen mobilen Betriebssystemen wie Googles Android und Apples iOS sammelt /e/OS praktisch keine persönlichen Daten von seinen Benutzern. Laut einer Studie hebt sich /e/OS als das datenschutzfreundlichste System unter verschiedenen Android-basierten Plattformen wie Samsung, Xiaomi und Huawei hervor.

- **Keine Daten an Google gesendet:** Im Gegensatz zu anderen Android-Varianten, die ständig mit Google-Servern kommunizieren, vermeidet /e/OS jegliche Verbindung zu Google-Diensten. Dadurch wird die automatische Sammlung sensibler Daten wie Standortverlauf, Suchanfragen und Gerätenutzung verhindert.

- **Minimale Datenerfassung:** Die Entwickler von /e/OS haben das System so konzipiert, dass es mit nahezu keiner Datenübertragung funktioniert, selbst wenn das Gerät im Leerlauf ist. Es gibt keine Übertragung von Gerätekennungen, Benutzerinteraktionen oder App-Nutzungsdaten, was bei anderen Android-Varianten üblich ist.

Fazit

In der heutigen digitalen Welt werden unsere persönlichen Daten zunehmend über mobile Apps und Webplattformen gesammelt. Große Akteure wie Google und Apple sammeln riesige Mengen an Benutzerdaten, was erhebliche Risiken birgt, da das Verhalten und die Präferenzen der Benutzer verfolgt und oft ohne deren klare Zustimmung verkauft werden.

Um Ihre Privatsphäre zu schützen:

- Deaktivieren Sie Standortverfolgung und verwenden Sie ein VPN.
- Ersetzen Sie Google-Dienste durch datenschutzfreundliche Alternativen.
- Bevorzugen Sie Messaging-Apps mit End-to-End-Verschlüsselung.
- Erwägen Sie Murena-Smartphones mit /e/OS, die so konzipiert sind, dass sie Ihre Privatsphäre schützen.