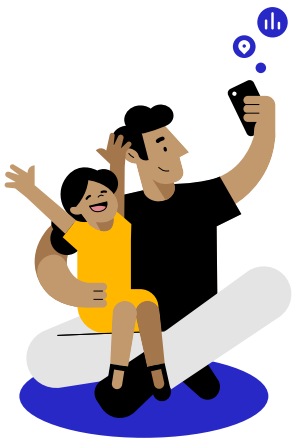


Ein Tag im Leben deiner Daten

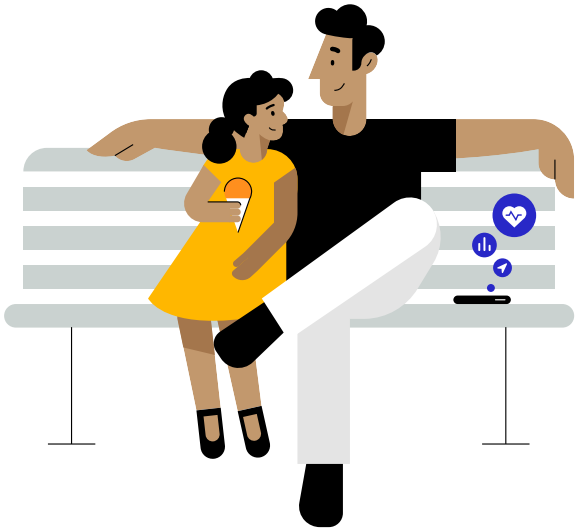
Der Vater-Tochter-Tag auf dem Spielplatz

April 2021

„Ich bin überzeugt davon, dass die Menschen intelligent sind, und dass manche bereit sind, mehr Daten zu teilen als andere. Fragt sie einfach danach. Fragt sie jedes Mal. Lasst sie euch sagen, wann sie nicht mehr gefragt werden wollen. Und lasst sie genau wissen, was mit ihren Daten gemacht wird.“

Steve Jobs

All Things Digital Conference, 2010



Im Laufe des letzten Jahrzehnts hat eine große und undurchschaubare Branche immer mehr personenbezogene Daten angehäuft.[1,2] Ein komplexes Ökosystem aus Websites, Apps, Unternehmen der sozialen Medien, Datenbrokern und Adtech Anbietern, die Benutzer:innen online und offline verfolgen und ihre persönlichen Daten sammeln. Diese Daten werden zusammengetragen, geteilt, zusammengefasst und für Echtzeit-Auktionen genutzt, wodurch eine Branche mit einem Umsatz von 227 Milliarden US-Dollar pro Jahr entstanden ist.[1] Das geschieht täglich im Alltag der Menschen, oft ohne ihr Wissen oder ihr Einverständnis.[3,4] Wir zeigen hier am Beispiel eines Vaters und seiner Tochter, was diese Branche über die beiden in Erfahrung bringt, während sie einen Tag im Park verbringen.

Schon gewusst?

In Apps, die du jeden Tag nutzt, sind Tracker integriert: eine durchschnittliche App hat 6 Tracker.[3] In den meisten beliebten Apps für Android und iOS sind Tracker integriert.[5,6,7]

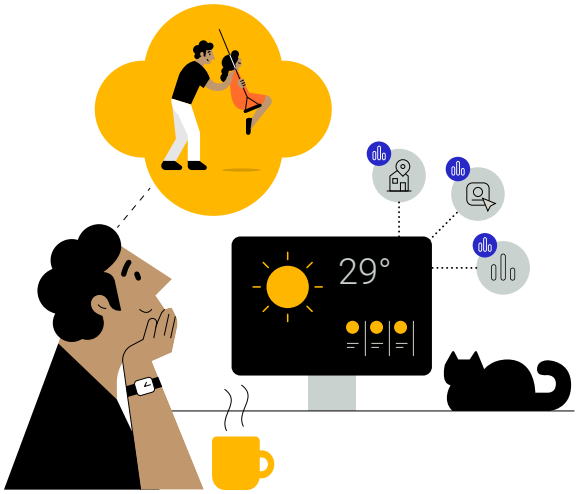
Die Tracker sind oft in Code von anderen Anbietern integriert, der Entwicklern bei der Erstellung ihrer Apps hilft. Durch die Integration von Trackern erlauben die Entwickler anderen Anbietern, Daten, die du mit ihnen geteilt hast, über verschiedene Apps hinweg und zusammen mit anderen Daten, die über dich gesammelt wurden, zu erfassen und zu verknüpfen.

Datenbroker sammeln, verkaufen und lizenzieren die persönlichen Daten bestimmter Personen, zu denen sie keine direkte Beziehung haben, oder geben sie anderweitig an andere Anbieter weiter.[3]

Hunderte von Datenbrokern sammeln online und offline Daten.[8] Ein Broker sammelt Daten von 700 Millionen Verbraucher:innen weltweit und erstellt Verbraucherprofile mit bis zu 5.000 Merkmalen.[9]

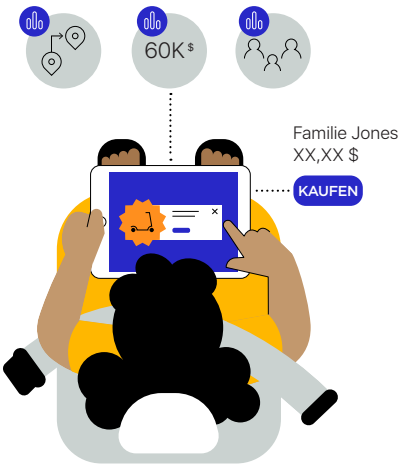
Eine Studie zeigt, dass in fast 20 % der Apps für Kinder persönliche Daten durch die Entwickler gesammelt und geteilt werden, ohne nachweisbare Einwilligung der Eltern.[10]

Jeden Tag und zu jeder Stunde werden Benutzer:innen Milliarden von digitalen Anzeigen online angezeigt.[11,12,13] In den Millisekunden, in denen eine Anzeige geladen wird, findet eine Echtzeit-Auktion statt, bei der Werbetreibende für den Werbeplatz bieten. Dafür werden häufig getrackte persönliche Daten über die Person verwendet.[14,15]



John will den Tag mit seiner Tochter im Park verbringen

John und seine 7-jährige Tochter Emma verbringen den Tag zusammen. Am Morgen schaut John auf seinem Computer nach dem Wetter, liest die Nachrichten und überprüft in einer Karten App auf seinem Smartphone die Verkehrslage für den Ausflug zum Spielplatz, der neben der Schule seiner Tochter liegt. Während der Fahrt sammeln und verfolgen im Hintergrund 4 Apps auf seinem Smartphone in regelmäßigen Abständen seine Standortdaten.[16,17,18] Nachdem die Daten vom Gerät abgerufen wurden, verkaufen die App Entwickler sie an eine Reihe unbekannter Datenbroker anderer Anbieter, von denen John noch nie etwas gehört hat.[16,17] Obwohl die Standortdaten angeblich anonym gesammelt werden, ermöglicht die Benutzerverfolgung den Datenbrokern, Johns Standortverlauf aus diesen Apps mit Daten abzugleichen, die aus seiner Nutzung anderer Apps gesammelt wurden.[16,19] Dadurch können die in verschiedenen Apps und aus mehreren Quellen verfolgten Daten von jedem Unternehmen oder jeder Organisation erworben werden, um ein umfassendes Profil über ihn zu erstellen, das seine täglichen Aktivitäten genau beschreibt.[3,16]



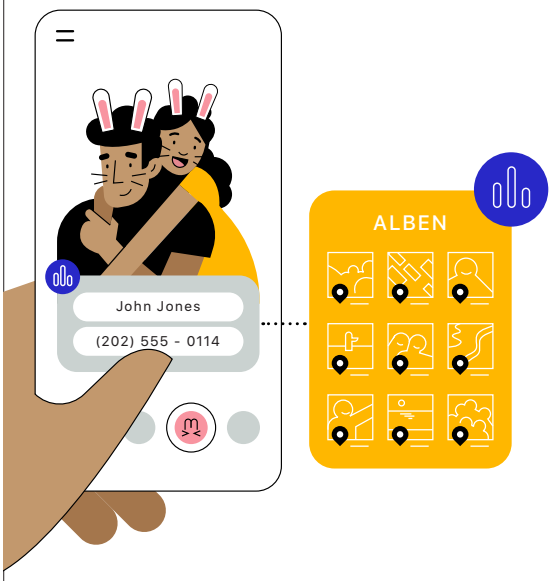
Emma spielt auf der Fahrt zum Park ein Spiel

Auf der Fahrt zum Spielplatz erlaubt John seiner Tochter, ein Spiel auf seinem Tablet zu spielen. Als sie die App öffnet, sieht sie eine Anzeige für einen Tretroller – und das ist kein Zufall. In dem Sekundenbruchteil, in dem die App geladen wurde, fand eine Auktion um den Werbeplatz statt.[14] Durch Zwischenhändler hat der Werbepartner der Tretrollerfirma von der verfügbaren Anzeige erfahren.[15] Dann wurde aufgrund der über John und Emma gesammelten persönlichen Daten auf die Anzeige geboten.[15] Der Werbepartner der Tretrollerfirma sammelt weitere Daten über Johns und Emmas Verhalten, nachdem sie die Anzeige gesehen haben, um festzustellen, ob sie darauf geklickt oder den Tretroller gekauft haben.[3] Und sie werden John und Emma weiterhin auf jede erdenkliche Art Werbung für den Tretroller zeigen, indem sie ihnen über verschiedene Apps und Websites auf allen Geräten von John folgen.[3,20,21]

Einige Apps fordern den Zugriff auf mehr Daten an, als für ihre Dienstleistung erforderlich sind, wie zum Beispiel eine Tastatur App, die genauen Zugriff auf den Standort verlangt.[5]

Die Daten können an Werbe-netzwerke, Werbeverlage, Attributionsanbieter und Anbieter von Messungen, Datenbroker, andere Unternehmen und sogar staatliche Organisationen weitergegeben werden.[3,15,40,41,42] Unternehmen im Bereich der sozialen Medien und der Anzeigen-technologie müssen entweder mit Geldstrafen in Millionenhöhe rechnen oder haben bereits solche gezahlt, weil sie personenbezogene Daten für Zwecke verwendet haben, die sie den Benutzer:innen zum Zeitpunkt der Erhebung nicht mitgeteilt hatten.[22,23,24,25]

Datenbroker weisen Benutzer:innen anhand der gesammelten Daten Attribute zu und gruppieren sie in äußerst detaillierte Marktsegmente, wie zum Beispiel Personen, die „abnehmen wollen, aber trotzdem Bäckereien lieben".[26] Doch diese Profile sind oft falsch: Eine Studie ergab, dass über 40 % der Attribute ungenau sind.[27,28]

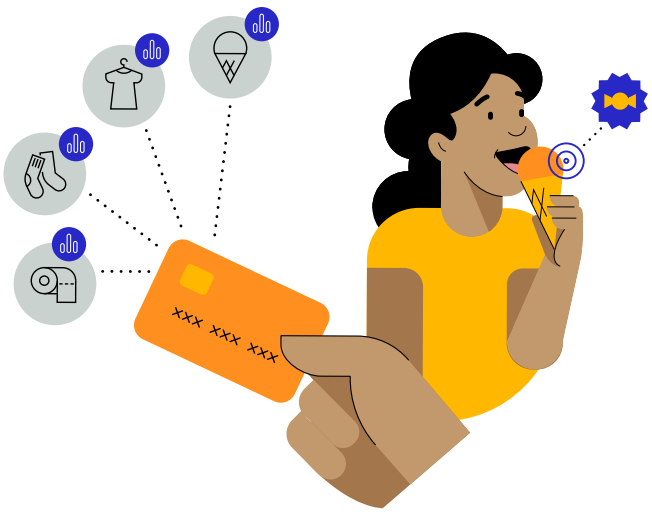


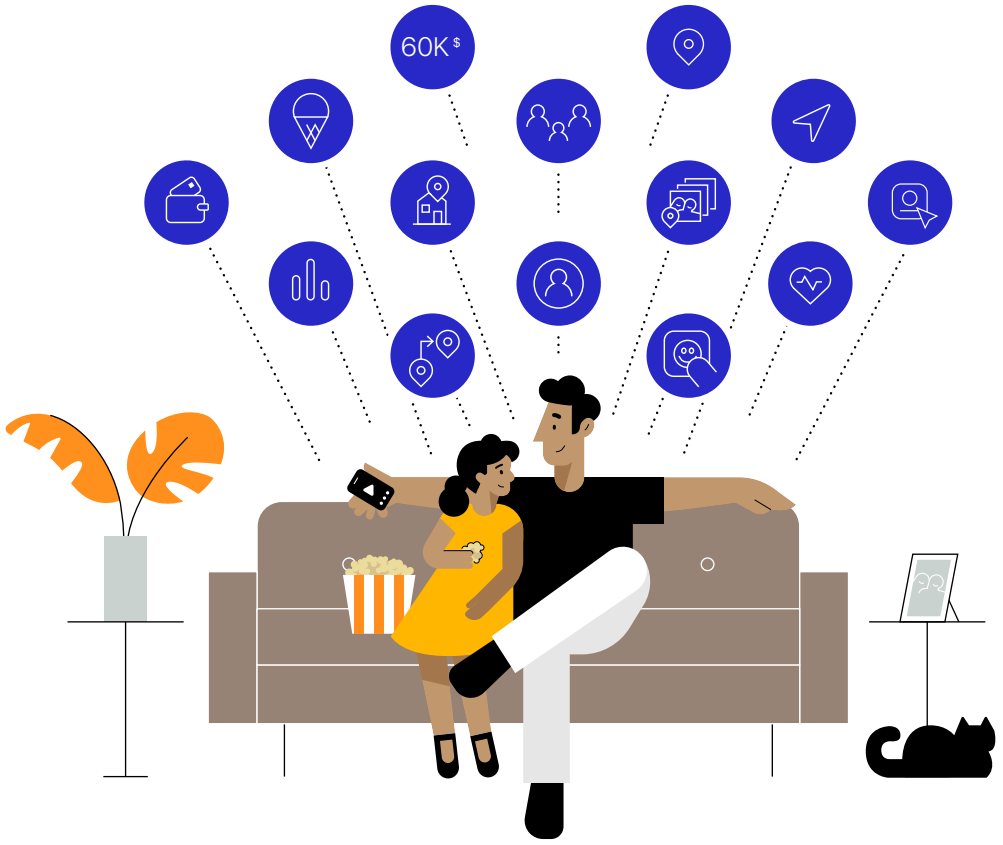
John und Emma machen im Park ein Selfie

Etwas später machen John und Emma auf dem Spielplatz ein Selfie. Sie probieren eine Fotofilter App aus und entscheiden sich für einen Filter mit Hasenohren. Die Filter App kann jedoch auf alle Fotos auf dem Gerät und die dazugehörigen Metadaten zugreifen, und nicht nur auf das Selfie vom Spielplatz.[29,30] John postet das Bild in einer App für soziale Medien. Die App verknüpft Johns aktuelle Online-Aktivitäten mit einer Fülle von Daten, die von anderen Apps gesammelt wurden, wie seine demografischen Daten und Kaufgewohnheiten, wobei eine E-Mail Adresse, eine Telefonnummer oder eine Werbekennung verwendet wird.[3]

Ein Halt an der Eisdiele auf dem Heimweg

Auf dem Nachhauseweg halten John und Emma an, um sich ein Eis zu holen. John bezahlt für das Eis mit einer Kreditkarte, und dem umfangreichen Datenprofil über seine Vorlieben werden weitere Daten hinzugefügt: der Standort der Eisdiele und wie viel er ausgegeben hat.[31,32,33] Eine der Apps, die Johns Standort verfolgen, kann feststellen, dass John und Emma auch in einem Spielzeugladen vorbeigeschaut haben.[3] Die Daten über die Orte, wo die Familie im Laufe des Tages eingekauft hat, werden an Datenbroker weitergegeben, die sie mit dem Wissen kombinieren, dass er ein kleines Kind hat, um auf Johns Geräte gezielt Werbung für Süßigkeiten und den besuchten Spielzeugladen zu schalten.[17]





Am Ende des Tages haben eine Reihe von Unternehmen, mit denen John noch nie interagiert hat, überall auf der Welt ihre Profile mit den Daten über ihn und seine Tochter aktualisiert. Diese Unternehmen wissen, wo sich das Haus der Familie befindet, welchen Park sie besucht haben, welche Nachrichten-Websites sie gelesen haben, welche Produkte sie sich angesehen haben, welche Werbung sie gesehen haben, welche Geschäfte sie besucht haben und kennen ihre Kaufgewohnheiten.[3,34] Diese Daten wurden in mehreren Apps gesammelt und getrackt, die John und seine Tochter im Laufe des Tages benutzt haben, stammen aber auch aus anderen Quellen. John weiß nicht, wie viele Daten im Laufe des Tages gesammelt wurden, er hatte nicht immer Kontrolle darüber und hat sein Einverständnis gegeben, ohne es zu wissen.[3,4] Während die Familie auf einer App in ihrem Smart TV nach einem Kinderfilm suchen, um den Abend ausklingen zu lassen, wiederholt sich der Kreislauf aus Tracking, Datenaustausch, Auktionen und Retargeting unaufhaltsam.[35,36]

Die Datenschutzrichtlinien von Apple

Apple ist davon überzeugt, dass Datenschutz ein grundlegendes Menschenrecht ist. Wir entwickeln unsere Produkte und Services nach vier wichtigen Datenschutzrichtlinien:

Datenminimierung

Nur das Minimum an Daten sammeln, das erforderlich ist, um einen bestimmten Service zu liefern.

On-Device Verarbeitung

Die Daten werden, wo immer das möglich ist, auf dem Gerät verarbeitet, anstatt sie an Apple Server zu senden, um die Privatsphäre der Benutzer:innen zu schützen und das Sammeln von Daten zu minimieren.

Transparenz und Kontrolle für Benutzer:innen

Es ist immer sichergestellt, dass Benutzer:innen wissen, welche Daten weitergegeben und wie sie verwendet werden, und dass sie die Kontrolle darüber haben.

Sicherheit

Hardware und Software arbeiten zusammen, um Daten zu schützen.

Diese vier Richtlinien waren immer die Grundlage für das Ziel von Apple, dass alle Benutzer:innen die Möglichkeit haben sollen, ihre Daten so zu teilen, wie sie es wollen. Deshalb hat Apple in den letzten zwei Jahrzehnten kontinuierlich Innovationen eingeführt, um die Privatsphäre der Benutzer:innen bei allen Produkten und Services zu schützen. So nutzen wir zum Beispiel On-Device Intelligenz und andere Features, um möglichst wenige Daten in unseren Apps, Browsern und Online-Services zu erfassen. Außerdem erstellen wir kein umfassendes Benutzerdatenprofil für alle unsere Apps und Services.

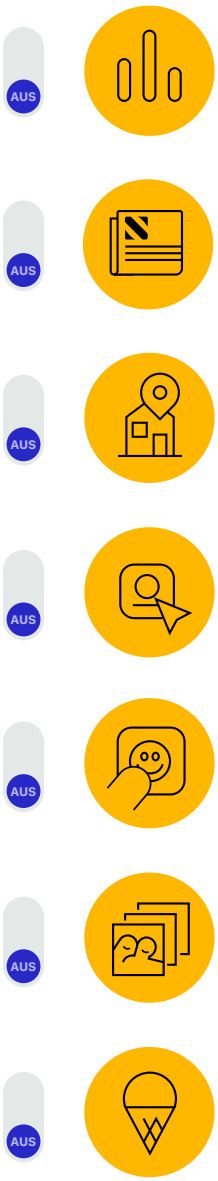
Weitere Infos zu den neuen Datenschutzfeatures von Apple und den Features, mit denen Apple deine Privatsphäre schützt, gibt es unter apple.com/de/privacy.

Weitere Infos dazu, wie Safari deine Daten schützt, findest du im Safari White Paper.

Weitere Infos dazu, wie Apple deine Standortdaten schützt, findest du im White Paper zu Ortungsdiensten.

Die Datenschutzfeatures von Apple geben John mehr Transparenz und Kontrolle über seine Daten

Die Geschichte von John und Emma zeigt die Probleme mit Datenschutz und die Lösungen, an denen wir bei Apple arbeiten.



John will den Tag mit seiner Tochter im Park verbringen

Hätte sich John das Wetter auf seinem Computer mit dem Safari Browser angesehen, wäre seine Aktivität durch den intelligenten Tracking-Schutz standardmäßig nicht verfolgt worden.

Hätte John die Nachrichten am Morgen mit Apple News gelesen, würde Apple ihm Inhalte basierend auf seinen Interessen anzeigen, ohne zu wissen, wer er ist, oder zu erfahren, was er liest.

Hätte John mit Apple Karten den Verkehr überprüft, wären seine Standortdaten mit einer Zufallskennung verknüpft worden, die regelmäßig zurückgesetzt wird und nicht mit John verbunden ist. Dadurch würde niemand außer John wissen, wo er gerade ist.

Auf einem iPhone würde John in regelmäßigen Abständen daran erinnert werden, welche Apps im Hintergrund auf seinen Standort zugreifen. Bevor er seinen Standort mit einer App teilt, kann John wählen, ob er seinen Standort nur ungefähr oder nur einmal teilen möchte.

Emma spielt auf der Fahrt zum Park ein Spiel

Auf einem iPad könnte John mit dem bald verfügbaren App Tracking Transparenz Feature selbst entscheiden, ob das Spiel Emmas Aktivitäten in Apps und auf Websites von anderen Unternehmen tracken darf.

Werbenetzwerke, die die SKAdNetwork API von Apple verwenden, könnten die Gesamtwirkung ihrer Werbung messen, ohne Zugriff auf Daten zu erhalten, die zu Johns Gerät zurückverfolgt werden könnten.

John und Emma machen im Park ein Selfie

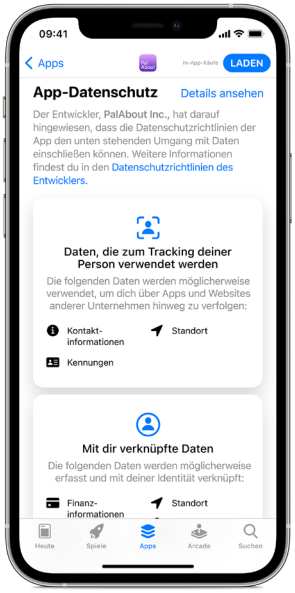
Auf einem iPhone hätte John die Wahl gehabt, der Filter App nur Zugriff auf das Selfie zu geben, statt auf die gesamte Fotomediathek.

Ein Halt an der Eisdiele auf dem Heimweg

Wenn John das Eis mit der Apple Card gekauft hätte, könnte seine Bank seine Transaktionsdaten nicht für Marketingzwecke nutzen. Mit Apple Pay hätte Apple die On-Device Intelligenz genutzt. So hätte John seinen Transaktionsverlauf auf seinem iPhone einsehen können, ohne dass Apple Daten darüber erhält, wo er eingekauft hat, was er gekauft hat oder wie viel er ausgegeben hat.

Letztendlich geben die Produkte und Datenschutzfeatures von Apple John im Laufe des Tages mehr Transparenz und Kontrolle darüber, wie viele seiner Daten weitergegeben und verwendet werden.

App Tracking Transparenz und die neuen Infos zum Datenschutz im App Store



Apple macht den nächsten Schritt, um die Daten der Benutzer:innen im App Ökosystem zu schützen. Da eine komplexe und wachsende Anzahl von Unternehmen auf persönliche Verbraucherdaten zugreift, sie verfolgt und monetarisiert, führt Apple zwei neue Features ein, die den Benutzer:innen mehr Transparenz, Sichtbarkeit und Wahlmöglichkeiten geben sollen. So können sie informierte Entscheidungen treffen und ihre Privatsphäre besser kontrollieren.

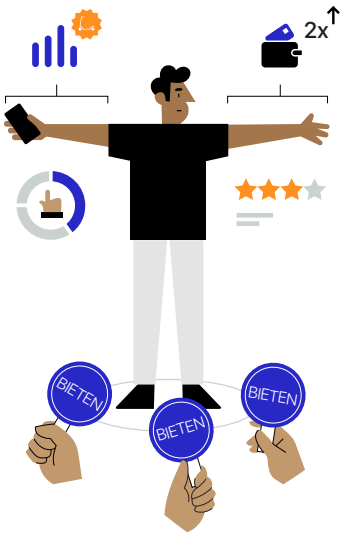
Die App Tracking Transparenz startet bald mit unserem nächsten Beta Update und macht es erforderlich, dass Apps die Erlaubnis der Benutzer:innen einholen, bevor sie persönliche Daten in Apps oder auf Websites von anderen Anbietern verfolgen. In den Einstellungen können Benutzer:innen sehen, welche Apps die Erlaubnis zum Tracken angefordert haben, und sie beliebig anpassen. Diese Voraussetzung wird am Anfang des Frühjahrs mit der nächsten Version von iOS 14, iPadOS 14 und tvOS 14 eingeführt und wird schon jetzt von Datenschützern auf der ganzen Welt unterstützt. Apple hat dieses Feature entwickelt, um Benutzer:innen mehr Transparenz und Kontrolle zu geben. Gleichzeitig sollte Werbung weiterhin als angemessenes und praktikables Mittel zur Unterstützung von Apps und Webinhalten ermöglicht werden. Die Einführung früherer Features, wie der intelligente Tracking-Schutz von Safari, hat gezeigt, dass Werbung weiterhin erfolgreich sein kann, und gleichzeitig die Privatsphäre der Benutzer:innen besser geschützt wird. Mit App Tracking Transparenz können Benutzer:innen besser entscheiden, welche Apps sie nutzen und was sie diesen Apps erlauben. Und mit App Tracking Transparenz können sie jetzt außerdem wählen, ob sie den Apps erlauben, sie zu tracken oder nicht. Bei Apps, denen Benutzer:innen vertrauen und die Erlaubnis zum Tracken erteilen, können Entwickler das weiterhin tun.

Zusätzlich zu der erforderlichen Benutzererlaubnis zum Tracking hat Apple für mehr Transparenz vor kurzem auch die Produktseiten im App Store geändert. Im neuen Bereich für den App Datenschutz im App Store können Benutzer:innen einige der Datenschutzpraktiken einer App besser verstehen. Jede Produktseite einer App muss Benutzer:innen eine übersichtliche Zusammenfassung der Datenschutzpraktiken der Anbieter geben. Die Seiten mit detaillierten Angaben enthalten Infos zu den von der App gesammelten Datentypen, wie Fotos, Standort- und Kontaktdaten. Auf diesen Seiten finden Benutzer:innen auch weitere Infos darüber, wie die einzelnen Datenarten von den App Entwicklern verwendet werden, auch ob sie zum Tracking verwendet werden und ob die Daten mit den jeweiligen Benutzer:innen verknüpft sind. Alle App Entwickler, auch Apple, sind verpflichtet, selbst Angaben zu ihren Datenschutzpraktiken zu machen.

Durch die neuen Einstellungen zum App Tracking und die Informationen zu Transparenz und Datenschutz auf den Produktseiten im App Store können Benutzer:innen einfacher erfahren, wie ihre persönlichen Daten verwendet werden, und so bisher undurchschaubare und unsichtbare Praktiken erkennen und mehr Kontrolle über ihre Daten ausüben.

Apple wird weiterhin innovative Technologien für den Datenschutz entwickeln und an neuen Möglichkeiten arbeiten, um persönliche Daten zu schützen.

Ein Tag im Leben einer Anzeige



Anzeigenauktionen

Es ist kein Zufall, dass Emma auf Johns Display eine Anzeige für einen Tretroller gesehen hat. Werbetreibende bieten in einer Auktion, um ihre Anzeige auf dem Gerät anzuzeigen.[37] Hier ist eine vereinfachte Erklärung, wie in einem Bruchteil einer Sekunde die Anzeige auf dem Display des Geräts ausgewählt wurde:

1.
Die Entwickler der App, die Emma nutzt, beauftragen ein Adtech Unternehmen, das den Werbeplatz in Echtzeit versteigert.[14]

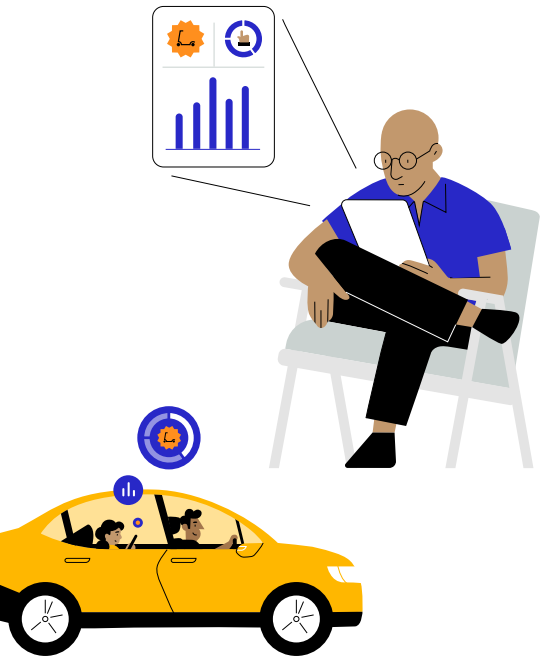
2.
Wenn Emma die App öffnet, sammelt das Werbenetzwerk Daten über die Nutzung von Johns Gerät (zum Beispiel, welche App genutzt wird, den Standort und Johns Werbekennung). Dazu kommen Daten von anderen Anbietern, die mit Johns Werbekennung oder anderen Daten arbeiten, die Tracking ermöglichen.[3]

3.
Das Werbenetzwerk teilt einige dieser Daten, speziell die Werbekennung, mit potenziellen Werbekunden. Bevor sie ein Gebot abgeben, versuchen Werbetreibende normalerweise, so viel wie möglich über den Benutzer oder die Benutzerin zu erfahren, sowohl aus ihren eigenen Daten als auch aus persönlichen Daten, die über Tracking und die Erstellung von Profilen gesammelt und zusammengefasst werden.[3,15]

4.
Je mehr Merkmale von John und Emma – die aus ihren Daten abgeleitet werden – mit der Zielgruppe des Werbetreibenden übereinstimmen, desto mehr werden die Werbetreibenden für den Werbeplatz bieten.[15,38]

5.
Die Anzeige des Gewinnergebots für einen Tretroller wird auf dem Gerät angezeigt, das Emma benutzt.[14]

Da die Anzeigenauktion in einem Bruchteil einer Sekunde abläuft, sammeln, teilen und nutzen sowohl Käufer als auch Verkäufer persönliche Daten, um für Werbeplätze und Anzeigen zu bieten.[14,15]



Anzeigenattribution

Nachdem die Anzeige Emma angezeigt wurde, wollen die Werbeunternehmen der Tretrollerfirma deren Wirkung auf Emmas Verhalten messen. Dieser Vorgang wird Anzeigenattribution genannt.

Dafür versucht der Werbetreibende, Emmas Verhalten auf dem Gerät zu verfolgen, um Daten darüber zu sammeln, was sie im Internet und in Apps macht. Und sogar, wann sie offline geht.

- **Wenn die Anzeige für ein Produkt ist,** könnte der Werbetreibende versuchen zu tracken, ob Benutzer:innen später seine Website oder das Ladengeschäft besucht haben, um es zu kaufen.[3]
- **Wenn die Anzeige für eine App ist,** könnte der Werbetreibende versuchen zu tracken, ob sie installiert wurde. Das nennt man App Installationsattribution.[39]

Werbetreibende nutzen Anzeigenattribution auch zur „Optimierung" ihrer Werbekampagne bei Gruppen, bei denen die Werbekampagne effektiver ist.[3]

Das muss aber nicht so sein. Werbetreibende können die Wirkung ihrer Werbekampagnen auf Gruppen messen, ohne Benutzer:innen zu tracken. Apple hat Tools entwickelt, die das ermöglichen und gleichzeitig die Privatsphäre der Benutzer:innen schützen:

SKAdNetwork zeigt Werbetreibenden, wie oft eine App installiert wurde, nachdem Anzeigen dafür gesehen wurden, damit Werbetreibende die Wirkung ihrer Werbekampagne messen können. Diese Informationen geben jedoch keine Daten auf Benutzer- oder Geräteebene weiter, damit Werbetreibende die Benutzer:innen nicht tracken können.

Private Click Measurement für Apps in iOS und iPadOS 14.5 macht es Werbetreibenden möglich, die Wirkung von Anzeigen, die Benutzer:innen auf eine Website leiten, zu messen. Gleichzeitig wird die Datenerfassung durch geräteinterne Verarbeitung minimiert. Nachdem auf eine Produktanzeige in einer App geklickt wurde, teilt der Browser selbst – mithilfe von Private Click Measurement – den Werbetreibenden mit, dass jemand auf ihre Anzeige geklickt hat und dass es zu einem bestimmten Ergebnis auf ihrer Website geführt hat, wie einem Besuch oder einem Kauf. Ohne ihnen Daten darüber zu geben, wer konkret auf die Anzeige geklickt hat.

Fragen und Antworten

Kann ich immer noch alle Funktionen der App nutzen, wenn ich „App Tracking ablehnen“ wähle?

Ja. App Entwickler können nicht von dir verlangen, dass du das Tracking erlaubst, um den vollen Funktionsumfang der App zu nutzen.

Was sind Kennungen und wie funktionieren sie?

Kennungen wie der „Identifier For Advertisers“ (IDFA) und die E-Mail Adresse helfen dabei, ein bestimmtes Gerät in einem Netzwerk zu identifizieren. Sie ermöglichen es Werbetreibenden außerdem, ein detailliertes Profil deiner Aktivität in verschiedenen Apps oder auf unterschiedlichen Websites zu erstellen, wenn sie deine Gerätekennung erfassen und deine Aktivität damit in Verbindung bringen.

Was ist der „Identifier For Advertisers“ (IDFA)?

Der „Identifier For Advertisers“ (IDFA) ist eine von dir kontrollierbare Kennung, die von iOS an jedes Gerät vergeben wird. Da es eine softwarebasierte Kennung ist, die nicht an die Hardware selbst gebunden ist, kannst du den IDFA mit der App Tracking Transparenz für eine bestimmte App sperren lassen. So hast du die Kontrolle über IDFA basiertes Tracking.

Kann Apple garantieren, dass eine App mich nicht trackt, wenn ich „App Tracking ablehnen“ wähle?

Wenn du „App Tracking ablehnen“ wählst, kann der Entwickler nicht auf die Kennung für Werbetreibende (IDFA) zugreifen, die häufig zum Tracking verwendet wird. Der App Entwickler ist außerdem verpflichtet, deine Entscheidung zu respektieren, auch außerhalb der Werbekennung. Das ist in den Richtlinien vorgeschrieben, denen der Entwickler zustimmt, wenn er seine App im App Store einreicht und anbietet. Wenn wir erfahren, dass ein Entwickler Benutzer:innen trackt, die nicht getrackt werden wollen, verlangen wir, dass diese Praktiken geändert werden, um deine Wahl zu respektieren. Andernfalls kann die App aus dem App Store entfernt werden.

Wenn ich mich mit meinen Account in den sozialen Medien bei einer App anmelde, kann das Unternehmen dieser sozialen Medien tracken, was ich in der App mache?

Das hängt davon ab, ob du der App erlaubt hast, dich zu tracken. Wenn du „App Tracking ablehnen“ wählst, sollte die App dich nicht in Apps oder auf Websites anderer Anbieter zu Werbezwecken verfolgen oder deine Daten mit einem Datenbroker teilen. Das bedeutet, dass sie deine Daten nicht an das Unternehmen dieser sozialen Medien weitergeben sollte, wenn sie für diesen Zweck verwendet werden.

Wie sorgt Apple dafür, dass die Informationen zum Datenschutz auf den Produktseiten im App Store korrekt sind?

Ähnlich wie bei der Altersfreigabe im App Store, melden die Entwickler ihre eigenen Datenschutz-praktiken. Wenn wir erfahren, dass Entwickler möglicherweise ungenaue Informationen bereitgestellt haben, arbeiten wir mit ihnen daran die Informationen zu korrigieren.

Was ist ein Datenbroker?

Im Grunde genommen ist ein Datenbroker ein Unternehmen, das regelmäßig die persönlichen Daten bestimmter Benutzer:innen, zu denen das Unternehmen keine direkte Beziehung hat, sammelt, verkauft, lizenziert oder anderweitig an andere Anbieter weitergibt. Datenbroker sind in einigen Ländern gesetzlich definiert.

Quellen

1. Florian Gröne, Pierre Péladeau, et al., „Tomorrow's data heroes", *Strategy+Business*, 19. Februar 2019.

2. David Reinsel, John Gantz, et al., „The Digitization of the World: From Edge to Core", *IDC*, November 2018.

3. Competition & Markets Authority, „Online platforms and digital advertising", 1. Juli 2020.

4. Paul Hitlin und Lee Rainie, „Facebook Algorithms and Personal Data", *Pew Research Center*, 16. Januar 2019.

5. AppCensus, „1,000 Mobile Apps in Australia: A Report for the ACCC", 24. September 2020.

6. Reuben Binns, Ulrik Lyngs, et al., „Third Party Tracking in the Mobile Ecosystem", *Proceedings of the 10th ACM Conference on Web Science*, 2018, S. 23-31.

7. MightySignal, „Most Used SDKs in Top 200 Free iOS Apps", mightysignal.com/top-ios-sdks.

8. State of California Department of Justice, „Data Broker Registry", oag.ca.gov/data-brokers.

9. Acxiom Corporation, 2018 Form 10-K, eingereicht am 25. Mai 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Irwin Reyes, Primal Wijesekera, et al., „Won't Somebody Think of the Children? Examining COPPA Compliance at Scale", *Proceedings on Privacy Enhancing Technologies*, Vol. 2018, No. 3, 2018, S. 63-83.

11. Jim Edwards, „Here's The Staggering Number of Ads Facebook Serves On Its Exchange Every Day", *Business Insider*, 9. November 2012.

12. Larry Kim, „How Many Ads Does Google Serve In A Day?", *Business 2 Community*, 2. November 2012.

13. John Deighton und Leora Kornfeld, „The Socioeconomic Impact of Internet Tracking", *Interactive Advertising Bureau*, Februar 2020.

14. Tim Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*, FSG Originals, 13. Oktober 2020.

15. Australian Competition and Consumer Commission, „Digital advertising services inquiry - Interim report", Dezember 2020.

16. Stuart A. Thompson und Charlie Warzel, „Twelve Million Phones, One Dataset, Zero Privacy", *The New York Times*, 19. Dezember 2019.

17. Janelle Nanos, „Every step you take: How companies use geolocation data to target you – and everyone around – in ways you're not even aware of", *The Boston Globe*, 21. Juli 2018.

18. Krish Vitaldevara, „Safer and More Transparent Access to User Location", *Android Developers Blog*, 19. Februar 2020.

19. Sam Schechner und Mark Secada, „You Give Apps Sensitive Personal Information. Then They Tell Facebook", *The Wall Street Journal*, 22. Februar 2019.

20. Facebook for Business, „Measuring Conversions on Facebook, Across Devices and in Mobile Apps", 14. August 2014.

21. Brad Bender, „New digital innovations to close the loop for advertisers", *Google Ads & Commerce Blog*, 26. September 2016.

22. Federal Trade Commission, „FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook", 24. Juli 2019.

23. Kimberly Chin, „Twitter Could Pay FTC Fine Over Alleged Privacy Violations", *The Wall Street Journal*, 3. August 2020.

24. Adam Satariano, „Google Is Fined $57 Million Under Europe's Data Privacy Law", *The New York Times*, 21. Januar 2019.

25. Zoe Schiffer, „Period tracking app settles charges it lied to users about privacy", *The Verge*, 13. Januar 2021.

26. Stuart A. Thompson, „These Ads Think They Know You", *The New York Times*, 30. April 2019.

27. Giridhari Venkatadri, Piotr Sapiezynski, et al., „Auditing Offline Data Brokers via Facebook's Advertising Platform", *The World Wide Web Conference*, 2019, S. 1920-1930.

28. Kalev Leetaru, „The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong", *Forbes*, 5. April 2018.

29. Michael Grothaus, „The top 7 iOS 14 privacy features: What you need to know", *Fast Company*, 16. September 2020.

30. Thomas Germain, „How a Photo's Hidden ‚Exif' Data Exposes Your Personal Information", *Consumer Reports*, 6. Dezember 2019.

31. Burt Helm, „Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism", *Fast Company*, 12. Mai 2020.

32. Edith Ramirez, Julie Brill, et al., „Data Brokers: A Call for Transparency and Accountability", *Federal Trade Commission*, Mai 2014.

33. Oracle, „12 Must-Ask Questions to Separate Fact from Fiction," www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf.

34. Alex Hern, „‚Anonymous' browsing data can be easily exposed, researchers reveal", *The Guardian*, 1. August 2017.

35. Geoffrey A. Fowler, „You watch TV. Your TV watches back", *The Washington Post*, 18. September 2019.

36. X-Mode, „Data Licensing", xmode.io/data-licensing/.

37. Wenn das Benutzeralter, das mit der für ein Gerät registrierten Apple ID verbunden ist, unter 18 Jahren liegt, ist der IDFA Zugriff standardmäßig deaktiviert und kann keinem Entwickler gewährt werden.

38. Google Ads Help, „About Smart Bidding", support.google.com/google-ads/answer/7065882?hl=en.

39. Marne Litfin, „What is Mobile ad attribution? An introduction to app tracking", *Adjust*, 4. Februar 2019.

40. Joseph Cox, „The IRS Is Being Investigated for Using Location Data Without a Warrant", *Vice*, 6. Oktober 2020.

41. Joseph Cox, „How the U.S. Military Buys Location Data from Ordinary Apps", *Vice*, 16. November 2020.

42. Joseph Cox, „CBP Bought ‚Global' Location Data from Weather and Game Apps", *Vice*, 6. Oktober 2020.