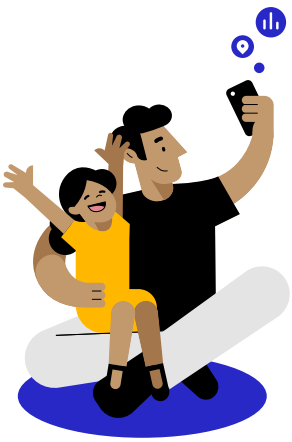


あなたのデータの一日

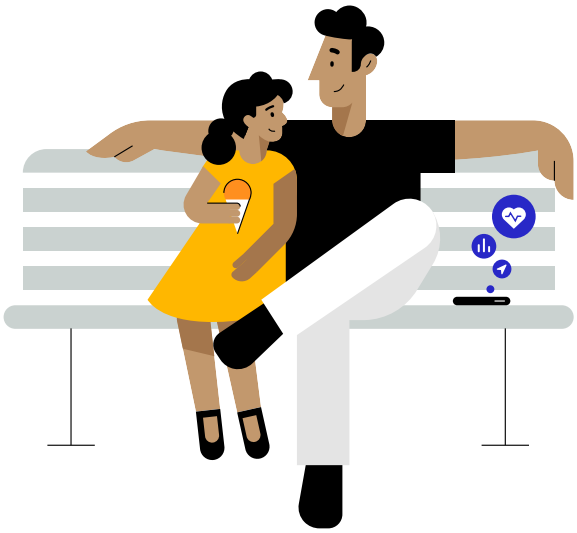
公園で。父と娘のストーリー

2021年4月

「人々は賢いと信じています。中には、ほかの人たちよりも多くのデータを共有したがる人もいるでしょう。だから彼らに聞くべきなんです。毎回、聞くべきです。聞かれるのが嫌になるまで聞くべきです。そして彼らのデータで自分たちが何をしようとしているのか、正確に説明すべきです」

Steve Jobs

All Things Digital Conference（2010年）



過去10年間にわたり、大きく不透明な業界によって収集される個人情報の量が増加しています[1,2]。ウェブサイト、アプリ、ソーシャルメディア企業、データブローカー、アドテクノロジー企業の複雑なエコシステムは、オンラインでもオフラインでもユーザーを追跡し、個人情報を収集しています。これらの情報をつなぎ合わせ、共有し、集め、リアルタイムのオークションで利用することで、年間総価値2,270億ドルの業界が利益を得ています[1]。皆さんが日々の生活を送っている間、多くの場合は知らないうちに、または許可もなく、このようなことが毎日行われているのです[3,4]。公園で楽しい一日を過ごす父と娘について、この業界がどのようなことを知ることができるのかを見てみましょう。

ご存知ですか？

あなたが毎日使うアプリには、平均的なアプリ1つ当たり6つのトラッカーが組み込まれています[3]。AndroidやiOSの人気が高いアプリの大半にも、複数のトラッカーが組み込まれています[5,6,7]。

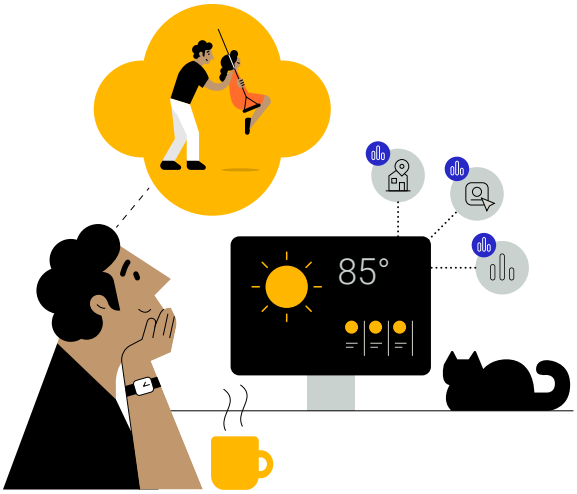
トラッカーは多くの場合、デベロッパがアプリを開発する際に活用するサードパーティコードに組み込まれています。デベロッパがトラッカーを組み込むことで、第三者もあなたが共有した情報を収集し、そのデータを複数のアプリ間で関連付けたり、あなたに関するそのほかの収集データと結びつけることができるようになります。

データブローカーは、直接関わりのない特定の個人に関する個人情報を収集し、第三者に売却したり、使用を許可したり、そのほかの方法で開示します[3]。

数百ものデータブローカーが、オンラインとオフラインで情報を収集しています[8]。世界中で7億人の消費者に関する情報を集め、最大5,000の特性を含む消費者プロフィールを作成しているブローカーもいます[9]。

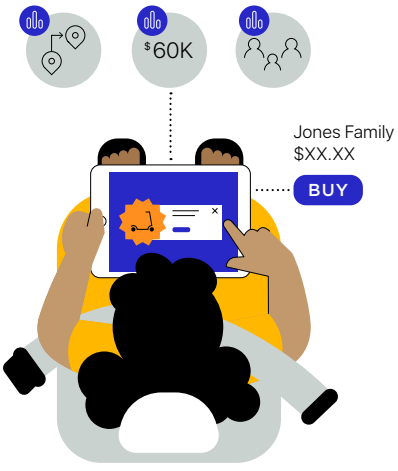
調査によると、20%近くの子ども向けアプリで、保護者が検証できる同意なしにデベロッパが個人を特定できる情報を収集および共有していました[10]。

インターネット上では毎日毎時間、ユーザーに対して数十億ものデジタル広告が表示されています[11,12,13]。広告が読み込まれる数ミリ秒の間に、リアルタイムでオークションが行われます。このオークションでは広告主が広告スペースに入札しますが、その多くがトラッキングされたユーザーの個人情報に依存しています[14,15]。



娘と公園に出かける一日の計画を立てるジョン

ジョンは今日一日、7歳の娘エマと一緒に過ごす予定です。その日の朝ジョンは、パソコンで天気を調べ、ニュースを読み、娘の学校の隣にある公園に行くためにスマートフォンの地図アプリで交通状況をチェックしました。車を運転中、ジョンのスマートフォン上では4つのアプリがバックグラウンドで2人の位置情報を定期的に収集し、追跡しています[16,17,18]。デバイスから情報が抽出されると、アプリのデベロッパはその情報をジョンが聞いたこともない正体不明の第三者データブローカーに売却します[16,17]。収集された位置情報は匿名とされていますが、データブローカーはユーザーを追跡することにより、これらのアプリに残っているジョンの位置情報の履歴と、彼が使ったほかのアプリから収集した情報を照合することができます[16,19]。これはつまり、異なるアプリや複数の情報源から追跡された情報をあらゆる企業や組織が購入でき、それを使って毎日の詳しい行動を含む彼の総合的なプロフィールを作成できるということです[3,16]。



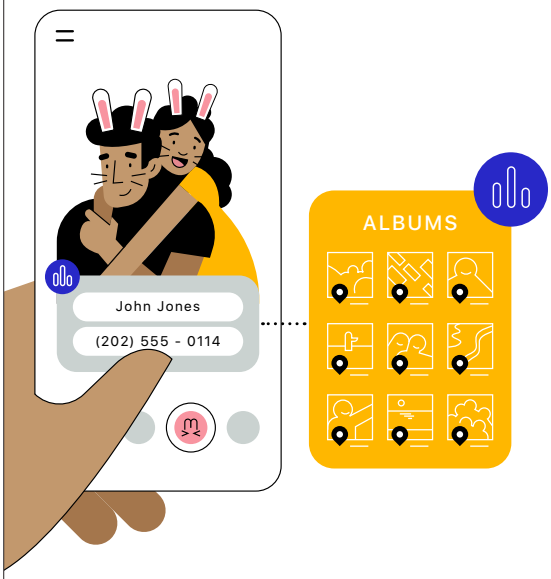
公園に向かう車の中でゲームをするエマ

公園に向かう車の中で、ジョンは娘にタブレットを渡してゲームで遊ばせています。エマがアプリを開くと、キックボードの広告が目に入りました。これは偶然ではありません。アプリが読み込まれるほんの一瞬の間に、広告スペースのオークションが行われたのです[14]。仲介業者を介して、キックボード会社の代理である広告会社が、利用可能な広告の情報を入手します[15]。そして、ジョンとエマについて集められた個人情報を使い、広告に入札します[15]。キックボード会社の広告パートナーは、2人が広告をクリックしたか、あるいはキックボードを購入したかを把握するため、広告を表示したあともジョンとエマの行動についての情報収集を続けます[3]。さらにこの会社は、ジョンのすべてのデバイス上で様々なアプリやウェブサイトにわたって2人を追跡し、あらゆる方法を使ってジョンとエマにキックボードの広告を表示し続けます[3,20,21]。

一部のアプリは、サービスの提供に必要となる範囲を超えたデータへのアクセスを求めてきます。正確な位置情報へのアクセスを要求するキーボードアプリなどはその例です[5]。

個人情報のやり取りは、広告ネットワーク、広告パブリッシャー、アトリビューションと測定のプロバイダ、データブローカー、そのほかの民間企業、そして政府機関にまで及ぶこともあります[3, 15, 40, 41, 42]。ソーシャルメディア企業やアドテクノロジー企業が情報収集時にユーザーに通知した以外の目的で個人情報を使用した場合、多額の罰金が科せられます。実際に罰金を支払った企業もあります[22, 23, 24, 25]。

データブローカーは収集した情報を使ってユーザーに特性を割り当て、「ダイエットしたいがパンが好きでやめられない」人など、極めて詳細なマーケットセグメントに分類します[26]。しかしこのようなプロフィールには間違いが多く、調査によると40%以上の特性が不正確であることがわかっています[27, 28]。

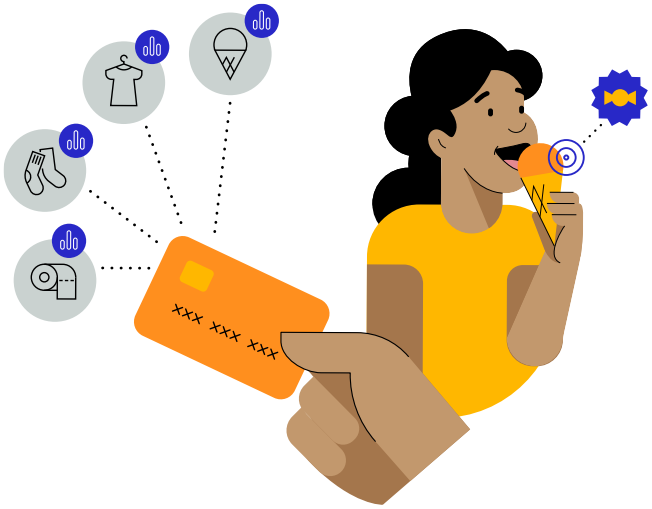


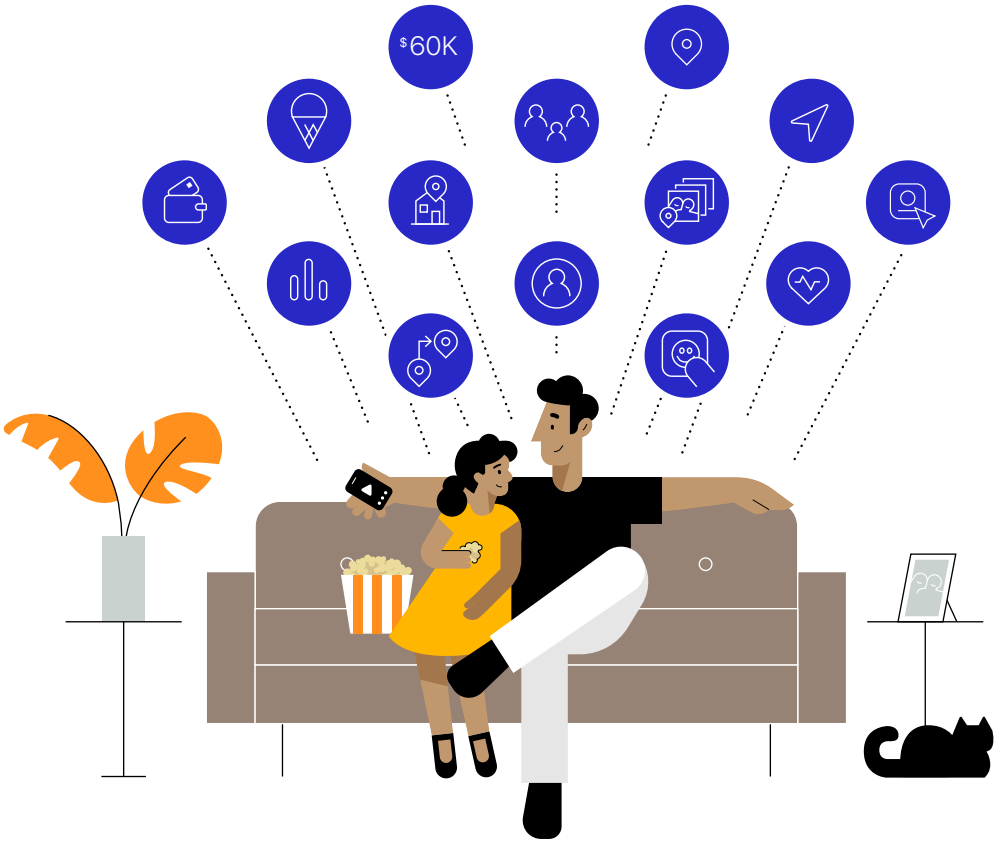
公園でセルフィーを撮るジョンとエマ

公園に着くと、ジョンとエマはセルフィーを撮りました。写真加工アプリを使って遊び、撮った写真にうさぎの耳を加えることにしました。ただしこの加工アプリは、公園で撮ったセルフィーだけではなく、デバイス上にあるすべての写真とそれらに添付されたメタデータにアクセスできます[29, 30]。ジョンはこの写真をソーシャルメディアアプリに投稿しました。このアプリはEメールアドレス、電話番号、広告識別子を使って、ジョンの現在のオンラインでの行動を、ジョンの特性情報や購入傾向など、ほかのアプリから収集したデータバンクに関連付けます[3]。

帰宅途中、アイスクリーム屋に寄り道

家に帰る途中、ジョンとエマはおやつを買うためにアイスクリーム屋に寄り道します。ジョンがアイスクリームの代金をクレジットカードで支払うと、店の場所や支払った金額などの情報が、ジョンの嗜好に関する総合的な情報プロフィールに追加されます[31, 32, 33]。ジョンの位置情報を追跡しているアプリの一つは、ジョンとエマがおもちゃ屋に立ち寄ったことも観察しています[3]。その日家族が買い物をした場所の情報はデータブローカーに引き渡され、ジョンに幼い子どもがいるという情報と組み合わせられて、ジョンのデバイスには甘いお菓子や立ち寄ったおもちゃ屋のターゲティング広告が表示されます[17]。





その日の終わりには、ジョンが関わったことのない世界中の様々な企業がジョンとエマに関する情報を追加して彼らのプロフィールを更新します。これらの企業は、彼らがどこに住んでいて、どの公園に行ったか、どのニュースサイトを読んだか、どんな商品を閲覧したか、どんな広告を見たか、どのような購入傾向があるか、どの店を訪れたかをすべて知っています[3、34]。この情報はジョンとエマがその日に使った複数のアプリやそのほかの情報源から収集され、追跡されたものです。ジョンはその日一日でどれだけの情報が収集されたかを知りません。その情報を常にコントロールできたわけでもなく、意図的に追跡を許可したわけでもありません[3、4]。のんびり夜を過ごそうと一家がスマートテレビのアプリで子ども向けの映画を検索している間も、追跡、データのやり取り、オークション、リターゲティングのサイクルは執拗に続けられています[35、36]。

Appleが導入しているプライバシー機能と、ユーザーのプライバシー保護のためにAppleが行っている活動については、apple.com/jp/privacy をご覧ください。

Safariがあなたのプライバシーをどのように保護しているかについては、Safariのホワイトペーパー（英語）をご覧ください。

Appleがあなたの位置情報をどのように保護しているかについては、位置情報サービスのホワイトペーパー（英語）をご覧ください。

Appleのプライバシーに関する原則

Appleでは、プライバシーは基本的人権の一つであると信じています。私たちは4つの主なプライバシーに関する原則を指針として、製品とサービスを設計しています。

データの最小化
特定のサービスを利用するにあたり、あなたのニーズに応えるために必要な最小限のデータのみを収集します。

デバイス上での処理
データをAppleのサーバに送信するのではなく、可能な限りデバイス上で処理することで、ユーザーのプライバシーを保護し、データ収集を最小限に抑えます。

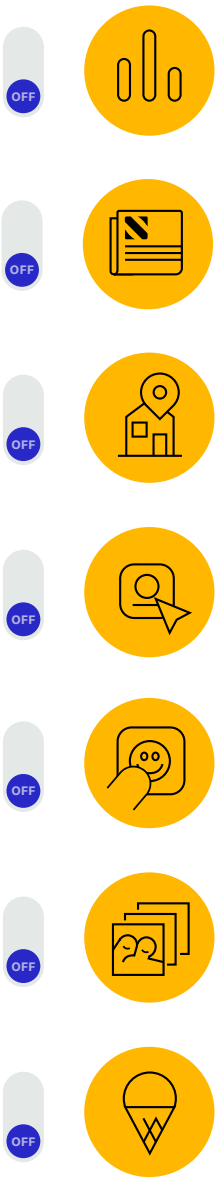
透明性の向上とユーザーによるコントロール
どのデータが共有され、どのように使われるかをユーザーが把握し、ユーザー自身がコントロールできるようにします。

セキュリティ
ハードウェアとソフトウェアが連係して、データを安全に守ります。

Appleはこれらの4つの原則を通じて、ユーザー自らが理解してコントロールできる安全な方法によりデータを望み通りに共有できるようにすることを、常に目標に掲げてきました。過去20年間にわたり、私たちがすべてのApple製品とサービスにおいてユーザーのプライバシーを守るための革新を続けてきたのはそのためです。デバイス上の知能などの機能を利用して、アプリ、ブラウザ、オンラインサービスで収集する情報を最小限に抑えているのもその一例です。すべてのアプリとサービスを横断する単一の総合的なユーザー情報のプロフィールを作成することもありません。

Appleのプライバシー機能はデータ共有の透明性を高め、ジョンが自分のデータをより細かくコントロールできるようにします。

ジョンとエマの一日を描いたこのストーリーは、Appleが取り組むプライバシーに関する問題とそのソリューションを示しています。



娘と公園に出かける一日の計画を立てるジョン

ジョンがコンピュータでSafariのブラウザを使って天気をチェックしていたら、デフォルト設定のインテリジェント・トラッキング防止機能がこの行動の追跡を防ぎました。

ジョンが今朝Apple Newsを使ってニュースを読んでいたら、Appleは彼が誰で何を読んだかを特定することなく、ジョンの興味にもとづいたコンテンツを提供しました。

ジョンがAppleのマップアプリを使って交通情報をチェックしていたら、ジョンの位置情報は彼に結びつけられることのない定期的にリセットされるランダムな識別子に関連付けられ、本人以外誰も彼の位置情報を知ることはありませんでした。

iPhoneでは、どのアプリがバックグラウンドでジョンの位置情報にアクセスしているかが定期的に通知されます。アプリに位置情報を共有する前に、ジョンはおおよその現在位置のみを共有するか、一度だけ位置情報を共有するかどうかを選択できます。

公園に向かう車の中でゲームをするエマ

iPadでは、アプリに対してトラッキングの透明性を求める機能が近々追加され、ゲームアプリが他社の所有するアプリやウェブサイトを横断してエマの行動を追跡できるかどうかをジョンが選べます。

AppleのSKAdNetwork APIを利用している広告ネットワークは、ジョンのデバイスと関連付けられる情報にアクセスすることなく、広告の総合的な効果を測ることができます。

公園でセルフィーを撮るジョンとエマ

iPhoneでは、写真加工アプリがフォトライブラリ全体ではなく、そのセルフィーだけにアクセスできるようジョンが選択できます。

帰宅途中、アイスクリーム屋に寄り道

ジョンがApple Cardを使ってアイスクリームを買っていたら、銀行がジョンの決済情報をマーケティング目的で使用することはありませんでした。彼がApple Payを使っていたら、Appleはデバイス上の知能を利用していたので、彼がどの店で何を買っていくら支払ったかの情報をAppleが取得することなく、ジョンはiPhone上で決済履歴を確認できました。

一日の終わりには、Appleの製品とプライバシー機能がより高い透明性でどれだけの情報が共有され、どう使われたかを示すので、ジョンは一日を通じてそれらを自分で一段とコントロールできるようになります。

アプリに対してトラッキングの透明性を求める機能と、App Storeに新しく加わったプライバシー情報セクション

Appleは、アプリのエコシステムの中でユーザーのプライバシーを守るために次のレベルの取り組みを始めました。現在、消費者の個人情報にアクセスし、それを追跡して収益化する事業者が増え、事業者の構造が複雑になっています。そこでAppleは、さらなる透明性、わかりやすさ、選択肢をユーザーに届けるために、2つの新機能を追加します。この機能によってユーザーは内容を理解して選択でき、自らのプライバシーを一段と自分でコントロールできるようになります。

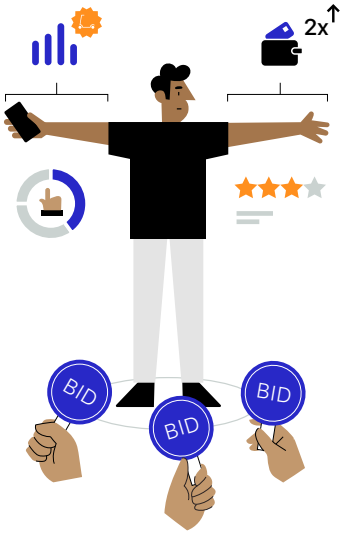
まもなく行われる次のベータアップデートの際に、アプリに対してトラッキングの透明性を求める機能が導入されます。これは、アプリが他社の所有するアプリやウェブサイトを横断してユーザーの行動を追跡する場合、ユーザーの許可を得ることを義務付ける機能です。ユーザーは、どのアプリが追跡の許可を求めているかを「設定」でチェックでき、自分にとって適切な設定に変更できます。今春に予定されているiOS 14、iPadOS 14、tvOS 14のアップデートによって様々な製品に広く導入されるこの要件は、世界中にいるプライバシー保護の提唱者からすでに支持を集めています。この機能を設計する際、Appleはユーザーにさらなる透明性と自分で一段とコントロールできる方法を届けられるように配慮しました。一方で広告は、アプリやウェブコンテンツを支援するための適切で効果的な手法として引き続き利用できます。Safariのインテリジェント・トラッキング防止機能など、すでに導入されている機能は、ユーザーのプライバシー保護を強化しながら、広告を引き続き有効な手段として利用できることを証明してきました。そしてアプリに対してトラッキングの透明性を求める機能を導入することで、ユーザーは自分が使うアプリやアプリに与える許可について、理解を一段と深めた上で選択できます。これからは、アプリによるユーザーの追跡を許可するかどうかを選ぶのはユーザー自身です。信頼して追跡の許可を与えたアプリでは、デベロッパがこれまで通りユーザーを追跡できます。

追跡に関してユーザーの許可を義務付けることに加えて、Appleは最近App Storeの製品ページを修正して透明性を一段と向上させました。新しく用意された「Appのプライバシー」のセクションでは、各アプリのプライバシーに関する方針の概要を、ユーザーがより深く理解できるようになっています。各アプリの製品ページでは、デベロッパによるプライバシーに関する方針の概要を、ユーザーが見やすい方法で表示することが義務付けられます。詳細ページには写真、位置情報、連絡先情報など、アプリが収集する情報のタイプが記載されます。このページでは、追跡目的での利用、ユーザーへの関連付けなど、アプリのデベロッパがそれぞれのタイプの情報をどのように使うかも詳しくわかります。そしてAppleを含めたすべてのアプリデベロッパには、プライバシーに関する方針を自主的に報告することを義務付けました。

アプリに対してトラッキングの透明性を求め、トラッキングを設定できるようにする機能と、App Storeの製品ページへのプライバシーに関する情報の追加により、ユーザーは自分の個人情報がどのように使われるかを一段と簡単に把握できます。そして、以前は不透明だったり、隠されていたプライバシーに関する方針を明らかにすることで、自分のデータを一段と自分でコントロールできるようになります。

あなたの個人情報の安全を確実に守れるように。Appleはこれからも革新的なプライバシー技術を開発しながら、新しい手法を取り入れ続けていきます。

ある広告の一日



広告オークション

ジョンのデバイス上でキックボードの広告をエマが見たのは、偶然ではありません。広告主たちは、デバイスに広告を表示させるためのオークションに入札するのです[37]。デバイスの画面に表示された広告が、わずか一瞬でどうやって選ばれたのかを簡単に説明します。

1.
エマが使っているアプリのデベロッパが、アプリ内の広告スペースをリアルタイムで競売にかけるアドテクノロジー企業を雇います[14]。

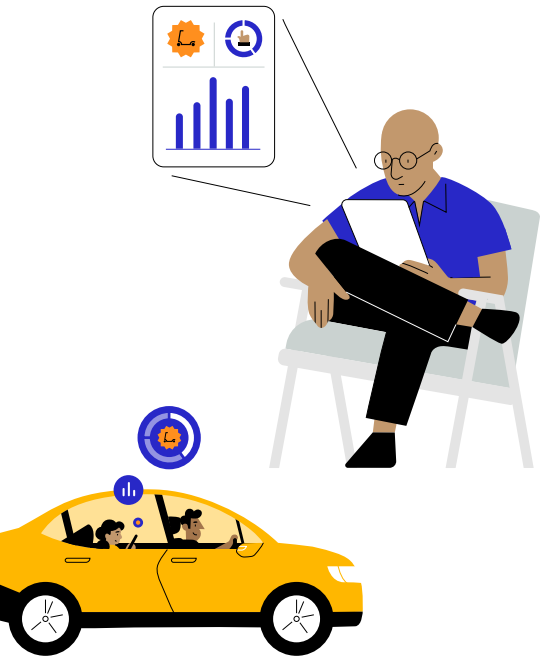
2.
エマがアプリを開くと、広告ネットワークがジョンのデバイスの使用状況（エマが使っているアプリ、エマの位置情報、ジョンの広告IDなど）からデータを集めます。同時に、トラッキングを可能にするそのほかの情報やジョンの広告IDをもとに、第三者からもデータを収集します[3]。

3.
広告ネットワークはこの情報の一部（特に広告ID）を、入札する可能性がある広告主と共有します。広告主は通常、自社が持つデータのほか、追跡とプロフィール作成によって収集・集計された個人情報をもとに、そのユーザーに関するできるだけ多くの情報を入札前に得ようとします[3,15]。

4.
ジョンとエマのデータから得られた特徴と、広告主がターゲットにするユーザーの一致度が高いほど、より多くの広告主がその広告スペースに入札します[15,38]。

5
広告スペースの落札者によるキックボードの広告が、エマが使っているデバイスに表示されます[14]。

この広告オークションのプロセスはほんの一瞬の間に起こるので、スペースに入札して広告を表示するために、買い手と売り手の両方が個人情報を収集、交換、使用します[14,15]。



広告アトリビューション

キックボード会社が雇っている広告会社は、広告を表示したあと、エマの行動に対する広告の効果を測ろうとします。このプロセスは、広告アトリビューションと呼ばれています。

この測定のために、広告主はエマが使っているデバイス上での行動追跡を試み、インターネットやアプリ上で彼女が何をしたか、さらにはどこでオフラインになったかという情報まで収集します。

- **製品広告の場合、**広告主は、ユーザーが広告を見たあとにウェブサイトや実際の店舗を訪れたか、そして製品を購入したかを知るための追跡を試みます[3]。
- **アプリの広告の場合は、**そのアプリをインストールしたかどうかを追跡によって知ろうとします。これは、アプリインストールのアトリビューションと呼ばれています[39]。

また、広告主は広告アトリビューションを利用して、広告キャンペーンがより効果的なグループを対象に、キャンペーンの「最適化」を図ります[3]。

しかし、こんなことをする必要はありません。広告主は、ユーザーを追跡しなくても、グループに対する広告キャンペーンの効果を測定できるのです。Appleは、ユーザーのプライバシーを守りながら広告キャンペーンの効果を測るツールの開発に取り組んできました。

SKAdNetworkは、広告キャンペーンの効果を評価できるように、広告の表示後にそのアプリがインストールされた回数を広告主に知らせます。ただし、この情報はユーザーやデバイスのデータを共有しないように設計されているため、広告主がユーザーを追跡することはありません。

Private Click MeasurementはiOS 14.5とiPadOS 14.5のアプリに対応し、オンデバイス処理を利用することでデータ収集を最小限にしながら、ユーザーをウェブサイトへ誘導する広告の効果を広告主が測定できるようにします。ユーザーがアプリ内で製品広告をクリックすると、ウェブブラウザ本体がPrivate Click Measurementを使って、ユーザーが広告をクリックしたという情報や、それがウェブサイト訪問や製品購入などの一定の成果につながったという情報を広告主に提供します。その際、具体的に誰が広告をクリックしたかという情報は提供しません。

よくある質問

「Appにトラッキングしないように要求」を選んでも、アプリの機能を制限なく使えますか？

はい。アプリのデベロッパは、あなたがアプリのすべての機能を使うために追跡を許可するよう求めることはできません。

識別子とは何ですか？どのように使われますか？

広告識別子（IDFA）やEメールアドレスなどの識別子は、ネットワーク上で特定のデバイスを識別するために使われます。また、広告主があなたのデバイスの識別子を確認してあなたの行動と関連付けることで、様々なアプリやウェブサイト上での行動をまとめた詳細なプロフィールを作ることができます。

広告識別子（IDFA）とは何ですか？

広告識別子（IDFA）は、iOSがそれぞれのデバイスに割り当てる、ユーザーがコントロールできる識別子です。これはハードウェアに関連付けられたものではなく、ソフトウェアベースの識別子です。そのため、アプリにトラッキングの透明性を求める機能を使って、特定のアプリではIDFAをブロックするようにユーザーが設定できます。これにより、IDFAにもとづくトラッキングをユーザー自身がコントロールできるようになります。

「Appにトラッキングしないように要求」を選んだ場合、Appleはアプリが私を追跡しないことを保証できますか？

あなたが「Appにトラッキングしないように要求」を選ぶと、そのアプリのデベロッパは追跡に使われることが多い広告識別子（IDFA）にアクセスできなくなります。さらにデベロッパは、広告識別子よりもあなたの選択を尊重するよう求められます。これは、App Storeでの配信用にアプリを提出する際にデベロッパが同意するポリシーによって義務付けられています。追跡を許可していないユーザーをデベロッパがトラッキングしていることが判明した場合は、プライバシーの方針を改め、ユーザーの選択を尊重するようデベロッパに要求します。これに従わない場合は、そのデベロッパのアプリがApp Storeから削除されることもあります。

ソーシャルメディアのアカウントを使ってアプリにサインインした場合、そのソーシャルメディアの企業はアプリ内での私の行動を追跡できますか？

あなたがそのアプリに対して追跡を許可しているかどうかによります。「Appにトラッキングしないように要求」を選ぶと、そのアプリが広告のために他社のアプリやウェブサイトを横断してあなたを追跡したり、あなたの情報をデータブローカーと共有することはありません。つまり、広告目的で使用される場合、アプリがあなたの情報をソーシャルメディア企業に提供することはないということです。

Appleは、App Storeの製品ページに記載されているプライバシー情報が正確であることをどのように確認していますか？

App Storeの年齢制限指定と同様、プライバシーに関する方針はデベロッパが自主的に報告しています。デベロッパの提出した情報が正確でないことが判明した場合は、デベロッパと一緒に正確な情報を記載するよう取り組みます。

データブローカーとは何ですか？

一般的にデータブローカーとは、業務上直接関わりのない特定のエンドユーザーの個人情報を定期的に収集して第三者に売却したり、その使用を許可したり、そのほかの方法で開示する企業です。一部の自治体では、データブローカーについて法律で定義されています。

Sources

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

2. Reinsel, David, 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," July 1, 2020.

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

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

6. Binns, Reuben, Ulrik Lyngs, et al., "Third Party Tracking in the Mobile Ecosystem," *Proceedings of the 10th ACM Conference on Web Science*, 2018, pp. 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, filed May 25, 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Reyes, Irwin, 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, pp. 63-83.

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

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

13. Deighton, John, and Leora Kornfeld, "The Socioeconomic Impact of Internet Tracking," *Interactive Advertising Bureau*, February 2020.

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

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

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

17. Nanos, Janelle, "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*, July 21, 2018.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. Ramirez, Edith, Julie Brill, et al., "Data Brokers: A Call for Transparency and Accountability," *Federal Trade Commission*, May 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. Hern, Alex, "'Anonymous' browsing data can be easily exposed, researchers reveal," *The Guardian*, August 1, 2017.

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

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

37. If the user age associated with the Apple ID registered to a device is under 18, IDFA access is disabled by default, and cannot be granted to any developer.

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

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

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

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

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