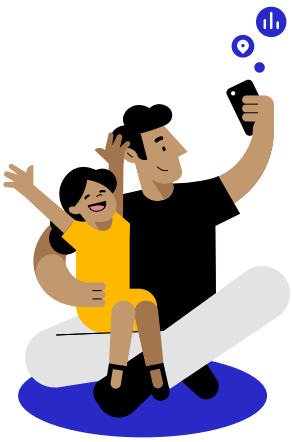


Um dia na vida dos seus dados

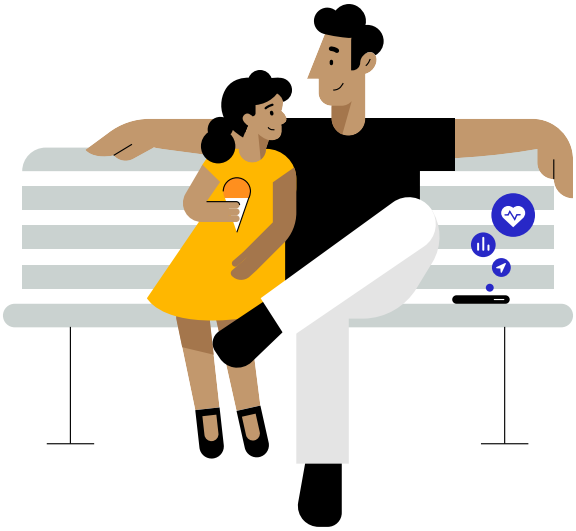
Pai e filha em um passeio no parque

Abril de 2021

“Acredito que as pessoas são inteligentes, e algumas querem compartilhar mais dados do que outras. Pergunte a elas. Pergunte todas as vezes. Faça com que elas tenham que pedir para você parar caso se cansem das suas perguntas. Explique exatamente o que você fará com os dados delas.”

Steve Jobs

Conferência “All Things Digital”, 2010



Na última década, um mercado grande e obscuro vem acumulando quantidades cada vez maiores de dados pessoais[1,2]. Um ecossistema complexo de sites, aplicativos, empresas de redes sociais, corretores de dados e empresas de tecnologia de publicidade rastreia usuários online e offline, coletando dados pessoais. Esses dados são reunidos, compartilhados, agregados e usados em leilões em tempo real, movimentando uma indústria que fatura US$ 227 bilhões por ano[1]. Isso ocorre todos os dias, enquanto as pessoas seguem suas rotinas, muitas vezes sem seu conhecimento ou permissão[3,4]. Vamos dar uma olhada no que essa indústria é capaz de descobrir sobre um pai e sua filha durante um dia aparentemente agradável no parque.

Você sabia?

Rastreadores estão integrados a apps que você usa todos os dias: um aplicativo tem, em média, seis rastreadores[3]. A maioria dos apps mais baixados para Android e iOS tem rastreadores integrados[5,6,7].

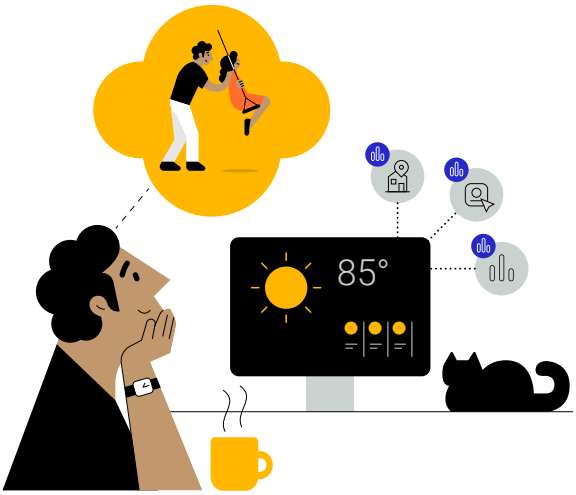
Os rastreadores geralmente fazem parte de códigos de terceiros que ajudam os desenvolvedores a criar seus apps. Ao incluir rastreadores, os desenvolvedores também permitem que os dados que você compartilhou com eles sejam coletados e vinculados por terceiros a diferentes apps e a outros dados coletados sobre você.

Uma prática de corretores de dados é coletar e vender, licenciar ou de outra forma divulgar a terceiros informações pessoais de indivíduos específicos com os quais eles não têm uma relação direta[3].

Centenas de corretores de dados coletam dados online e offline[8]. Um corretor coleta dados sobre 700 milhões de consumidores em todo o mundo, criando perfis de consumidor com até cinco mil características[9].

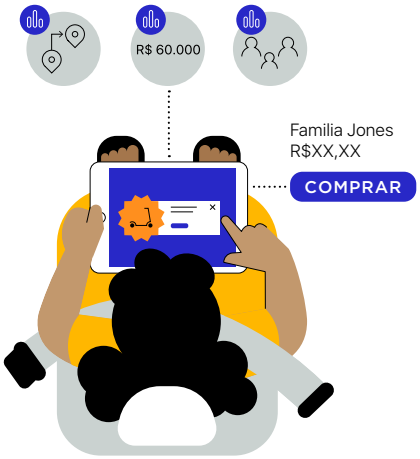
Um estudo constatou que, em quase 20% dos apps para crianças, desenvolvedores coletaram e compartilharam informações de identificação pessoal sem autorização comprovada dos pais[10].

A cada hora, todos os dias, usuários online veem bilhões de anúncios digitais[11,12,13]. Nos milissegundos que um anúncio leva para carregar, ocorre um leilão em tempo real, durante o qual os anunciantes dão lances no espaço do anúncio, muitas vezes contando com dados pessoais rastreados sobre o indivíduo[14,15].



John planeja um dia no parque com a filha

John e sua filha Emma, de sete anos, vão passar o dia juntos. De manhã, John usa o computador para saber a previsão do tempo e ler as notícias. Em seu smartphone, ele usa um app de mapa para ver como está o trânsito até o parque próximo da escola da filha. Durante o percurso, quatro apps no telefone dele coletam e rastreiam dados de localização periodicamente em segundo plano[16,17,18]. Os dados extraídos do aparelho são vendidos por desenvolvedores de apps para diferentes corretores de dados de terceiros dos quais John nunca ouviu falar[16,17]. Embora os dados de localização coletados sejam considerados anônimos, o rastreamento de usuário permite aos corretores combinar o histórico de localização desses apps com as informações coletadas durante o uso de outros aplicativos[16,19]. Isso significa que as informações rastreadas em diferentes apps e de diferentes fontes estão disponíveis para qualquer empresa ou organização comprar e podem ser usadas para criar um perfil completo sobre John, incluindo suas movimentações diárias precisas[3,16].



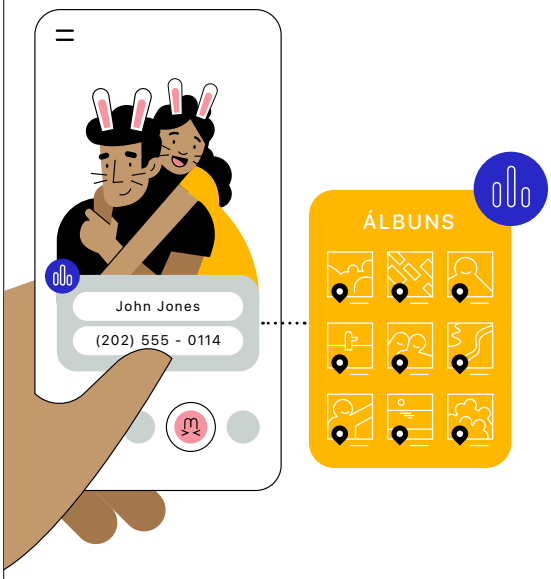
Emma joga no tablet no caminho até o parque

No caminho para o parque, John deixa a filha jogar no tablet. Ao abrir o app, ela vê um anúncio de patinete, o que não é nenhuma coincidência. Na fração de segundo em que o app carregou, ocorreu um leilão pelo espaço do anúncio[14]. Por meio de intermediários, as empresas de publicidade que trabalham em nome da fabricante de patinetes ficaram sabendo sobre o anúncio disponível[15]. Depois, usando os dados pessoais coletados sobre John e Emma, elas deram um lance no anúncio[15]. Os parceiros de publicidade da fabricante de patinetes continuam coletando informações sobre o comportamento de John e Emma depois que eles viram o anúncio para descobrir se clicaram nele ou se compraram o patinete[3]. E eles continuarão a anunciar o patinete de todas as maneiras possíveis para John e Emma, seguindo-os em diferentes apps e sites em todos os aparelhos de John[3,20,21].

Alguns apps solicitam acesso a mais dados do que o necessário para seus serviços, como um aplicativo de teclado que pede acesso à localização exata[5].

A troca de informações pode ir para redes de publicidade, editores de publicidade, provedores de atribuição e medição, corretores de dados, outras empresas privadas e até organizações governamentais[3,15,40,41,42]. Redes sociais e empresas de teclogia de publicidade podem ter que ou já tiveram que pagar milhões em multas por usar informações pessoais para fins diferentes dos que especificaram para o usuário no momento da coleta[22,23,24,25].

Corretores de dados usam os dados coletados para definir atributos aos usuários e classificá-los em segmentos de mercado hiperdetalhados, como pessoas que estão "tentando perder peso, mas amam padarias"[26]. O problema é que esses perfis muitas vezes estão errados: um estudo constatou que mais de 40% dos atributos são imprecisos[27,28].

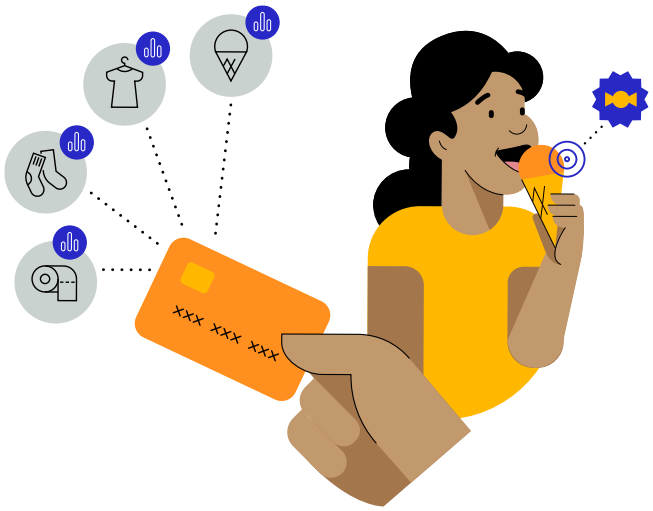


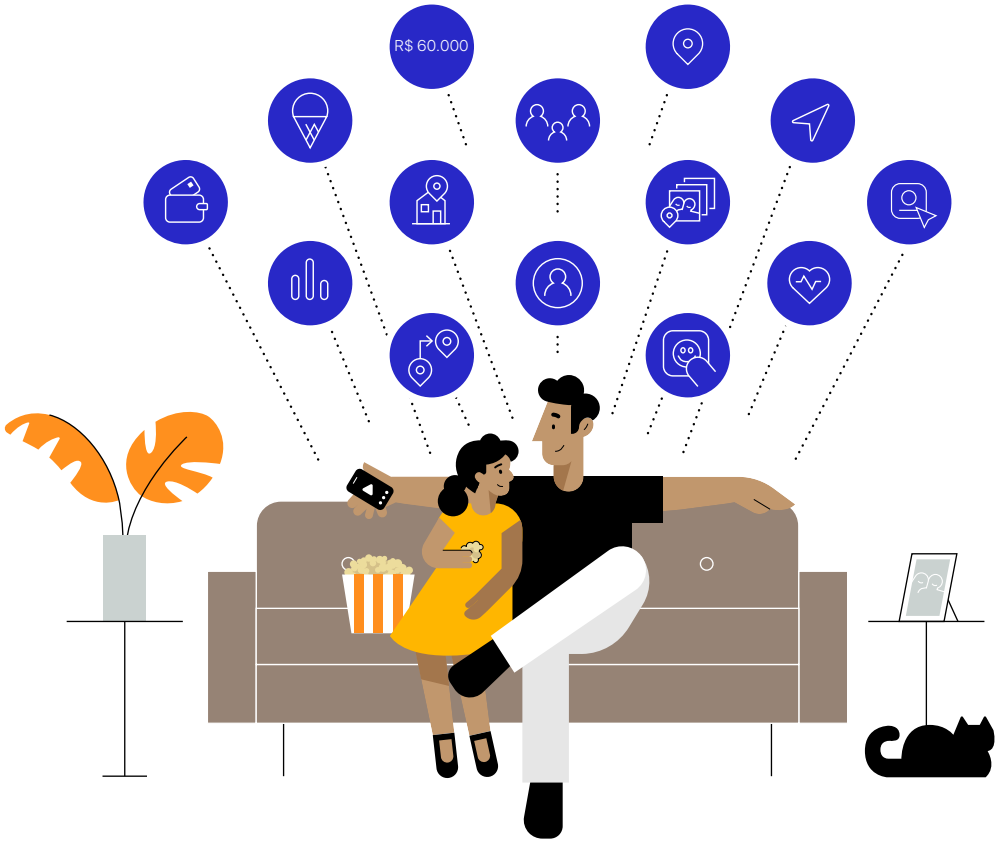
John e Emma tiram uma selfie no parque

Mais tarde, no parque, John e Emma tiram uma selfie. Eles brincam com um app de filtros para fotos e acabam escolhendo orelhas de coelho. No entanto, o aplicativo de filtros consegue acessar todas as fotos no aparelho e os metadados anexados, não só a selfie tirada no parque[29,30]. John posta a foto em um app de rede social. O aplicativo vincula a atividade online atual de John a um conjunto de dados coletados por outros apps, como perfil demográfico e hábitos de compra, usando um endereço de e-mail, um número de telefone ou um identificador de publicidade[3].

Uma parada na sorveteria

Na volta para casa, John e Emma decidem tomar um sorvete. John paga o sorvete com um cartão de crédito, adicionando mais informações ao longo perfil de dados sobre suas preferências: o endereço da loja e quanto ele gastou[31,32,33]. Um dos apps que rastreiam a localização de John consegue perceber que ele e Emma também entraram em uma loja de brinquedos[3]. As informações sobre onde a família fez compras durante o dia são repassadas aos corretores de dados, que combinam esses dados com o conhecimento de que John tem uma filha pequena para salpicar os aparelhos dele com anúncios direcionados de guloseimas e da loja de brinquedos que eles visitaram[17].





No final do dia, várias empresas do mundo inteiro com as quais John nunca interagiu atualizaram seus perfis com informações sobre ele e a filha. Essas empresas sabem o endereço residencial da família, o parque onde passaram o dia, os sites de notícias que leram, os produtos que pesquisaram na internet, os anúncios que viram, os hábitos de compra e as lojas que visitaram[3,34]. Esses dados foram coletados e rastreados em vários apps que John e a filha usaram durante o dia, além de outras fontes. John não tinha ideia de quantos dados estavam sendo coletados ao longo do dia, nem sempre tinha controle sobre eles e não deu permissão explícita para que isso acontecesse[3,4]. À noite, enquanto procuram um filme infantil em um aplicativo na Smart TV para relaxar, o ciclo de rastreamento, troca de dados, leilões e redirecionamento continua sem dar trégua[35,36].

Para saber mais sobre os recursos de privacidade introduzidos pela Apple e o trabalho que a empresa está fazendo para proteger a privacidade dos usuários, acesse apple.com/br/privacy.

Para entender como o Safari protege sua privacidade, leia o documento sobre Privacidade no Safari.

Para saber como a Apple protege seus dados de localização, leia o documento sobre os Serviços de Localização.

Princípios de privacidade da Apple

A Apple acredita que a privacidade é um direito humano fundamental. Criamos nossos produtos e serviços com base em quatro princípios de privacidade:

Redução de dados

Coleta da quantidade mínima necessária de dados para oferecer o que você precisa em cada serviço.

Processamento no aparelho

Para proteger a privacidade dos usuários e reduzir a coleta de dados, sempre que possível processamos dados no aparelho em vez de enviá-los aos servidores da Apple.

Transparência e controle do usuário

Fazemos questão que os usuários saibam quais dados são compartilhados e como são usados e que possam exercer controle sobre eles.

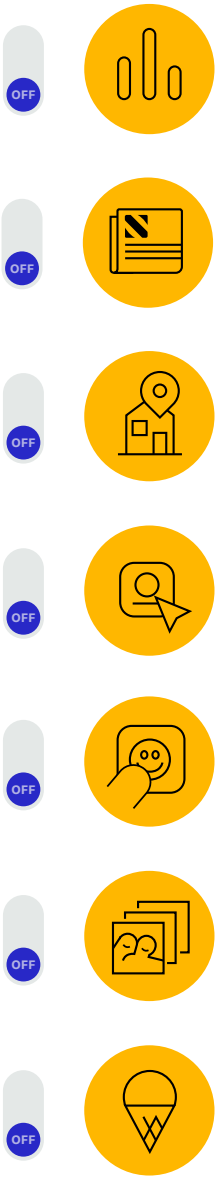
Segurança

Hardware e software trabalham juntos para manter os dados seguros.

Por meio desses quatro princípios, o objetivo da Apple sempre foi permitir que os usuários compartilhem dados como quiserem, de uma maneira que seja segura e que entendam e tenham controle. Essa é a razão pela qual, nas últimas duas décadas, a Apple constantemente promoveu inovações para preservar a privacidade do usuário em todos os nossos produtos e serviços. Por exemplo, utilizamos inteligência do aparelho e outros recursos para reduzir os dados coletados em nossos apps, navegadores e serviços online, e não criamos um perfil único e extenso de dados de usuário em nenhum dos nossos aplicativos e serviços.

Os recursos de privacidade da Apple dão a John mais transparência e controle sobre seus dados

A história de John e Emma ilustra os problemas de privacidade e as soluções que estamos desenvolvendo na Apple.



John planeja um dia no parque com a filha

Se John tivesse usado o navegador Safari para ver a previsão do tempo no computador, a Prevenção de Rastreamento Inteligente teria, como padrão, impedido o rastreamento dessa atividade.

Se John tivesse usado o Apple News para ler as notícias pela manhã, a Apple teria mostrado conteúdo de acordo com os interesses de John, sem saber quem ele é ou o que leu.

Se John tivesse usado o app Mapas da Apple para conferir o trânsito, seus dados de localização teriam sido vinculados a um identificador aleatório, que é reiniciado regularmente e não associado ao usuário. Como resultado, ninguém além de John saberia a localização dele.

Em um iPhone, John seria lembrado com regularidade de quais apps estão acessando sua localização em segundo plano. Antes de compartilhar a localização com um app, John teria as opções de compartilhar apenas sua localização aproximada ou de compartilhar somente uma vez.

Emma joga no tablet no caminho até o parque

Em um iPad, o recurso Transparência no Rastreamento em Apps, que será lançado em breve, daria a John a escolha de permitir ou não que o jogo rastreie a atividade de Emma em apps e sites de outras empresas.

As redes de anúncios que usam a API SKAdNetwork da Apple conseguiriam medir a eficácia geral de seus anúncios sem ter acesso a informações que pudessem ser rastreadas até o aparelho de John.

John e Emma tiram uma selfie no parque

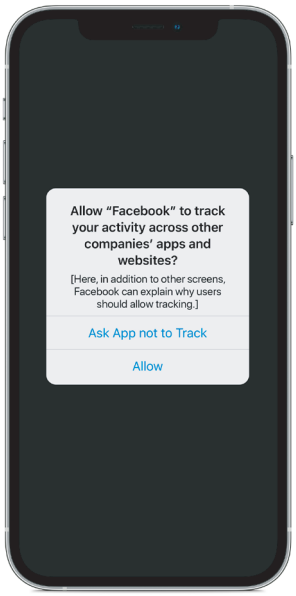
Em um iPhone, John teria tido a opção de dar ao app de filtro acesso apenas à selfie, e não à biblioteca de fotos inteira.

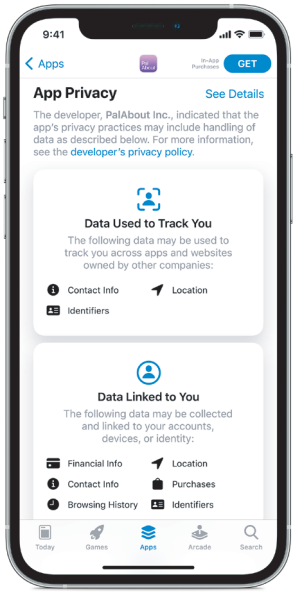
Uma parada na sorveteria

Se John tivesse comprado o sorvete com o Apple Card, seu banco não teria como usar as informações da transação para fins de marketing. Caso tivesse pagado com o Apple Pay, a Apple teria usado a inteligência do aparelho para que John pudesse ver o histórico de transações no iPhone sem que a Apple obtivesse informações sobre onde ele fez compras, o que comprou ou quanto gastou.

No final das contas, os produtos e recursos de privacidade da Apple podem dar a John mais transparência e controle ao longo do dia sobre quais dados são compartilhados e como são usados.

Transparência no Rastreamento em Apps e a nova seção de informações sobre privacidade na App Store





A Apple está dando o próximo passo para proteger a privacidade dos usuários dentro do ecossistema de apps. Com o objetivo de combater um conjunto complexo e crescente de entidades que acessam, rastreiam e monetizam dados pessoais do consumidor, vamos introduzir dois novos recursos destinados a fornecer aos usuários mais transparência, visibilidade e escolha para que possam tomar decisões informadas e exercer maior controle sobre sua privacidade.

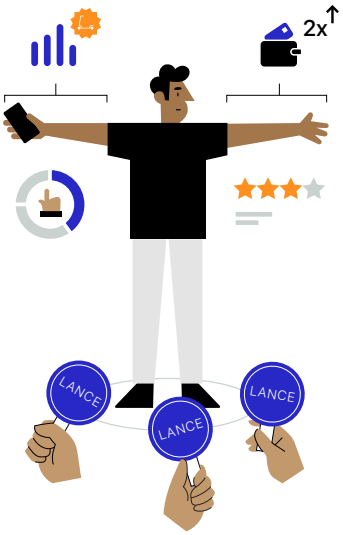
Em breve, com nossa próxima atualização beta, o recurso Transparência no Rastreamento em Apps exigirá que os aplicativos obtenham a permissão do usuário antes de rastrear seus dados em apps ou sites de outras empresas. Em Ajustes, os usuários poderão ver quais apps solicitaram permissão para rastrear. Com essa informação, eles podem fazer as alterações que quiserem. Esse requisito será implementado em vários sistemas com o lançamento do iOS 14, iPadOS 14 e tvOS 14, e já vem recebendo o apoio de defensores da privacidade em todo o mundo. Ao desenvolver esse recurso, a Apple procurou dar aos usuários mais transparência e controle e, ao mesmo tempo, continuar a permitir a publicidade como um meio adequado e viável de oferecer apps e conteúdo da web. A introdução de recursos anteriores, como a Prevenção de Rastreamento Inteligente no Safari, mostrou que a publicidade pode continuar sendo eficaz e ainda aumentar a proteção da privacidade dos usuários. A Transparência no Rastreamento em Apps permite ao usuário fazer escolhas mais informadas sobre os aplicativos e as permissões que concede a eles. Com esse recurso, os usuários agora podem escolher se querem ser rastreados pelos apps. Para os aplicativos nos quais os usuários confiam e dão permissão, os desenvolvedores podem continuar o rastreamento.

Além de exigir permissão do usuário para o rastreamento, a Apple também introduziu mudanças recentes nas páginas de produtos da App Store para aumentar a transparência. Com a nova seção Privacidade do App, a App Store ajuda os usuários a entender melhor algumas das práticas de privacidade de cada aplicativo. A página de produto de cada app deve fornecer aos usuários um resumo fácil de visualizar das práticas de privacidade dos desenvolvedores. As páginas de detalhes incluem informações sobre os tipos de dado que o app coleta, como fotos, localização e informações de contato. As páginas também fornecem aos usuários detalhes adicionais sobre o que o desenvolvedor do aplicativo faz com cada tipo de informação, incluindo se é usado para rastreamento e se os dados estão vinculados ao usuário. Todos os desenvolvedores de apps, incluindo a Apple, são obrigados a divulgar informações sobre suas práticas de privacidade.

Graças à adição de ajustes de rastreamento em apps e informações de transparência e privacidade nas páginas de produtos da App Store, os usuários podem descobrir mais facilmente como seus dados pessoais são usados. Esse conhecimento revela práticas que antes eram obscuras e ficavam ocultas, oferecendo maior controle sobre os dados.

A Apple continuará desenvolvendo tecnologias inovadoras de privacidade e criando novas maneiras de manter suas informações pessoais seguras.

Um dia na vida de um anúncio



Leilões de anúncios

Quando Emma viu um anúncio de patinete na tela de John, não foi coincidência. Os anunciantes dão lances em um leilão para exibir seus anúncios no aparelho[37]. Veja uma explicação simplificada de como, em uma fração de segundo, o anúncio exibido na tela do aparelho foi escolhido:

1.
O desenvolvedor do app que Emma está usando contrata uma empresa de tecnologia de publicidade que leiloa o espaço publicitário em tempo real[14].

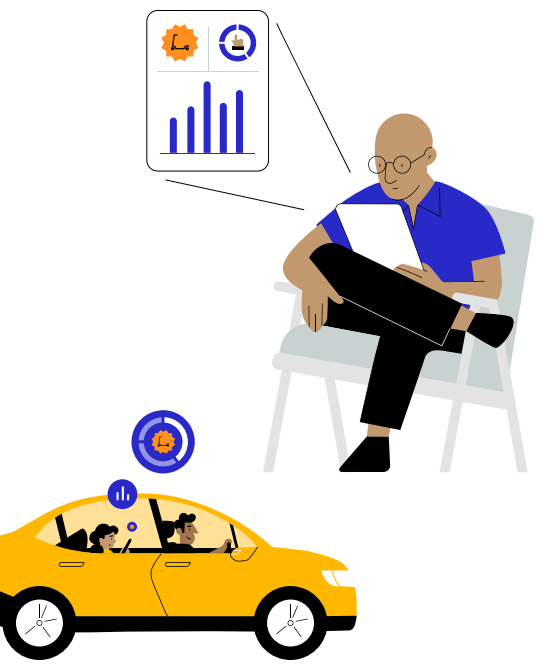
2.
Quando Emma abre o app, a rede de publicidade coleta dados de uso do aparelho de John (por exemplo, qual app ela está usando, sua localização e o ID de publicidade de John), bem como de terceiros, dependendo do ID de publicidade de John ou de outras informações que permitem o rastreamento[3].

3.
A rede de publicidade compartilha parte dessas informações, em especial o ID de publicidade, com anunciantes em potencial. Antes de dar um lance, os anunciantes geralmente tentam aprender o máximo possível sobre o usuário, a partir de seus próprios dados, e também usando dados pessoais coletados e agregados por meio de rastreamento e obtenção de perfil[3,15].

4.
Quanto mais as características de John e Emma — que derivam de seus dados — se alinham com o público-alvo do anunciante, mais os anunciantes darão lances pelo espaço do anúncio[15,38].

5
O anúncio do licitante vencedor para um patinete é exibido no aparelho que Emma está usando[14].

Como o processo de leilão de anúncios acontece em uma fração de segundo, compradores e vendedores coletam, trocam e usam dados pessoais para dar lances por espaço e exibir anúncios[14,15].



Atribuição de anúncios

Depois que o anúncio é exibido para Emma, as empresas de publicidade da fabricante de patinetes estão interessadas em medir o efeito que isso teve no comportamento dela. Esse processo é chamado de atribuição de anúncios.

- Para fazer isso, o anunciante tenta rastrear o comportamento no aparelho que Emma está usando, com o objetivo de coletar informações sobre o que ela faz na internet, em apps e até os lugares que ela frequenta offline.
- **Se o anúncio for de um produto,** o anunciante pode tentar descobrir se Emma visitou seu site ou loja física depois para fazer a compra[3].
- **Se o anúncio for de um app,** o anunciante tentaria descobrir se ela o instalou. Isso é chamado de atribuição de instalação do aplicativo[39].

Os anunciantes também usam a atribuição de anúncios para "otimizar" sua campanha publicitária, direcionando-a para grupos com os quais a campanha é mais eficaz[3].

Não precisa ser assim. Os anunciantes podem medir o impacto de suas campanhas publicitárias em relação aos grupos sem rastrear os usuários. A Apple vem trabalhando em ferramentas que fazem isso preservando a privacidade do usuário:

A **SKAdNetwork** permite aos anunciantes saber quantas vezes um app foi instalado depois que as pessoas viram anúncios dele. Com isso, podem medir o impacto de sua campanha publicitária. Mas essas informações não compartilham dados no nível do usuário ou aparelho, ou seja, os anunciantes não rastreiam os usuários.

O recurso **Private Click Measurement** em apps para iOS e iPadOS 14.5 permite aos anunciantes medir o impacto dos anúncios que levam os usuários a um site, minimizando a coleta de dados ao usar o processamento no aparelho. Depois que o usuário clica em um anúncio de produto em um app, o próprio navegador, por meio do Private Click Measurement, pode fornecer aos anunciantes informações de que um usuário clicou no anúncio e que isso levou a um determinado resultado no site, como uma visita ou compra – sem fornecer informações sobre quem especificamente clicou no anúncio.

Perguntas frequentes

Se eu selecionar “Pedir ao App para Não Rastrear”, poderei usar todos os recursos do aplicativo?

Sim. Desenvolvedores não podem exigir a ativação do rastreamento para liberar todos os recursos do app.

O que são e como são usados os identificadores?

Identificadores como o IDFA (Identificador para Anunciantes) e o endereço de e-mail ajudam a identificar um aparelho específico em uma rede. Eles também permitem ao anunciante criar um perfil detalhado de sua atividade em diferentes apps ou sites quando virem o identificador de seu aparelho e associarem sua atividade a ele.

O que é o IDFA (Identificador para Anunciantes)?

O IDFA (Identificador para Anunciantes) é um identificador controlável pelo usuário atribuído pelo iOS a cada aparelho. Como um identificador baseado em software, sem estar vinculado ao próprio hardware, o IDFA pode ser bloqueado para um app específico pelo usuário nas opções da Transparência no Rastreamento em Apps. Isso significa que o usuário tem controle sobre o rastreamento baseado em IDFA.

A Apple pode garantir que um aplicativo não esteja me rastreando se eu selecionar “Pedir ao App para Não Rastrear”?

Se você ativar essa opção, o desenvolvedor não poderá acessar o IDFA (Identificador para Anunciantes), que geralmente é usado para rastreamentos. O desenvolvedor do app também deve respeitar sua escolha, além do acesso ao identificador de publicidade. O desenvolvedor do app também deve respeitar sua escolha para além do acesso ao identificador de publicidade. Isso está incluído nas políticas com as quais o desenvolvedor concorda ao enviar um app para distribuição na App Store. Se descobrirmos que um desenvolvedor está rastreando usuários sem autorização, exigiremos a atualização de suas práticas para respeitar a escolha do usuário — caso contrário, o aplicativo pode ser rejeitado pela App Store.

Se eu usar minha conta de rede social para entrar em um app, a empresa de rede social pode rastrear o que eu faço nesse aplicativo?

Depende se você permitiu o rastreamento no app. Se você selecionar “Pedir ao App para Não Rastrear”, o aplicativo não deve permitir o rastreamento em apps ou sites de outras empresas para publicidade, nem compartilhar suas informações com um corretor de dados. Isso significa que eles não devem fornecer seus dados à empresa de rede social caso a intenção seja usá-los para fins de marketing.

Como a Apple garante a precisão das informações de privacidade nas páginas de produtos da App Store?

Da mesma forma que ocorre com as classificações etárias na App Store, os próprios desenvolvedores relatam suas práticas de privacidade. Se descobrirmos que um desenvolvedor forneceu informações imprecisas, entraremos em contato para garantir a precisão do conteúdo.

O que é um corretor de dados?

Em geral, o corretor de dados é uma empresa que coleta e vende, licencia ou de outra forma divulga a terceiros as informações pessoais de usuários finais específicos com os quais a empresa não mantém um relacionamento direto. Os corretores de dados são definidos por lei em algumas jurisdições.

Fontes

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

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

3. Competition & Markets Authority, "Online platforms and digital advertising", 1º de julho de 2020.

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

5. AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC", 24 de setembro de 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, arquivado em 25 de maio de 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*, 9 de novembro de 2012.

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

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

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

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

16. Edelman, Gilad, "Can Killing Cookies Save Journalism?", *WIRED*, 5 de agosto de 2020.

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

18. 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*, 21 de julho de 2018.

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

20. Schechner, Sam, e Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook", *The Wall Street Journal*, 22 de fevereiro de 2019.

21. O'Reilly, Lara, "New Facebook Tools Help Marketers Serve Ads to People Most Likely to Spend Money", *The Wall Street Journal*, 12 de junho de 2017.

22. Ramirez, Edith, Julie Brill, et al., "Data Brokers: A Call for Transparency and Accountability", *Federal Trade Commission*, maio de 2014.

23. Facebook for Business, "Measuring Conversions on Facebook, Across Devices and in Mobile Apps", 14 de agosto de 2014.

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

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

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

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

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

29. Thompson, Stuart A., "These Ads Think They Know You", *The New York Times*, 30 de abril de 2019.

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

31. Leetaru, Kalev, "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly

Wrong", *Forbes*, 5 de abril de 2018.

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

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

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

35. 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.

36. Hern, Alex, "'Anonymous' browsing data can be easily exposed, researchers reveal", *The Guardian*, 1º de agosto de 2017.

37. Se o usuário associado ao ID Apple registrado em um aparelho tiver 18 anos ou menos, o acesso ao IDFA é desabilitado por padrão e não pode ser concedido a nenhum desenvolvedor.

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, 4 de fevereiro de 2019.

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

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

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