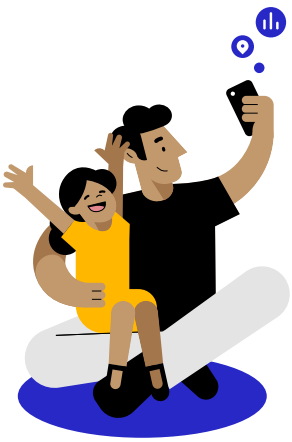


Verilerinizin Bir Günü

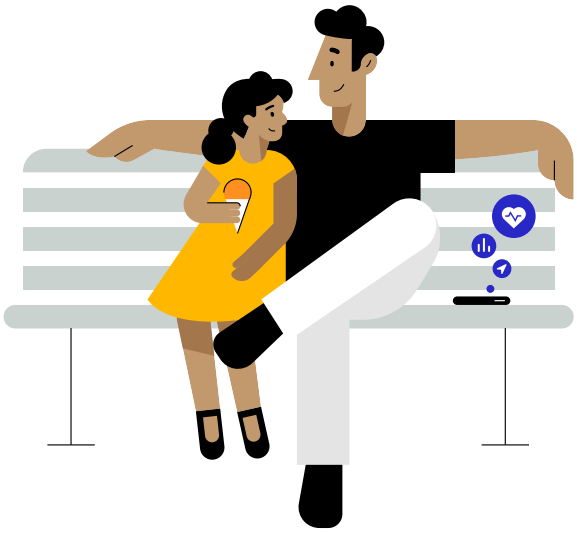
Parkta Baba-Kız Günü

Nisan 2021

“Bence insanlar gayet akıllı ve aralarında diğerlerinden daha fazla veri paylaşmak isteyenler de var. Onlara sorun. Her seferinde sorun. Sorularınızdan bıkıp yeter diyene kadar sormaya devam edin. Verileriyle tam olarak ne yapacağınızı bilmelerini sağlayın.”

Steve Jobs

All Things Digital Konferansı, 2010



Son on yıldır, farkında olmadığımız fakat son derece geniş bir sektör giderek artan miktarda kişisel veri toplamaya devam ediyor.[1,2] Web siteleri, uygulamalar, sosyal medya şirketleri, veri aracıları ve reklam teknolojileri şirketleri kullanıcıları online ve offline olarak takip edip onların kişisel verilerini topluyor. Daha sonra bu veriler birleştiriliyor, paylaşılıyor, kümeleniyor, gerçek zamanlı açık artırmalarda kullanılıyor ve yılda 227 milyar ABD doları değere ulaşan bir sektöre kaynak sağlıyor.[1] Bu durum her gün, insanlar günlük yaşantılarını sürdürürken, çoğunlukla onların bilgisi veya izni olmadan devam ediyor.[3,4] Bu sektörün, normalde parkta hoş bir gün geçiren bir baba ve kızı hakkında neler öğrenebildiğine bir bakalım.

Biliyor muydunuz?

Takipçiler her gün kullandığınız uygulamalarda yerleşik olarak bulunuyor. Bir uygulamada ortalama 6 adet takipçi yer alıyor.[3] Popüler Android ve iOS uygulamalarının çoğunda yerleşik olarak takipçiler bulunuyor.[5,6,7]

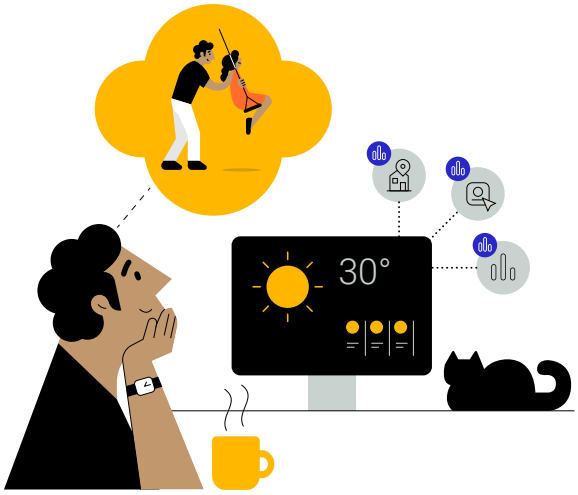
Takipçiler genellikle geliştiricilerin uygulamaları hazırlamasına yardımcı olan üçüncü taraf kodlarında yer alıyor. Geliştiriciler takipçi ekleyerek, sizin onlarla paylaştığınız verileri üçüncü tarafların da toplamasına, farklı uygulamalara bağlamasına ve sizinle ilgili toplanan diğer verilerle ilişkilendirmesine izin veriyor.

Veri aracıları doğrudan ilişkileri olmayan belirli kişiler hakkındaki kişisel verileri toplayıp üçüncü taraflara satıyor, açıklıyor veya bu veriler için kullanım yetkisi veriyor.[3]

Online ve offline veri toplayan yüzlerce veri aracısı var.[8]
Tek bir veri aracısı, dünya genelinde 700 milyon tüketiciye dair veri topluyor, 5000 adede kadar karakteristik özellikle tüketici profilleri oluşturuyor.[9]

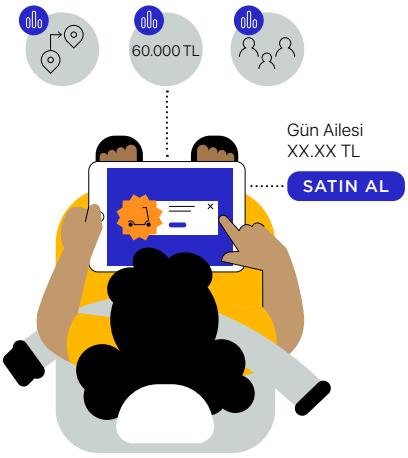
Yapılan bir araştırmada, çocuklara yönelik uygulamaların yaklaşık %20'sinde geliştiricilerin, kimliği ortaya çıkarabilecek bilgileri ebeveynlerin onayı olmadan toplayıp paylaştığı tespit edildi.[10]

Günün her saati, internette kullanıcılara milyarlarca dijital reklam gösteriliyor.[11,12,13]
Bir reklamın yüklendiği milisaniyeler içinde gerçek zamanlı bir açık artırma gerçekleşiyor. Reklam verenler genellikle kullanıcının takip ettikleri kişisel verilerine göre, bu sürede reklam alanı için teklif veriyor.[14,15]



Murat kızıyla parkta bir gün geçirmeyi planlıyor

Murat ve 7 yaşındaki kızı Damla günü birlikte geçiriyor. Murat sabah bilgisayarından hava durumuna bakıp haberleri okuduktan sonra akıllı telefonundaki harita uygulamasını açıp kızının okulunun yanındaki parka kadar trafiğin durumunu kontrol ediyor. Murat'ın telefonundaki 4 adet uygulama yoldayken arka planda belirli aralıklarla konum verilerini takip edip topluyor.[16,17,18] Veriler aygıttan alındıktan sonra, uygulama geliştiricileri bunları Murat'ın daha önce hiç duymadığı gizli üçüncü taraf veri aracılarına satıyor.[16,17] Toplanan konum verileri anonim olsa da veri aracıları, kullanıcı takibi sayesinde Murat'ın bu uygulamalardaki konum geçmişini diğer uygulamalardan toplanan bilgilerle eşleştiriyor.[16,19] Böylece farklı uygulamalardan ve farklı kaynaklardan takip edilen bilgiler herhangi bir şirket veya kurum tarafından satın alınabiliyor. Bu bilgilerle Murat'ın adım adım günlük hareketlerini de içeren kapsamlı bir profil oluşturulabiliyor.[3,16]



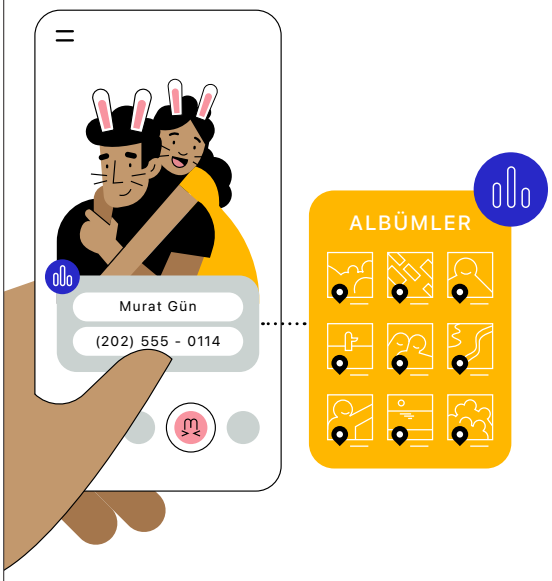
Damla parka giderken yolda oyun oynuyor

Murat arabayla parka giderken kızının tablette oyun oynamasına izin veriyor. Kızı uygulamayı açtığında bir scooter reklamıyla karşılaşıyor. Bu tesadüfen karşısına çıkan bir şey değil. Uygulama yüklendiği anda reklam alanı için bir açık artırma gerçekleşiyor.[14] Scooter şirketi adına çalışan reklam şirketleri, aracılar üzerinden reklam fırsatı hakkında bilgi alıyor.[15] Murat ve Damla hakkında toplanan kişisel verileri kullanarak reklama teklif veriyorlar.[15] Scooter şirketinin reklam ortakları, Murat ve Damla'nın reklamı gördükten sonraki davranışları hakkında da bilgi toplamaya devam ediyor. Reklama tıklayıp tıklamadıklarını veya scooter satın alıp almadıklarını belirliyorlar.[3] Ve Murat'ın aygıtlarındaki farklı uygulamalar ve web sitelerinde takibi sürdürerek Murat ve Damla'ya her yoldan scooter reklamı göstermeye devam edecekler.[3,20,21]

Bazı uygulamalar hizmetlerini sunmak için gerekenden daha fazla veriye erişim talebinde bulunuyor. Örneğin, bir klavye uygulaması tam konuma erişmek isteyebiliyor.[5]

Elde edilen bilgiler reklam ağlarına, reklam yayıncılarına, ilişkilendirme ve ölçüm sağlayıcılarına, veri aracılarına, başka özel şirketlere ve hatta devlet kurumlarına gidebiliyor.[3,15,40,41,42] Sosyal medya ve reklam teknolojileri şirketleri, bilgi alırken kullanıcıya belirttikleri amaçlar dışında kişisel veri topladıkları için bugüne kadar milyonlarca ABD doları cezaya çarptırıldı veya ceza ödemek zorunda kaldı.[22,23,24,25]

Veri aracıları, topladıkları verileri kullanıcıları belirli niteliklerle ilişkilendirmek için kullanıyor. Ardından kullanıcılar, "kilo vermeye çalışan fakat hamur işinden vazgeçmeyenler" gibi son derece ayrıntılı pazar segmentlerine ayrılıyor.[26] Ancak bu profiller genellikle doğru olmuyor. Yapılan bir araştırmada, bu niteliklerin %40'ının hatalı olduğu belirlendi.[27,28]

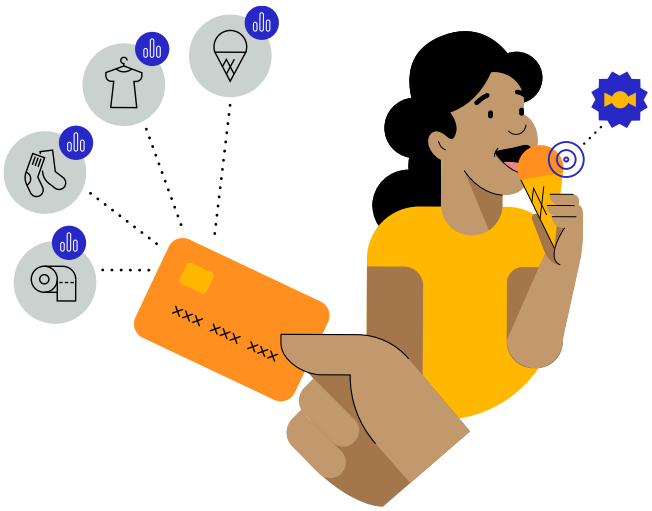


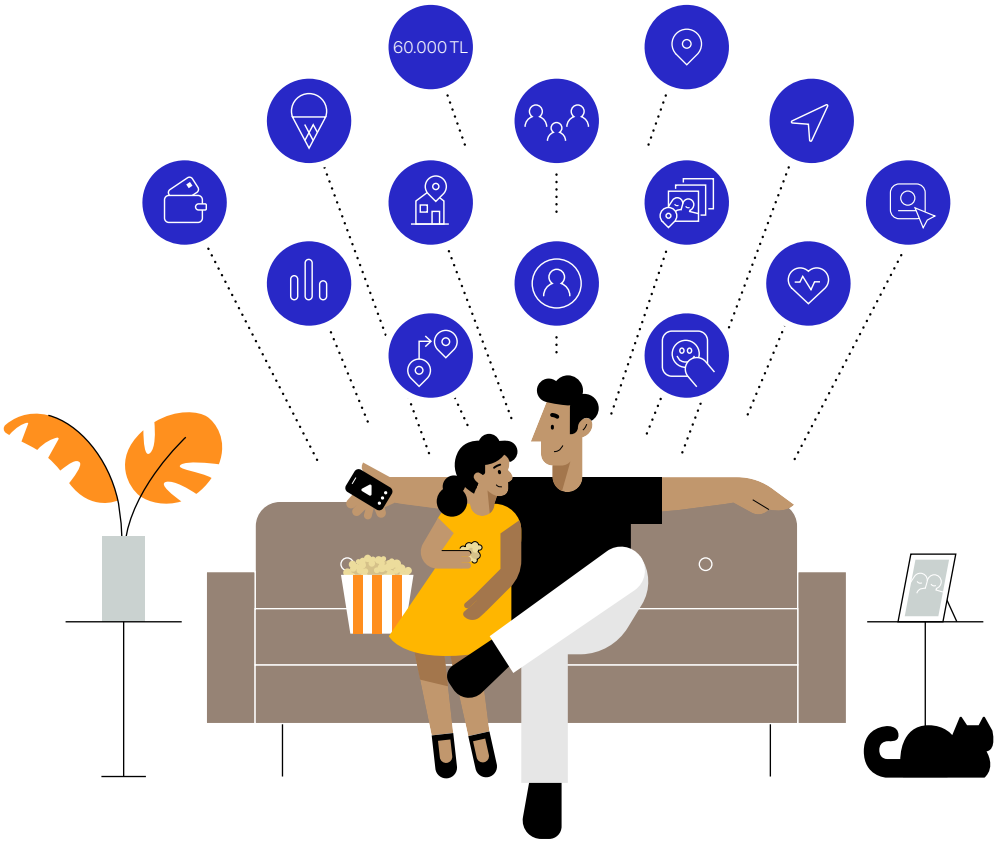
Murat ve Damla parkta selfie çekiyor

Murat ve Damla daha sonra parkta selfie çekiyor. Bir fotoğraf filtresi uygulamasını kurcalayıp fotoğrafta kendilerine tavşan kulakları eklemeye karar veriyorlar. Filtre uygulaması ise yalnızca parkta çekilen bu selfie'ye değil, aygıttaki tüm fotoğraflara ve bunlara bağlı üst verilere erişebiliyor.[29,30] Murat bu fotoğrafı bir sosyal medya uygulamasında paylaşıyor. Bu uygulama da mail adresi, telefon numarası veya bir reklam tanıtıcısı kullanarak Murat'ın o anki online faaliyetlerini diğer uygulamaların topladığı demografi bilgileri ve satın alma alışkanlıkları gibi birçok veriyle eşleştiriyor.[3]

Eve dönüşte dondurma molası

Murat ve Damla, eve dönerken kendilerine ödül olarak dondurma molası veriyor. Murat dondurmanın ücretini kredi kartıyla ödüyor ve böylece tercihlerine dair kapsamlı veri profiline dükkanın konumu ve harcanan para miktarı gibi yeni bilgiler ekleniyor.[31,32,33] Murat'ın konumunu takip eden uygulamalardan biri Murat ve Damla'nın bir oyuncakçıda da durduğunu gözlemliyor.[3] Ailenin gün içinde nerelerde alışveriş yaptığına dair bilgi, veri aracılarına iletiliyor. Onlar da bu bilgiyi Murat'ın küçük bir kızı olduğu bilgisiyle birleştirerek, aygıta şekerlemeler ve ziyaret edilen oyuncakçı için hedeflenmiş reklamlar gönderiyor.[17]





Günün sonunda, dünyanın her yerinden Murat'ın hiç etkileşime girmediği birçok şirket, profillerini Murat ve kızına dair bilgilerle güncellemiş oluyor. Bu şirketler ailenin evinin nerede olduğunu, ziyaret ettikleri parkı, okudukları haber sitelerini, aradıkları ürünleri, izledikleri reklamları, satın alma alışkanlıklarını ve girdikleri mağazaları öğreniyor.[3,34] Bu veriler, Murat ve kızının gün boyu kullandığı uygulamalardan ve diğer kaynaklardan izlenip toplanıyor. Murat gün içinde ne kadar verinin toplandığının bilmiyor, bunu her zaman kontrol edemiyor ve bu işlem için izin de vermiş değil.[3,4] Akşam rahatlamak için akıllı TV'deki uygulamadan bir çocuk filmi ararlarken takip, veri toplama, açık artırma ve yeniden hedefleme döngüsü de aralıksız devam ediyor.[35,36]

Apple'ın sunduğu gizlilik özellikleri ve kullanıcıların gizliliğini korumak için yaptıkları hakkında daha fazla bilgi edinmek için **apple.com/tr/privacy** sayfasını ziyaret edebilirsiniz.

Safari'nin gizliliğinizi nasıl koruduğu hakkında daha fazla bilgi edinmek için **Safari Bilgi Sayfası**'nı okuyun.

Apple'ın konum verilerinizi nasıl koruduğu hakkında daha fazla bilgi edinmek için **Konum Servisleri Bilgi Sayfası**'nı okuyun.

Apple'ın gizlilik prensipleri

Apple gizliliğin temel bir insan hakkı olduğuna inanıyor. Ürünlerimizi ve hizmetlerimizi tasarlarken dört temel gizlilik prensibimize uyuyoruz:

Veri Miktarını En Aza İndirme
Belirli bir hizmeti sunmak için yalnızca gereken en az miktarda veriyi toplamak.

Aygıtta İşleme
Verileri Apple sunucularına göndermek yerine mümkün olan her an aygıtta işleyerek kullanıcı gizliliğini korumak ve toplanan veri miktarını en aza indirmek.

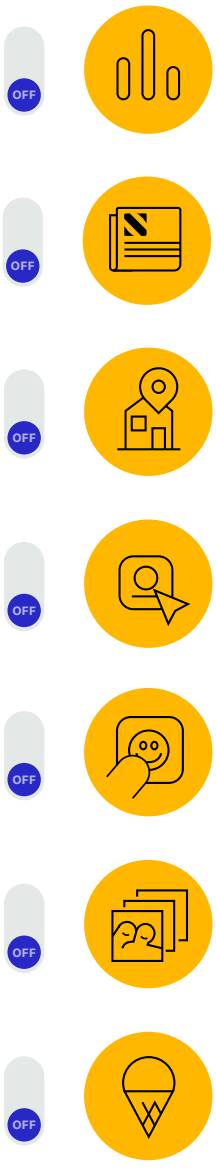
Kullanıcı Şeffaflığı ve Denetimi
Kullanıcıların hangi verilerin paylaşıldığını ve verilerin nasıl kullanıldığını bilmesini sağlamak ve onlara bunu denetleme imkanı vermek.

Güvenlik
Verileri güvende tutmak için donanım ve yazılımı birlikte kullanmak.

Bu dört prensiple, Apple'ın hedefi her zaman kullanıcıların verilerini güvenle, anladıkları ve denetleyebildikleri bir biçimde, diledikleri gibi paylaşmalarını sağlamaktır. İşte bu nedenle Apple son yirmi yıldır tüm ürün ve hizmetlerinde kullanıcı gizliliğini koruyacak yenilikler yapmayı sürdürüyor. Örneğin, uygulamalarımızda, tarayıcılarımızda ve online hizmetlerimizde topladığımız veri miktarını azaltmak için aygıt içi akıllı teknolojilerden ve diğer özelliklerden yararlanıyoruz. Tüm uygulamalarımız ve hizmetlerimiz için kullanacağımız tek bir geniş kapsamlı kullanıcı veri profili oluşturmuyoruz.

Apple'ın gizlilik özellikleri Murat'a daha fazla şeffaflık ve verilerinin üzerinde daha fazla denetim imkanı sunuyor

Murat ve Damla'nın hikayesi, Apple olarak çözmek için çalıştığımız gizlilik sorunlarını yansıtıyor.



Murat kızıyla parkta bir gün geçirmeyi planlıyor

Murat bilgisayarında hava durumuna bakmak için Safari tarayıcısını kullanmış olsaydı Akıllı Takip Önleme özelliği bu hareketin takip edilmesini kendiliğinden engelleyecekti.

Murat sabah haberleri Apple News üzerinden okumuş olsaydı Apple onun kim olduğunu bilmeden veya ne okuduğunu öğrenmeden ilgi alanlarına yönelik içerikler sunacaktı.

Murat trafik durumuna bakmak için Apple Harita uygulamasını kullanmış olsaydı konum verileri, düzenli olarak sıfırlanan ve Murat ile bağlantılı olmayan rastgele bir tanıtıcıyla ilişkilendirilecekti. Sonuç olarak konumunu Murat'tan başka kimse bilmeyecekti.

Murat iPhone kullansaydı hangi uygulamaların arka planda konum verilerine eriştiği kendisine belirli aralıklarla bildirilecekti. Bir uygulamayla konum bilgilerini paylaşmadan önce, Murat konumunu sadece bir kez paylaşmayı veya yaklaşık konumunu paylaşmayı tercih edebilecekti.

Damla parka giderken yolda oyun oynuyor

iPad'e gelecek Şeffaf Uygulama Takibi özelliği sayesinde Murat, oyunun Damla'nın başka şirketlere ait uygulamalarda ve web sitelerinde yaptıklarını takip etmesine izin vermemeyi seçebilecek.

Apple'ın SKAdNetwork API'ını kullanan reklam ağları, Murat'ın aygıtına kadar takip edilebilen bilgilere erişmeden reklamlarının genel etkinliğini ölçebilecek.

Murat ve Damla parkta selfie çekiyor

Murat iPhone kullansaydı filtre uygulamasına, tüm fotoğraf arşivi yerine yalnızca çekilen selfie'ye erişim hakkı verebilecekti.

Eve dönüşte dondurma molası

Murat dondurmanın ücretini Apple Card ile ödemiş olsaydı bankası bu işlemin bilgilerini pazarlama amacıyla kullanmayacaktı. Murat Apple Pay kullanmış olsaydı Apple'ın kullandığı aygıt içi akıllı teknolojiler sayesinde nerede alışveriş yaptığı, ne satın aldığı ve ne kadar para harcadığı hakkında Apple'a bilgi vermeden, iPhone'undan işlem geçmişini görebilecekti.

Sonuç olarak, Apple ürünleri ve gizlilik özellikleri sayesinde Murat, gün içinde ne kadar veri paylaştığı ve bunların nasıl kullanıldığı hakkında daha şeffaf bilgilere ve daha geniş denetim imkanına sahip olacaktı.

Şeffaf Uygulama Takibi ve App Store'daki yeni gizlilik bilgileri bölümü

Apple, uygulama ekosisteminde kullanıcıların gizliliğini korumak için yeni adımlar atıyor. Sayısı her geçen gün artan karmaşık yapılar tüketicilerin kişisel verilerine erişip bunları takip ederek maddi gelir elde ederken, Apple kullanıcılara daha fazla şeffaflık, görünürlük ve seçenek sunarak onların daha bilinçli karar vermesini ve gizlilikleri üzerinde daha fazla kontrole sahip olmasını sağlayan iki yeni özellik sunuyor.

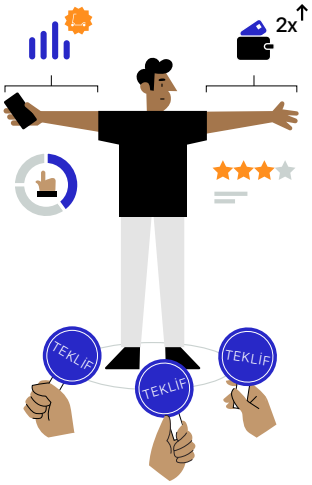
Yakında bir sonraki beta güncellemesiyle kullanılmaya başlanacak Şeffaf Uygulama Takibi özelliği, uygulamaların kullanıcı verilerini diğer şirketlere ait uygulamalarda veya web sitelerinde takip etmek için izin almalarını gerektirecek. Kullanıcılar, Ayarlar bölümünün altında hangi uygulamaların takip izni istediğini görüp uygun gördükleri değişiklikleri yapabilecek. Dünyanın her yerinden gizlilik hakları savunucularının şimdiden desteklediği bu zorunluluk ilkbaharda yayınlanacak iOS 14, iPadOS 14 ve tvOS 14 sürümleriyle geniş bir alanda kullanıma sunulacak. Apple bu özelliği tasarlarken kullanıcılara daha fazla şeffaflık ve denetim imkanı sunmanın yanı sıra reklamların uygulamaları ve web içeriklerini desteklemek için uygun ve geçerli bir yöntem olarak kullanılmaya devam etmesini hedefledi. Safari Akıllı Takip Önleme gibi daha önce sunulan özellikler, kullanıcı gizliliğini daha iyi koruyan önlemler alındığında da reklamların başarılı olmayı sürdürebileceğini gösterdi. Şeffaf Uygulama Takibi özelliği, kullanıcıların uygulamalar ve bunlara verdikleri izinler hakkında daha bilinçli tercihler yapmasını sağlıyor. Şeffaf Uygulama Takibi ile kullanıcılar artık uygulamaların kendilerini takip etmelerine izin verip vermemeyi seçebiliyor. Kullanıcıların güvendiği ve takip izni verdiği uygulamalarda geliştiriciler takip işlemlerine devam edebiliyor.

Takip için kullanıcı izni zorunluluğuna ek olarak, Apple ayrıca şeffaflığı artırmak için App Store ürün sayfalarında da kısa süre önce bazı değişikliklere gitti. App Store'da-ki yeni Uygulama Gizliliği bölümü sayesinde, kullanıcılar uygulamaların gizlilik şartlarının bazılarını daha iyi anlayabiliyor. Geliştiriciler her uygulamanın ürün sayfasında gizlilik şartlarını kullanıcıların kolayca görebileceği şekilde özetlemek zorunda. Ayrıntıları içeren sayfalarda uygulamanın topladığı fotoğraf, konum veya iletişim bilgileri gibi veri türleri hakkında bilgiler yer alıyor. Kullanıcılara bu sayfalarda uygulama geliştiricilerin topladıkları her tür veriyi nasıl kullandıklarına ilişkin ek ayrıntılar sunuluyor. Toplanan verilerin takip için mi kullanıldığı ve kullanıcıyla ilişkilendirilip ilişkilendirilmediği de bu sayfalarda görülebiliyor. Apple dahil tüm uygulama geliştiricilerinin, gizlilik şartlarıyla ilgili bilgileri raporlaması gerekiyor.

Uygulama takip ayarlarının eklenmesi ve App Store'daki ürün sayfalarında şeffaflık ve gizlilik bilgilerinin yer almasıyla birlikte, kullanıcılar kişisel verilerinin nasıl kullanıldığını çok daha kolay bir şekilde öğrenebiliyor. Daha önce şeffaf olmayan, gizli yöntemler açığa çıkarılarak kullanıcılara verileri üzerinde daha fazla denetim imkanı veriliyor.

Apple gizlilikle ilgili yenilikçi teknolojiler geliştirmeye ve kişisel bilgilerinizi güvende tutacak yeni yollar bulmak için çalışmaya devam edecek.

Reklamın Bir Günü



Reklam Açık Artırmaları

Damla'nın, Murat'ın ekranında scooter reklamı görmesi bir tesadüf değildi. Reklamverenler bir aygıtta reklamlarını göstermek için açık artırmada teklif verir. 37 Aygıtın ekranında gösterilen reklamın bir saniyeden de kısa süre içinde nasıl belirlendiğini kısaca açıklayalım:

1.
Damla'nın kullandığı uygulamanın geliştiricisi, reklam alanlarını gerçek zamanlı olarak açık artırmaya çıkaran bir reklam teknolojileri şirketiyle çalışıyor.[14]

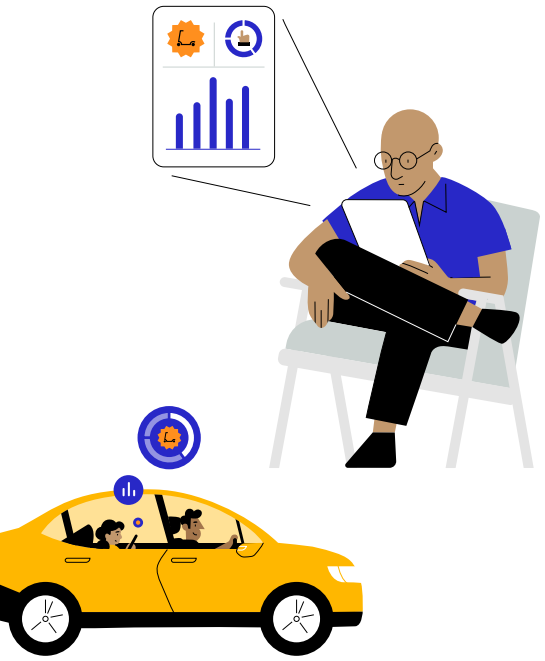
2.
Damla uygulamayı açtığında reklam ağı, Murat'ın reklam kimliğine veya takibe izin verilen diğer bilgilerine göre aygıtın kullanım verilerini (örneğin Damla'nın hangi uygulamayı kullandığını, konumunu ve Murat'ın reklam kimliğini) ve üçüncü taraflardan topladığı verileri alıyor.[3]

3.
Reklam ağı, başta reklam kimliği olmak üzere bu bilgilerin bazılarını potansiyel reklamverenlerle paylaşıyor. Reklamverenler teklif vermeden önce genellikle kullanıcı hakkında olabildiğince çok şey öğrenmek istiyor. Bunun için kendi verilerinin yanı sıra takip ve profil çıkarmayla toplanıp kümelenmiş kişisel verilerden yararlanıyorlar.[3,15]

4.
Murat ve Damla'nın verilerinden çıkarılan karakteristik özellikler reklamverenin hedef kitlesiyle ne kadar örtüşüyorsa, reklam alanı için o kadar fazla teklif geliyor.[15,38]

5
Kazanan teklifi yapan şirketin scooter reklamı Damla'nın kullandığı cihazda gösteriliyor.[14]

Reklam açık artırma süreci bir saniyeden de kısa bir sürede gerçekleştiğinden, hem satın alanlar hem de satıcılar reklam alanına teklif vermek ve reklam göstermek için, kişisel verileri topluyor, takas ediyor ve kullanıyor.[14,15]



Reklam İlişkilendirme

Reklamı kullanıcıya gösterilen scooter şirketiyle birlikte çalışan reklamverenler, bu reklamın Damla'nın davranışlarına nasıl etki ettiğini ölçmek istiyor. Bu işleme reklam ilişkilendirme adı veriliyor.

Reklamveren şirket bunun için Damla'nın kullandığı aygıttaki hareketleri takip etmeye çalışıyor. Damla'nın internette ve uygulamalarda ne yaptığına, hatta nerede offline olduğuna dair bilgi topluyor.

- **Reklam bir ürün içinse,** reklamveren şirket kullanıcının daha sonra markanın web sitesini veya mağazasını ziyaret ederek ürünü satın alıp almadığını takip etmeye çalışabiliyor.[3]
- **Reklam bir uygulama içinse,** reklamveren şirket kullanıcının uygulamayı kurup kurmadığını takip etmeye çalışıyor. Buna uygulama yükleme ilişkilendirmesi deniyor.[39]

Reklamverenler reklam ilişkilendirme işlemini, reklam kampanyalarını daha etkili olacakları gruplara göre düzenlemek için de kullanıyor.[3]

İşlerin böyle yürümesi gerekmiyor. Reklamverenler, reklam kampanyalarının belirli gruplara etkisini kullanıcıları takip etmeden de ölçebilir. Apple bunun kullanıcıların gizliliğini korurken de yapılabilmesini sağlayan araçlar üzerinde çalışıyor:

SKAdNetwork, reklam görüldükten sonra uygulamanın kaç kere yüklendiğini reklamverenlere bildiriyor. Böylece reklam kampanyasının etkisi ölçülebiliyor. Ancak bu bilgi, reklamverenler kullanıcıları takip etmesin diye hiçbir kullanıcı verisi veya aygıt düzeyinde veri paylaşmayacak şekilde tasarlanıyor.

Gizli Tıklama Ölçümü, reklamverenlere iOS ve iPadOS 14.5'teki uygulamalarda kullanıcıları bir web sitesine yönlendiren reklamların etkisini ölçme imkanı veriyor. Aygıtta işleme teknolojisinden yararlanan bu yöntem, toplanan veri miktarını en aza indiriyor. Kullanıcı uygulamada bir ürün reklamına tıkladığında, Gizli Tıklama Ölçümü özelliğini kullanan web tarayıcısı reklamverenlere kullanıcının reklama tıkladığını ve bunun web sitesine ziyaret veya satın alma gibi bir sonuca neden olduğunu bildiriyor. Tüm bu veriler reklama tam olarak kimin tıkladığı hakkında bilgi vermeden iletiliyor.

Sık Sorulan Sorular

"Uygulama Beni Takip Etmesin" seçeneğini belirlediğimde uygulamanın tüm özelliklerini kullanmaya devam edebilecek miyim?

Evet. Uygulama geliştiricileri, uygulamanın tüm özelliklerinden yararlanmanız için takibe izin vermenizi zorunlu kılamazlar.

Kimlik tanıtıcılar nedir ve nasıl kullanılır?

Reklamverenler İçin Kimlik Tanıtıcı (IDFA) ve mail adresleri gibi kimlik tanıtıcılar, belirli bir aygıtı bir ağ içinde tanımlamaya yardımcı olur. Aygıt tanıtıcınızı gören reklamveren, yaptığınız aktiviteyi bununla ilişkilendirir. Aygıt tanıtıcıları, reklamverenlerin farklı uygulamalarda veya web sitelerinde yaptıklarınızdan yola çıkarak ayrıntılı bir profilinizi oluşturmalarını da sağlar.

Reklamverenler İçin Kimlik Tanıtıcı (IDFA) nedir?

Reklamverenler İçin Kimlik Tanıtıcı (IDFA), iOS'in her aygıta atadığı, kullanıcı tarafından kontrol edilebilen bir kimlik tanıtıcıdır. Donanıma bağlı olmak yerine yazılım tabanlı bir kimlik tanıtıcı olan IDFA, kullanıcı tarafından Şeffaf Uygulama Takibi özelliği aracılığıyla belirli bir uygulama için engellenebilir. Bu da kullanıcıya IDFA tabanlı takip üzerinde denetim imkanı verir.

"Uygulama Beni Takip Etmesin" seçeneğini belirlediğimde Apple bir uygulamanın beni takip etmediğinin garantisini verebilir mi?

"Uygulama Beni Takip Etmesin" seçeneğini belirlediğinizde geliştirici, reklamverenler için kimlik tanıtıcıya (IDFA) erişemez. Bu kimlik tanıtıcı genellikle takip için kullanılır. Reklam tanıtıcısının dışında uygulama geliştiricisinin tercihinize saygı duyması gereklidir. Bu durum, geliştiricilerin uygulamalarını App Store'da dağıtmak için başvuru yaparken kabul ettikleri politikalarda şart koşuluyor. Bir geliştiricinin takip edilmek istemeyen bir kullanıcıyı takip ettiğini öğrendiğimizde, ondan tercihinize saygı duyarak uygulamayı güncellemesini talep ediyoruz. Bu gerçekleşmediği takdirde uygulamayı App Store'dan çıkarabiliyoruz.

Bir uygulamada oturum açmak için sosyal medya hesabımı kullanırsam sosyal medya şirketi uygulamada yaptıklarımı takip edebilir mi?

Bu durum, uygulamanın sizi takip etmesine izin verip vermemenize bağlıdır.
"Uygulama Beni Takip Etmesin" seçeneğini belirlediyseniz uygulamanın reklam amacıyla sizi diğer şirketlerin uygulamalarında veya web sitelerinde takip etmemesi ya da bilgilerinizi veri aracılarıyla paylaşmaması gerekir. Bu da bilgilerinizi reklam amacıyla kullanacaklarsa sosyal medya şirketine sunmamaları gerektiği anlamına gelir.

Apple, App Store ürün sayfalarındaki gizlilik bilgilerinin doğruluğundan nasıl emin oluyor?

App Store'daki Yaş Derecelendirmelerine benzer bir şekilde, geliştiriciler kendi gizlilik şartlarını raporluyor. Bir geliştiricinin hatalı bilgi verdiğini öğrendiğimizde bilginin doğru olmasını sağlamak için onlarla birlikte çalışıyoruz.

Veri aracısı nedir?

Genel olarak, işletmelerin doğrudan ilişkisinin olmadığı belirli son kullanıcılara ait kişisel bilgileri düzenli olarak toplayan ve satan, üçüncü taraflara açıklayan veya bu bilgiler için kullanım izni veren şirketlere veri aracısı adı verilir. Veri aracıları bazı ülkelerde yasayla tanımlanmıştır.

Kaynaklar

1. Gröne, Florian, Pierre Péladeau ve ark., "Tomorrow's data heroes" (Yarının veri kahramanları), *Strategy+Business*, 19 Şubat 2019.

2. Reinsel, David, John Gantz ve ark., "The Digitization of the World: From Edge to Core" (Dünyanın Dijitalleşmesi: Kenardan Merkeze), Kasım 2018.

3. Competition & Markets Authority, "Online platforms and digital advertising" (Online platformlar ve dijital reklamcılık), 1 Temmuz 2020.

4. Hitlin, Paul ve Lee Rainie, "Facebook Algorithms and Personal Data" (Facebook Algoritmaları ve Kişisel Veriler), *Pew Research Center*, 16 Ocak 2019.

5. AppCensus, "1,000 Mobile Apps in Australia: A Report for the ACCC" (Avustralya'daki 1.000 Mobil Uygulama: ACCC İçin Bir Rapor), 24 Eylül 2020.

6. Binns, Reuben, Ulrik Lyngs ve ark., "Third Party Tracking in the Mobile Ecosystem" (Mobil Ekosistemde Üçüncü Tarafların Yaptığı Takip), *10. ACM Web Bilimleri Konferansı konuşmaları*, 2018, sayfa 23-31.

7. MightySignal, "Most Used SDKs in Top 200 Free iOS Apps" (En İyi 200 Ücretsiz iOS Uygulamasında En Çok Kullanılan Yazılım Geliştirme Kitleri), mightysignal.com/top-ios-sdks.

8. Kaliforniya Eyaleti Adalet Departmanı, "Data Broker Registry" (Veri Aracıları Kayıt Defteri), oag.ca.gov/data-brokers.

9. Acxiom Corporation, 2018 Form 10-K, kayıt tarihi 25 Mayıs 2018, www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm.

10. Reyes, Irwin, Primal Wijesekera ve ark., "'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale" ('Kimse Çocukları Düşünmeyecek mi?' COPPA Uyumluluğunun Her Ölçekte İncelenmesi), *Gizliliği Artıran Teknolojilerle İlgili Tutanaklar*, Cilt 2018, No. 3, 2018, sayfa 63-83.

11. Edwards, Jim, "Here's The Staggering Number of Ads Facebook Serves On Its Exchange Every Day" (Facebook'un Kendi Borsasında Her Gün Sunduğu Şaşırtıcı Reklam Sayısı), *Business Insider*, 9 Kasım 2012.

12. Kim, Larry, "How Many Ads Does Google Serve In A Day?" (Google Bir Günde Kaç Reklam Sunuyor?), *Business 2 Community*, 2 Kasım 2012.

13. Deighton, John ve Leora Kornfeld, "The Socioeconomic Impact of Internet Tracking" (İnternet Takibinin Sosyoekonomik Etkisi), *Interactive Advertising Bureau*, Şubat 2020.

14. Hwang, Tim, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet (Yüksek Riskli İlgi Krizi: Reklamcılık ve İnternetin Kalbindeki Saatli Bomba)*, FSG Originals, 13 Ekim 2020.

15. Avustralya Rekabet ve Tüketici Komisyonu, "Digital advertising services inquiry - Interim report" (Dijital reklam hizmetleri soruşturması - Ara rapor), Aralık 2020.

16. Thompson, Stuart A. ve Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy" (On İki Milyon Telefon, Bir Veri Seti, Sıfır Gizlilik), *The New York Times*, 19 Aralık 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" (Attığınız her adım: Şirketler sizi ve çevrenizdeki herkesi farkınızda olmadan hedeflemek için coğrafi konum verilerini nasıl kullanıyor), The Boston Globe, 21 Temmuz 2018.

18. Vitaldevara, Krish, "Safer and More Transparent Access to User Location" (Kullanıcı Konumuna Daha Güvenli ve Daha Şeffaf Erişim), *Android Developers Blog*, 19 Şubat 2020.

19. Schechner, Sam ve Mark Secada, "You Give Apps Sensitive Personal Information. Then They Tell Facebook" (Siz Uygulamalara Hassas Kişisel Bilgilerinizi Veriyorsunuz. Onlar da Bunları Facebook'a Anlatıyor), *The Wall Street Journal*, 22 Şubat 2019.

20. Facebook for Business, "Measuring Conversions on Facebook, Across Devices and in Mobile Apps" (Facebook'ta, Aygıtlar Arasında ve Mobil Uygulamalarda Dönüşüm Ölçümü), 14 Ağustos 2014.

21. Bender, Brad, "New digital innovations to close the loop for advertisers" (Reklamverenler için döngüyü tamamlayan yeni dijital inovasyonlar), *Google Ads & Commerce Blog*, 26 Eylül 2016.

22. Federal Ticaret Komisyonu, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (FTC Facebook'a 5 Milyar ABD Doları Ceza Kesti ve Yeni Gizlilik Kısıtlamaları Getirdi), 24 Temmuz 2019.

23. Chin, Kimberly, "Twitter Could Pay FTC Fine Over Alleged Privacy Violations" (Twitter Gizlilik İhlali İddiaları Nedeniyle FTC'ye Ceza Ödeyebilir), *The Wall Street Journal*, 3 Ağustos 2020.

24. Satariano, Adam, "Google Is Fined $57 Million Under Europe's Data Privacy Law" (Google, Avrupa'nın Yeni Veri Gizliliği Yasası Uyarınca 57 Milyon ABD Doları Cezaya Çarptırıldı), *The New York Times*, 21 Ocak 2019.

25. Schiffer, Zoe, "Period tracking app settles charges it lied to users about privacy" (Menstrüel döngü takip uygulaması kullanıcılara gizlilik konusunda yalan söylediği iddialarını kabul etti), *The Verge*, 13 Ocak 2021.

26. Thompson, Stuart A., "These Ads Think They Know You" (Bu Reklamlar Sizi Tanıdığını Sanıyor), *The New York Times*, 30 Nisan 2019.

27. Venkatadri, Giridhari, Piotr Sapiezynski ve ark., "Auditing Offline Data Brokers via Facebook's Advertising Platform" (Facebook'un Reklam Platformu Üzerinden Offline Veri Aracılarının Denetimi), *World Wide Web Conference*, 2019, sayfa 1920-1930.

28. Leetaru, Kalev, "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong" (Facebook'un Bile Veri Satın Aldığı Çok Güçlü Veri Aracıları - Fakat Beni Epey Yanlış Anladılar), *Forbes*, 5 Nisan 2018.

29. Grothaus, Michael, "The top 7 iOS 14 privacy features: What you need to know" (iOS 14'ün en iyi 7 gizlilik özelliği: Bilmeniz gerekenler), *Fast Company*, 16 Eylül 2020.

30. Germain, Thomas, "How a Photo's Hidden 'Exif' Data Exposes Your Personal Information" (Bir Fotoğrafın Gizli 'Exif' Verileri Kişisel Bilgilerinizi Nasıl Açığa Çıkarıyor), *Consumer Reports*, 6 Aralık 2019.

31. Helm, Burt, "Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism" (Kredi kartı şirketleri alışveriş yapan kişileri daha önce hiç olmadığı kadar takip ediyor: Gözetlemeci kapitalizmin bir sonraki aşamasında), *Fast Company*, 12 Mayıs 2020.

32. Ramirez, Edith, Julie Brill ve ark., "Data Brokers: A Call for Transparency and Accountability" (Veri Aracıları: Bir Şeffaflık ve Sorumluluk Çağrısı), *Federal Ticaret Komisyonu*, Mayıs 2014.

33. Oracle, "12 Must-Ask Questions to Separate Fact from Fiction" (Gerçek ile Kurguyu Ayırmak İçin Sorulması Gereken 12 Soru), 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" (Araştırmacılar, 'anonim' tarayıcı verilerinin kolaylıkla ortaya çıkarılabildiğini belirledi), *The Guardian*, 1 Ağustos, 2017.

35. Fowler, Geoffrey A., "You watch TV. Your TV watches back" (Siz TV'yi izliyorsunuz, TV sizi izliyor), *The Washington Post*, 18 Eylül 2019.

36. X-Mode, "Data Licensing" (Veri Lisanslama), xmode.io/data-licensing/.

37. Aygıta kayıtlı Apple ID'nin bağlı olduğu kullanıcının yaşı 18'den küçükse IDFA erişimi varsayılan olarak devre dışı bırakılır ve hiçbir geliştiriciye sunulmaz.

38. Google Ads Yardım, "About Smart Bidding" (Akıllı Teklif Verme Hakkında), support.google.com/google-ads/answer/7065882?hl=en.

39. Litfin, Marne, "What is Mobile ad attribution? An introduction to app tracking" (Mobil reklam ilişkilendirme nedir? Uygulama takibine giriş), *Adjust*, 4 Şubat 2019.

40. Cox, Joseph, "The IRS Is Being Investigated for Using Location Data Without a Warrant" (IRS İzinsiz Konum Verileri Kullandığı İçin Soruşturma Altında), *Vice*, 6 Ekim 2020.

41. Cox, Joseph, "How the U.S. Military Buys Location Data from Ordinary Apps" (ABD Ordusu Sıradan Uygulamalardan Konum Verilerini Nasıl Satın Alıyor), *Vice*, 16 Kasım 2020.

42. Cox, Joseph, "CBP Bought 'Global' Location Data from Weather and Game Apps" (CBP Hava Durumu ve Oyun Uygulamalarından 'Küresel' Konum Verileri Satın Aldı), *Vice*, 6 Kasım 2020.