

Kullanıcı Veri Gizlilięi Konusunda Google Ve Apple Karşılařtırması

Google Vs Apple On User Data Privacy

Ayça GÜRSES*, İlayda KOŞTUR**

* Bilgisayar Mühendisi, Niřantaşı Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yapay Zekâ Mühendislięi Bölümü, ayca.gurses@std.nisantasi.edu.tr

** İş Analisti, Niřantaşı Üniversitesi, Lisansüstü Eğitim Enstitüsü, Yapay Zekâ Mühendislięi Bölümü, ilayda.kostur@std.nisantasi.edu.tr

ÖZET

Teknolojinin gelişmesiyle birlikte veri oluşturma ve işleme hızı daha da artmış, bu nedenle nicelik, hız, çeşitlilik ve değer gibi unsurlara sahip büyük veri kavramı ortaya çıkmıştır. Aslında bugün dijital çaęa büyük veri çaęı da diyebiliriz. Büyük veri, pazarlamadan eğitime, bilimden siyasete hemen hemen her alanda kullanılmaktadır. İş modellerinin evrimi, teknolojinin sunduęu olanaklar ve insanların her dakika oluşturduęu devasa veri miktarı, doğru veri analizinin petrolden daha değerli olduęunu göstermiştir. Kullanıcı verilerinin çeşitli durumlarda paylaşılması büyük verinin faydalarını arttırmayı sağlar. Fakat bu verilerin mahremiyetini koruyarak paylaşmak veya olabildiğince dikkatli ve yalın şekilde yayınlamak gerekmektedir. Günümüzde teknolojik donanımların büyük verinin oluşumuna katkı sağlayan en önemli araçlardan biri olduęu söylenebilir. Teknolojik cihazlar, kullanıcıların kişisel bilgilerini paylaştıęı özel alanlar olduęu için çok fazla kişisel veri barındırmaktadır. Bazı şirketler çok fazla veri toplamaktadır ve ticari amaçlarla kullanmaktadır. Büyük veri analizi, sunduęu avantajların yanı sıra kişisel bilgilerin gizlilięini tehdit eden güvenlik açıkları da oluşturabilmektedir. Bu verilerin yeterince korunup korunmadıęı ve başka kişi veya kuruluşlarla paylaşılıp paylaşılmadıęı etik bir tartışma konusudur. Kullanıcıların kişisel verilerinin korunmasına ilişkin veri saklama ve imhası ile ilgili gizlilik bilgileri verilmesi amacıyla veri politikası yönetmelięe konulmuştur. Veri politikası, şirketin kişisel verileri nasıl yönettięini açıklayan bir politikadır. Bir veri politikasının temel işlevi, tüketicileri verilerinin nasıl işlendięi, korunduęu ve paylaşıldıęı konusunda bilgilendirmektir.

Bu çalışmada; Apple ve Google cihazlarının ve uygulamalarının gizlilik politikaları karşılaştırılmış olup, bu kapsamda bir kullanıcının bir günü incelenmiş, veri toplama işlemi örnek vaka üzerinden verilmiştir.

Anahtar Kelimeler: Veri Gizlilięi, Büyük Veri, Apple-Google, Gizlilik politikası.

1. GİRİŞ

The Economist'in bildirdięi gibi, veriler artık dünyanın en değerli kaynaęı[1]. Seagate sponsorluęunda International Data Corporation (IDC) tarafından hazırlanan ve Kasım 2018'de yayınlanan "Data Age 2025" raporuna göre, 2018'de dünya çapında 33 ZB veri vardı ve 2025'te bu verinin boyutu 175 ZB'ye çıkacak. Ancak aynı rapor, dünyadaki veri kümelerinin yaklaşık %30'unun gerçek zamanlı işleme gerektirdiğini belirtiyor [2]. Ayrıca yapay zekâ arařtırmalarının hızla ilerlemesi, özellikle derin öğrenme modellerinin gelişmesi büyük veriden ayrılamaz. Yapay zekanın yakıtı veridir ki bu da veriye sahip olmanın önemini artırmaktadır. Veriler, paydařları için değer yaratmak, onlarla "daha iyi" bir ilişki kurmak ve rekabet avantajı sağlamak isteyen kuruluşlar için önemlidir. Bu kuruluşların yařam döngüsü boyunca verileri yüksek kalitede işleyebilme becerisi ile insanları içeren kapsamlı bir veri yönetişim yapısı oluřturması gerekir. İyi veri yönetişimi, büyük veri ve gelişmiş veri analitięinin kullanılmasını saęlayan dijital dönüşüm olarak bilinen rekabetçi farklılaşma için de önemli bir temel oluřturur. Veri işleme, veriler veya veri kümeleri üzerinde gerçekleştirilen veya yapılmayan herhangi bir işlemi ifade eder. Kişisel veri tanımının yanı sıra odaklanmamız gereken bir dięer konu da kişisel verilerin işlenmesinin uygulamada ne anlama geldiğidir. Kişisel verileri gerçekten korumak için, bunların nasıl ve nerede saklandığını anlamamız gerekir.

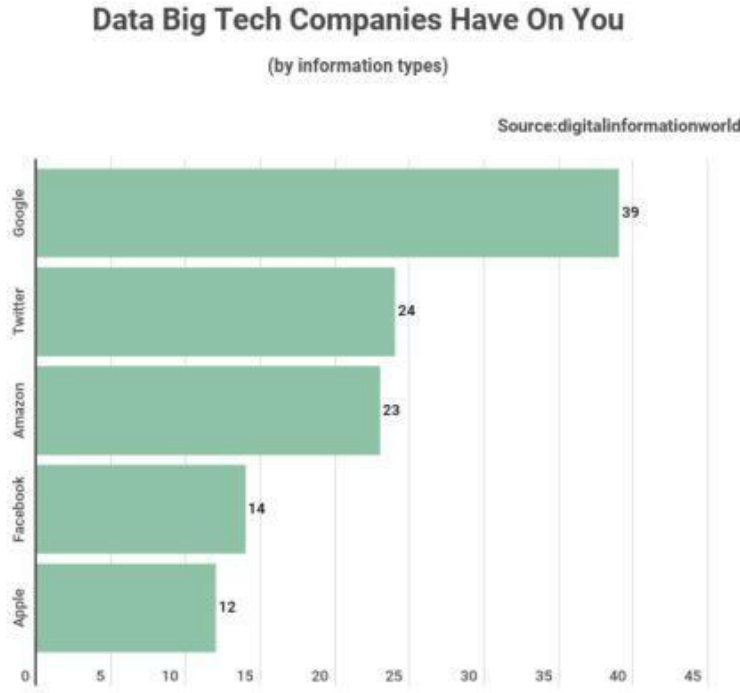
Bir kişinin kimlięinin gerçekten tespit edilebileceğini ve kişisel verileri elinde bulunduranların, bu verileri doğrudan bir kişiye bağlama yetkisine, ekipmanına ve erişimine sahip olması gerektiğini aklımızda tutmalıyız. Kişisel veri olarak tanımladığımız veri yelpazesi çok geniş olduğundan, bir kuruluşun gizlilik riskini azaltmak için yapması gereken tek şey, topladığı kişisel veri miktarını azaltmaktır. Başka bir deyişle, ihtiyaç duymadıkları verileri bireylerden istememeliler. İhtiyaç duyduğunuzdan daha fazla veri toplarlarsa, verileri anonimleřtirmeyi seçmelidirler. Anonimleřtirmenin en büyük faydası, sahip olunan verilerden yararlanmaya izin verirken gizlilik risklerini azaltmasıdır.

Dijitalleşme sayesinde iş dünyasında veriye dayalı yaklaşım sadece popülerlik kazanmakla kalmıyor, aynı zamanda kişisel verilerle ilgili endişe ve ihtiyat da artıyor. Artık tüm müşteriler, veri gizlilięi haberleri ve bunun sonuçları konusunda endişeli. Veri gizlilięine yönelik hassasiyet artarken, bu hassasiyeti karřılamak için kanun ve yönetmelikler geliştirilmektedir. Bugüne kadar, mahremiyet ve veri güvenlięi endişeleri nedeniyle hapse atılan kişiler bilgisayar korsanı ve kimlik hırsız olma eğilimindeydi. Ancak son zamanlarda şirketler, özellikle GDPR, CCPA ve KVKK gibi yasalar nedeniyle medyaya en çok yansıyan ve en çok cezalandırılan şirketler olarak dikkatleri üzerine çekti. FTC'nin Cambridge Analytica skandalı nedeniyle Facebook'a verdięi 5 milyar dolarlık rekor ceza, yeni bir döneme girdiğimizi gösteriyor. Tüm bunların KVKK uyumu çerçevesinde veri yönetişimi için gerekli olan kültürel deęişimi, yapıları, rolleri ve mekanizmaları önemli ölçüde teşvik ettiğini görüyoruz. Mahremiyet uzun zamandır bir insan hakkı olmuřtur; hatta Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nde (ICCPR) kutsal sayılmıştır [3]. İnternet, insanların büyük ölçekte bağlantı kurması için bir araç olarak ortaya çıksa bile, mahremiyet hakkı korunmalıdır. Yine de birçok teknoloji devinin kullanıcı verilerine erişimi ve kontrolü var; bu da çoęu zaman bu temel insan haklarının sınırlarını bulanıklařtırıyor. Bu yazıda, Apple ve Google'ın kullanıcı gizlilięine yaklaşımını inceliyor ve nihai olarak haklarınızı ihlal edip etmediklerini tespit edeceęiz.

2. VERİ TOPLAMA ÜZERİNE BİR ÇALIřMA

Apple, mahremiyeti "temel bir insan hakkı" olarak nitelendirmesiyle tanınır. Çoęu büyük teknoloji şirketinin aksine Apple, reklam odaklı bir şirket olmadığını, yani ürün satmak ve para kazanmak için verilerinizi toplaması gerektiğini söylüyor. Arařtırmalar, Apple'ın aslında dięer şirketlerden daha az veri

topladığını gösteriyor. StockApps analizine göre Google, beř büyük dijital řirket arasında (Google, Twitter, Apple, Amazon ve Facebook) en fazla kullanıcı verisi toplayan řirket [4]. Google, kullanıcı başına 39 veri noktası toplarken, Apple yalnızca 12 veri toplamakta.



Şekil 1

Araştırmaya göre Apple, yalnızca kullanıcı hesaplarını korumak için gereken bilgileri saklıyor ve kullanıcı gizliliğini koruma konusunda başı çekiyor (Şekil 1). Apple'ın yalnızca kullanıcı hesaplarını korumak için gereken bilgileri saklamasının nedeni; web sitelerinin Google, Twitter ve Facebook gibi reklam gelirlerine güvenmemesidir.

3. APPLE'IN GİZLİLİK KONUSUNA YAKLAŞIMI

Raporlara göre, kullanıcıların yaklaşık %25'i internet geçmişlerinin izlenmesine izin veriyor. Apple ise son yıllarda kendisini gizlilik konusunda lider olarak konumlandırmak için hamleler yaptı. Bu değişiklikler, kullanıcılara izleyicileri bildiren ve onları etkinleştirmelerini veya devre dışı bırakmalarını isteyen bir Uygulama İzleme Şeffaflığı (ATT) seçeneğinin sunulmasını içermektedir. Ancak, Apple'ın gizlilik politikasında birçok boşluk var. Fiziksel ürünleri özel ve güvenli olsa da Apple'ın iCloud hizmetinin güvenlik kaygıları vardır. Apple'ın tahminen 745 milyon kullanıcısı olan bulut depolama hizmeti, insanların kişisel bilgilerini depolamanın en popüler yollarından biri haline geldi, ancak Apple, şirketin gerektiğinde kullanıcı verilerine erişmesine olanak tanıyan şifreleme anahtarlarını saklamayı seçti. Bu yöntem, Apple aygıtları çocuk istismarı kanıtı gibi yasa dışı görüntüler için taradığında kullanılmakta.

4. GOOGLE'IN GİZLİLİK KONUSUNA YAKLAŞIMI

Google, kullanıcı gizlilięine odaklanan başka bir şirkettir. Şirket, aęını güvenli hale getirmek için adımlar attı. Örneęin Google, Google Drive sunucuları için 256 bit Gelişmiş Şifreleme Standardı kullanmakta. Ayrıca, Apple'ın Uygulama İzleme Şeffaflığına benzer şekilde Android cihazlardaki uygulamalar tarafından izlemeyi azaltacak yeni gizlilik kısıtlamaları benimsemeye hazırlanıyor. Google CEO'su Sundar Pichai (Sundar Pichai), "Google hiçbir zaman kişisel bilgileri üçüncü taraflara satmayacaktır." açıklamasında bulunmuştur [5]. Pichai ayrıca New York Times'a veri toplamının yalnızca şirketin kullanıcı deneyimini iyileştirmek için kullanıldığını ve yalnızca küçük bir kısmının kullanıldığını açıkladı. Açıklamasında; "Veriler "reklam deneyimini özelleştirmek" için kullanılır." cümlesini kullandı. Fakat Pichai'nin açıklığı kavuşturmadığı şey, Google'ın gerçek zamanlı teklif verme sisteminin "satmak" kelimesinin teknik özelliklerini kullanmasıydı. Şirket, kişisel verileri hiçbir zaman doğrudan üçüncü şahıslara satmamakla birlikte, reklamcılarla paylaşır ve onlara hedef kitlelerine reklam gösterme hakkını satar. Bu süreçte Google, coęrafî konum, cihaz kimliği, tanımlayıcı tanımlama bilgileri ve tarama geçmişı dahil olmak üzere çok sayıda üçüncü tarafla hassas bilgileri paylaşır. Gerçek zamanlı teklif verme her zaman web'in arka planında çalışırken, reklam şirketleri Google tarafından düzenlenen canlı açık artırmalarda kişisel bilgiler için rekabet eder. Sırasıyla çevrimiçi ve mobil reklamcılık şirketleri DoubleClick ve AdMob'u satın alan popüler arama motoru şirketi, gerçek zamanlı teklif verme ekosisteminin çoęunu da kontrol ediyor. Google'ın bu eylemleri tepkiyle karşılandı ve Mayıs 2020'de gizliliklerinden endişe duyan kullanıcılar, şirketin kişisel bilgilerini satmama sözünü ihlal ettiğini iddia ederek şirkete karşı federal bir toplu dava açtı [6]. Google'ın gelirinin %90'dan fazlası reklam verenlerden gelir. Reklam şirketleri Google'ın müşterisidir ve reklam veren firmalar tatmin olmazsa Google iflas eder. Bu onlar için bir hayatta kalma meselesi, bu sebepten dolayı Google, reklam şirketlerini memnun etmelidir. Peki reklam ajansları ne istiyor? Elbette verilerimizi. Google, Facebook'un gelirinin %95'inden fazlasını reklamlardan alıyor [7]; Apple neredeyse hiçbirini almıyor ve Apple reklamlardan neredeyse hiçbir şey elde etmedięi için, kullanıcılarının verilerinin gizliliğini savunuyor.

5. APPLE'IN VE GOOGLE'IN VERİ KORUMA PROGRAMLARI

Bir veri koruma planı, dijital gizlilięi korumak için gereken basit adımların bir adım ötesine geçer. Bu hizmet yetkisiz kullanıcıların hesabınıza erişme olasılığını en aza indirmek için uçtan uca şifreleme ve fiziksel güvenlik anahtarları kullanır. Veri Koruma Planı Programlarına herkes kaydolabilirken, günlük kullanıcılar ekstra adımları gereksiz bulabilir. Hizmetler gazeteciler, aktivistler, iş dünyası yöneticileri, seçim görevlileri ve diplomatlara yöneliktir ve cihazlarında çok hassas veriler taşıyan kişiler içindir. Kedilerinizin fotoęrafları için yalnızca iCloud veya Google Drive depolama kullanıyorsanız, muhtemelen bu hizmetlere ihtiyacınız yoktur. Her ikisi de teknik olarak ücretsiz olsa da fiziksel bir anahtar satın alma gereklilięi bazı insanları rahatsız edebilir. Ancak parolaların giderek geçerliliğini yitirdięi bir çağda, bu programlar, hedefli çevrimiçi saldırılara karşı daha az savunmasız olanlar için bile giderek daha değerli hale geldi. Kimlik Hırsızlığı Kaynak Merkezi'nin 2021 Veri İhlali Raporu'na göre, veri ihlallerinin sayısı tüm zamanların en yüksek seviyesinde [8]. Fiziksel güvenlik anahtarı, hesap erişimini doğrulamanın en kolay ve en etkili yoludur.

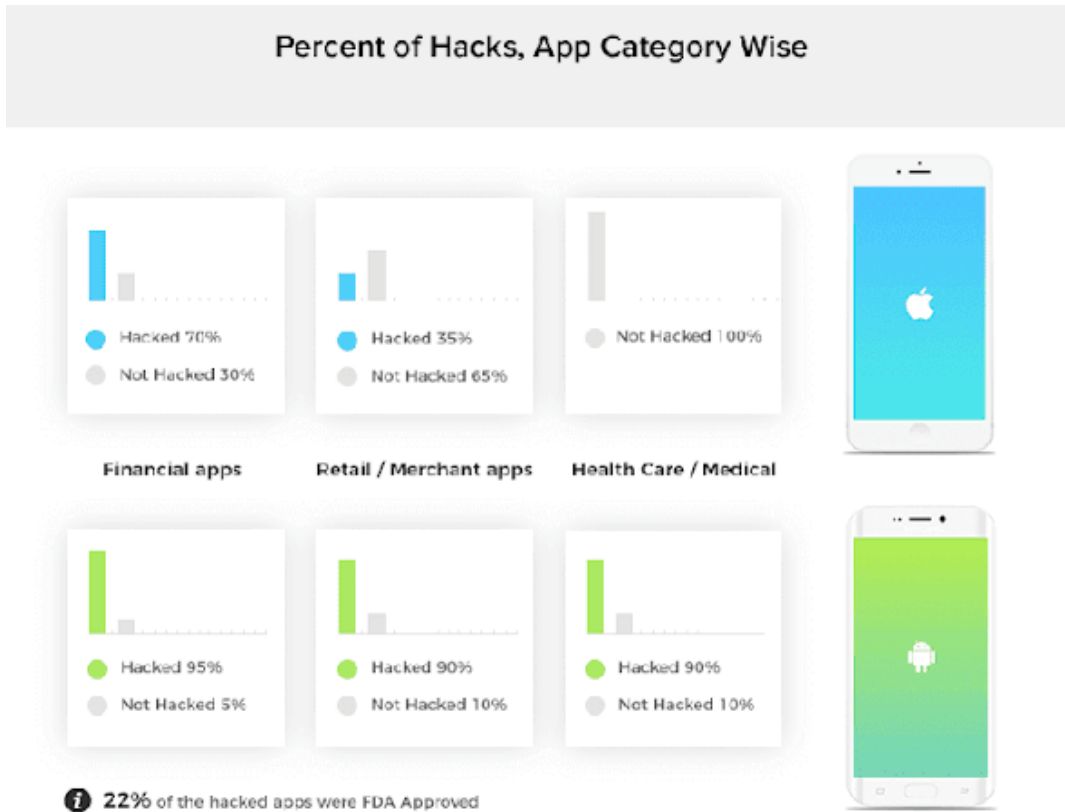
5.1. GOOGLE GELİŞMİŞ VERİ KORUMA PROGRAMI

Gelişmiş Koruma Programı üç ana alanı kapsar: fiziksel güvenlik anahtarları, indirme denetimleri ve kimliği doğrulanmamış hesap erişimini önleme [9]. Chrome, bir sayfanın tehlikeli olabileceęi konusunda sizi uyardığında, sayfanın iş başında olduğunu görmenizi sağlar. Advanced Protector, indirmeler üzerinde ek kontroller gerçekleştirerek bunu bir sonraki seviyeye taşıyor. Zararlı olabilecek dosyalar işaretlenir ve Android telefonunuz bunları yalnızca Play Store gibi doğrulanmış uygulama mağazalarından indirebilir. Bunlar, bu kontrollerin hiçbirini gerçekleştirmeyen Apple programından temel farklardır. Gelişmiş Koruma, yalnızca Google'ın ve doğrulanmış üçüncü taraf uygulamalarının Google Hesabı verilerinize ve yalnızca sizin izninizle erişmesine izin verir. Bu, Google Hesabı verilerinize erişim isteyen

yeni uygulamaları kaydetmenizi engelleyebilir. Bu nedenle, kötü niyetli aktörler, hesap verilerinize erişmek için üçüncü bir tarafın kimliğine bürünemez. Google'ın Gelişmiş Koruma Programı, kötü niyetli kişilerin Google Hesabınız, indirmeleriniz veya göz atma etkinliğiniz yoluyla verilerinize erişememesini sağlar.

5.2. APPLE GELİŞMİŞ VERİ KORUMA PROGRAMI

Apple Kimliğiniz için bir güvenlik anahtarı gerektirmesine ek olarak, Apple çevrimiçi verilerinizi korumak için iki özellik daha sunar, ancak bu iki hizmet henüz dünya genelinde mevcut değildir [10]. Güvenlik anahtarları ve iMessage doğrulaması, 2023'ün başlarında tüm dünyada kullanıma sunulacaktır. iCloud Gelişmiş Veri Koruma ise 2023'ün başlarında tüm dünyada kullanıma sunulacak (Beta yazılım programı üyeleri artık buna erişebilir.). iMessage zaten uçtan uca şifreleme içerir, ancak bu yeni özellik, konuşmalara fazladan bir güvenlik katmanı ekler. Hizmetin kullanıcıları, yalnızca istedikleri kişilere mesaj gönderdiklerini doğrulamayı seçebilirler. Her ikisi de hizmete sahip olan sohbet üyeleri, birinin kuralları çiğneyip konuşmalarına kulak misafiri olması durumunda otomatik uyarılar alabilecek. Bu, bilgilerinizi korumanın harika bir yolu olsa da her iki alıcı da programa kaydolduklarında iMessage'ı kullanmalıdır. Android kullanıcıları ile güvenli bir şekilde iletişim kurabilmek için WhatsApp gibi başka bir şifreli mesajlaşma uygulaması kullanmak gerekiyor.



6. ÖRNEK VAKA ÜZERİNDE VERİLERİN BİR GÜNÜNÜN İNCELENMESİ

John kızıyla parkta bir gün planlıyor John ve 7 yařındaki kızı Emma, günü birlikte geçiriyorlar. [11] Sabahları, John hava durumuna bakmak, haberleri okumak ve bir harita uygulamasını kontrol etmek için bilgisayarını kullanır. Yolculuk sırasında, telefonunda arka planda periyodik olarak konum verilerini toplayan ve izleyen 4 uygulama vardır. Veriler cihazdan çıkarıldıktan sonra, uygulama geliřtiricileri bunları bir dizi belirsiz üçüncü taraflara satarlar. John'un adını hiç duymadıęı komisyoncular. Toplanan konum verilerinin anonim olduęu iddia edilse de, kullanıcı izleme, veri komisyoncularının John'un bu uygulamalardaki konum gemiřini dięer uygulamaları kullanımından toplanan bilgilerle eřleřtirmesine olanak tanır. Bu, farklı uygulamalarda ve birden fazla kaynaktan izlenen bilgilerin herhangi bir řirket veya kuruluř tarafından satın alınabileceęi ve onun hakkında günlük kesin hareketlerini içeren kapsamlı bir profil oluřturmak için kullanılabileceęi anlamına gelir. Oyun alanına giderken John, kızının tabletinde oyun oynamasına izin veriyor. Uygulamayı açtıęında bir scooter reklamı görüyor ve bu bir tesadüf deęil. Uygulamanın yüklendięi bir saniye içinde, reklam alanı için bir açık artırma gerekleřti. Aracılar aracılıęıyla, scooter řirketi adına alıřan reklam řirketleri mevcut reklamı öğrendi. Scooter řirketinin reklam ortakları, reklamı gördükten sonra John ve Emma'nın davranıřları hakkında bilgi toplamaya devam ederek, reklamı tıklayıp tıklamadıklarını belirler veya scooter'ı satın aldıklarını. Ayrıca, John ve Emma'yı tüm cihazlarındaki farklı uygulamalar ve web sitelerinde takip ederek, mümkün olan her řekilde John ve Emma'ya scooter'ın reklamını yapmaya devam edecekler. Daha sonra, oyun alanında John ve Emma bir selfie ekerler. Fotoęrafa tavřan kulakları eklemeye karar vererek bir fotoęraf filtresi uygulamasıyla oynuyorlar. Ancak filtreleme uygulaması, yalnızca oyun alanı selfie'si yerine cihazdaki tüm fotoęraflara ve ekli meta verilere erişebilir. John resmi bir sosyal medyada yayınlıyor Uygulama, John'un mevcut evrimii etkinlięini, e-posta adresi, telefon numarası veya bir reklam tanımlayıcısı kullanarak demografik bilgileri ve satın alma alışkanlıkları gibi dięer uygulamalar tarafından toplanan bir veri hazinesini de öğrenmiř olur. Eve dönüş yolunda, John ve Emma dondurma için dururlar. John öder ve tercihlerinin kapsamlı veri profiline daha fazla bilgi eklenir: maęazanın konumu ve ne kadar harcadıęı. Bu bilgileri John'un konumunu izleyen uygulamalardan biri gözlemleyebiliyor. Kısaca Ailenin gün boyunca nereden alışveriř yaptıęıyla ilgili bilgiler, John'un cihazlarına řekerli ürünlere yönelik hedefli reklamlar sunması için küçük bir ocuęu olduęu bilgisiyle birleřtiren veri simsarlarına iletilir. řirketler ailenin evinin yerini, ziyaret ettikleri parkı, okudukları haber sitelerini, gezindikleri ürünleri, izledikleri reklamları, satın alma alışkanlıklarını ve ziyaret ettikleri maęazaları biliyorlar. John ve kızının gün boyunca kullandıęı birden fazla uygulamanın yanı sıra dięer kaynaklardan. John'un gün boyunca ne kadar veri toplandıęı hakkında hiçbir fikri yoktu, her zaman üzerinde kontrol sahibi deęildi ve bilerek bunun gerekleřmesine izin vermedi. Akřam akıllı TV'lerinde bir ocuk filmi ararken, izleme, veri alışveriři, açık artırma ve yeniden -hedefleme aralıksız devam ediyor.

6.1. JOHN VE EMMA APPLE ÜRÜN VE CİHAZLARINI KULLANSAYDI YAřANACAKLAR

John, bilgisayarında hava durumunu kontrol etmek için Safari tarayıcısını kullanmıř olsaydı, Akıllı İzleme Önleme varsayılan olarak bu etkinlięin izlenmesini engellerdi. John sabah haberleri okumak için Apple News'i kullansaydı, Apple onun kim olduęunu bilmeden veya ne okuduęunu öğrenmeden John'a ilgi alanlarına göre içerik sunardı. John, trafięi kontrol etmek için Apple Haritalar'ı kullanmıř olsaydı, konum verileri, düzenli olarak sıfırlanan ve John'a baęlı olmayan rastgele bir tanımlayıcıya baęlanırdı. Sonuç olarak, John'dan bařka hiç kimse onun yerini bilmeyecekti. Bir iPhone'da, John'a arka planda

hangi uygulamaların konumuna eriştięi düzenli aralıklarla hatırlatılır. John, bir uygulamayla konum paylaşmadan önce yalnızca yaklaşık konumunu veya konumunu yalnızca bir kez paylaşmayı seçebilirdi. Bir iPad'de, yakında çıkacak olan Uygulama İzleme Şeffaflığı özellięi, John'a oyunun Emma'nın dięer şirketlerin sahip olduęu uygulamalar ve web siteleri üzerindeki etkinlięini izlemesine izin verip vermeme konusunda bir seçenek sunacaktı. Apple'ın SKAdNetwork (ESKEYAD NETWORK) API'sini kullanan reklam aęları, John'un cihazına kadar izlenebilecek bilgilere erişmeden reklamlarının genel etkinlięini ölçebilir [12]. Bir iPhone'da John, filtre uygulamasının tüm fotoğraf kitaplıęı yerine yalnızca özçekime erişmesine izin verme seçeneęine sahip olacaktı. John, dondurmayı Apple Card kullanarak satın almış olsaydı, bankası onun işlem bilgilerini pazarlama amacıyla kullanmazdı. Apple Pay'i kullanmış olsaydı, John, Apple'ın nereden alışveriş yaptıęı ne satın aldıęı veya ne kadar harcadıęı hakkında bilgi edinmeden işlem geęmiřini iPhone'unda görüntüleyebilmesi için cihazdaki zekayı kullanırdı.

7. ANDROİD VE İOS'TA GÜVENLİK FARK NOKTALARI

Güvenlik Yazılımı Güncellemesi: Android, Android Güvenlik Bülteni'nde aylık güncellemeler sunar [13]. Android ayda bir güncelleme verse de kullanıcıları cihazları güncellemeye zorlamıyor. Güncellemeyi yok sayma ve cihazı aynı şekilde çalıştırma seçeneęi, kullanıcılara bir kaçış planı vererek Android uygulama geliştirme hizmetlerini güvenlik ihlali olasılıęına sürüklüyor. Apple, ayda bir, güvenlik güncellemelerinin birkaç sürümünü kullanıma sunmakta ve her kullanıcının en son güvenlik yükseltmelerini indirmesini zorunlu kılıyor. İşletim sistemi, sürekli bildirimler vererek, kullanıcılarının güvenlik yükseltmelerini göz ardı etmesini zorlaştırmakta.

Dokunma Kimlięi: Android kısa süre önce Parmak İzi Tarama seçeneęi sunan üreticilerle ortaklık kurmaya başlasa da sayı hala çok sınırlı [14]. Apple'da durum böyle deęil. Apple, cihazlarında biyometrik doğrulama söz konusu olduęunda her zaman çok titiz olmuştur. Sadece Touch ID için deęil, Iris Scan ve Face ID gibi teknolojiler de ilk olarak Apple tarafından icat edildi [15].

Donanım Entegrasyonu: Apple'ın aksine, donanımla ilgili Android uygulama güvenlięi tamamen üreticilere baęlıdır. Genel olarak, maliyet açısından ana kategorilere ait olan cihazlar, düşük fiyatlı ürünlere göre daha fazla güvenlik desteęi ile gelir. Öte yandan Apple, donanım güvenlięi üzerinde tam kontrole sahiptir.

Cihaz Parçalanması: Parçalanma ne kadar büyük olursa, artan bilgisayar korsanlıęı ve veri ihlali olayları için rahat bir alan olan boşlukların ortaya çıkma şansı o kadar artar. Apple, hem cihaz hem de işletim sistemi sürümünü daha düşük bir seviyede tutarak, bir IOS uygulama geliştirme şirketinin bilgisayar korsanlıęı sorunuyla karşılaşma olasılıęını çok yönlü olarak azaltmakta. Ancak Android'de durum aynı deęil. Hem cihaz deęişkenlerinin hem de işletim sistemi sürümlerinin sayısı platformda çok yüksek, bu da saldırılara ve ihlallere yol açacak açık bir ekosistem saęlıyor.

Uygulama Mağazaları: Apple kriterlerini karşılamayan her uygulamayı inceleme, reddetme ve kaldırma hakkını çok ciddiye alıyor; bu, reddedilmeyen uygulamalar geliştirebilen bu tür iPhone uygulama geliştirme

řirketlerine talep getirdi. Google, bir Android uygulamasını onaylarken katı kurallara uymanın gereklilięini uzun süre göz ardı etti. Ancak artık önemli adımlar atmakta. Google, geliřtiricileri Android uygulama geliřtirmede güvenlięe odaklanmaya teřvik etmenin yanı sıra, 2017'de Play Store'daki kötü amaçlı uygulamaları tespit etmek ve kaldırmak için makine öğrenimini kullandı [16].

8. ANDROID VE İOS: 2021-22'DE İŞLETİM SİSTEMİ GÜVENLİĞİ KARŞILAŞTIRMASI

8.1.iOS 14 Gizlilik Özellikleri [17]

IDFA'daki Deęişiklikler: iOS uygulama geliřtiricileri, uygulamaların bilgilerini promosyon ve pazarlama amaçlarıyla kullanmasına izin verdiklerini belirtene kadar artık kullanıcıların verilerine erişemeyecek [18].

Konum paylaşımındaki deęişiklikler: Kullanıcılar artık kesin konum paylaşımını devre dışı bırakma olanağına sahip olacak. Bu şekilde, uygulamalar ve pazarlamacılar, kullanıcıların yalnızca yaklaşık bir konumunu elde edebilmekte.

Gizlilik raporu: Apple artık kullanıcılara hangi uygulamaların verilerine ne kadar süreyle eriştiğine ilişkin ayrıntıları içeren bir gizlilik raporu gönderecek.

8.2. Android 11 Gizlilik Özellikleri [19]

İzinlerdeki Deęişiklikler: Herhangi bir yeni uygulamayı ilk açtığınızda size izin açısından üç seçenek sunulur; her zaman, yalnızca uygulamayı kullanırken, asla.

İzin iptali: Android, bir süredir kullanmadığınız uygulamaları takip edecek ve ona vermiş olduğunuz izinleri iptal edecektir. Bu sayede bir aradan sonra uygulamayı açtığınızda tekrar izin vermeniz gerekecek.

SONUÇ

Artık yeni güncellemelerde Android ve iOS gizliliğinin yeni eklemelerini incelediğimize göre, bir sonraki adım bunları dięer ortak faktörlere göre ölçmek ve bir sonuca varmak olacak. Her iki işletim sistemini de dört önemli faktör temelinde karşılařtırabiliriz.

Pazar Yeri Güvenlięi: Play Store'un App Store'dan çok daha geniş olması hem bir nimet hem de bir sorun olarak karşımıza çıkıyor. Genişlik, bir yandan Android kullanıcılarına aralarından seçim yapmaları için geniş bir seçenek sunarken, aynı zamanda bilgisayar korsanlarına kötü amaçlı yazılım uygulamalarını milyonlarca kalabalığın arasında bırakmak için bir fırsat sunmakta. Apple ise App Store'u yakından takip ediyor. Her uygulamanın geçmesi gereken denetim düzeyi, kullanıcılar için mevcut seçeneęi azaltmakta, kötü amaçlı yazılım saldırılarının olasılığını en aza indirmekte.

Platformun Popülerlięi: Android, řüphesiz dünya akıllı telefon pazarında büyük bir paya sahip ve bu, Apple'ın kapsayamayacaęı bir sayı. Platform popüleritesi arttıkça, baęlanan kullanıcı sayısı da ve dolayısıyla güvenlik ihlali olasılıęı da artmakta. Ancak, sadece yüksek popüleritesine dayanarak Android uygulama güvenlięine daha az puan vermek doęru deęildir. Artan kullanıcı sayısı nedeniyle, Android uygulama

geliřtirici topluluęu, en iyi mobil uygulama güvenlik uygulamalarını sunmaya ve hack'e dayanıklı bir uygulama sunmaya daha fazla odaklanmaya bařladı.

Cihaz Üreticilerinin Sayısı: Android'in 'Android'e karřı iOS güvenlięi' konusunda Apple'ın %100 gerisinde kalmasının bir nedeni varsa, yüksek cihaz üreticisi sayısından kaynaklanan saldırılardır. Farklı cihazlar, Güvenlik koruması özelliklerine farklı odaklanarak geldięinden, řemsiyesi altında binlerce cihaz bulunan Google'ın, iř ortaęı OEM'lerinin her biri için ortak bir protokol seti oluřturması imkansızdır [20]. Üretilen cihaz üzerindeki yoğun denetimi nedeniyle Apple'ın asla karřılařmak zorunda kalmayacaęı bir sorun.

Kaynak Kodu Güvenlięi: Her iki iřletim sistemi de kullanıcılarını güvende tutmak için çok benzer güvenlik özelliklerinden yararlanır, ancak Apple kaynak kodunu yakından takip ederken ve iOS'ta SSL Sabitleme gibi iřlemlere sahipken [21], Android'in açık kaynaklı doęası, iřletim sisteminin alışmasını zorlařtırır. Bu açığı özmek için Google, yalnızca saldırının kaynaęını belirlemek için bilgisayar korsanlarını istihdam etmekle kalmadı, aynı zamanda markanın her yıl yeni güvenlik açıkları bildirenler için ödemeye hazır olduęu ödölünü de artırıyor.

Android'in 2021'de Güvenlik Cephesinde yeni özellikler sunacak olmasına raęmen iOS bu yıl da Android-iOS Uygulama Güvenlięi Karřılařtırması unvanını kazanmıřtır.

KAYNAKÇA

- [1] <https://www.dijitalhabitat.com/dunyanin-en-degerli-kaynagi-artik-petrol-degil-veri/>
- [2] <https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf>
- [3] <https://www.ihd.org.tr/sasve-medenhaklar-uluslararası-slees/>
- [4] <https://stockapps.com/blog/google-tracks-39-types-of-private-data-the-highest-among-big-tech-companies/>
- [5] <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html>
- [6] <https://www.courthousenews.com/tracking-for-ads/>
- [7] <https://www.vox.com/2017/7/24/16020330/google-digital-mobile-ad-revenue-world-leader-facebook-growth>
- [8] https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
- [9] <https://landing.google.com/intl/tr/advancedprotection/>
- [10] <https://support.apple.com/tr-tr/guide/security/secf6276da8a/web>
- [11] https://www.apple.com/tr/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf
- [12] <https://www.appsflyer.com/glossary/skadnetwork/>
- [13] https://www.android.com/intl/tr_tr/enterprise/security/
- [14] <https://support.google.com/nexus/answer/6285273?hl=tr>
- [15] <https://support.apple.com/tr-tr/HT208108>
- [16] <https://support.google.com/accounts/answer/9924802?hl=tr&co=GENIE.Platform%3DAndroid>
- [17] <https://www.apple.com/tr/privacy/features/>
- [18] <https://www.adjust.com/glossary/idfa/>
- [19] https://www.android.com/intl/tr_tr/android-11/
- [20] <https://support.google.com/google-ads/answer/9702452?hl=tr>
- [21] <https://medium.com/trendyol-tech/securing-ios-applications-with-ssl-pinning-38d551945306>