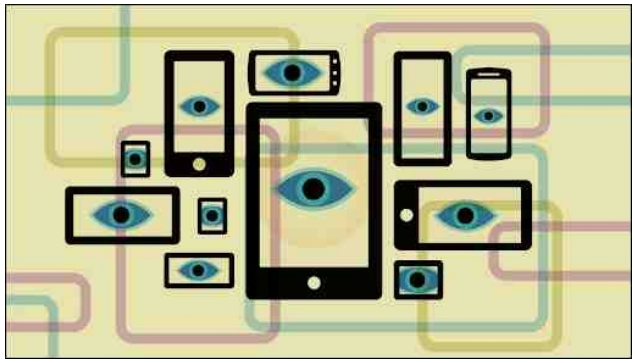
Hirdetési nyomkövetés kikapcsolása iOS és Android alatt hogyan és miért kell most megtenni

PCLinuxOS Magazine – 2022. június

Írta:Bennett Cyphers
Electronics Frontier Foundation



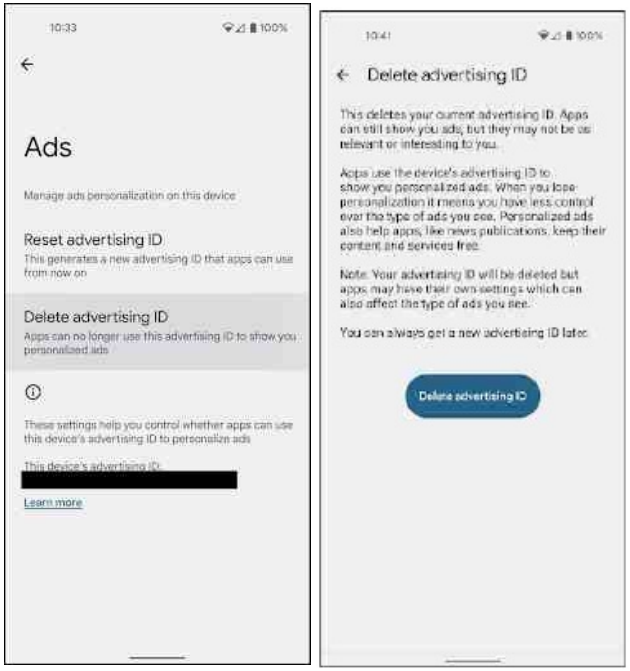
A hirdetési azonosító (ad ID) – IDFA az iOS-on és AAID Androidnál – a kulcs, ami lehetővé teszi harmadik fél számára a nyomkövetést mobilon. Kikapcsolásával jelentősen megnehezedik a hirdetők és adatkereskedők számára a követés és profilalkotás, illetve korlátozza az eladható személyes adatokat.

A bejegyzés leírja a hirdetési eszközazonosítók történetét és a folyamatos követés, azonosítás és más személyes adatok megsértésének lehetővé tételét.

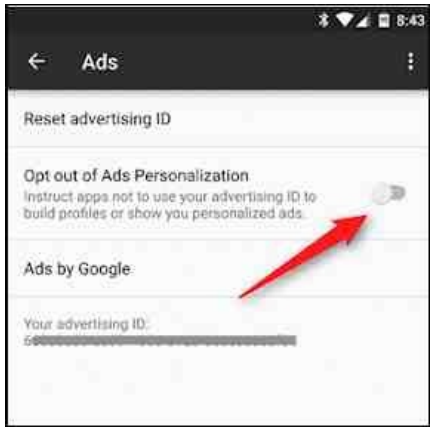
Kezdjük az elején. Íme, ahogy a követők azonnal kizárhatók az „ad ID”-hez hozzáféréséből:

Androidon

Nyisd meg a **Beállítások** applikációt és **Adatvédelem → Hirdetések. Hirdetésazonosító törlése** opcióra kattints és hagyd jóvá. Ez lehetetlenné teszi bármely alkalmazás számára, hogy hozzáférjen a későbbiekben.



A kikapcsolás (opt out) Android 12 alatt lehetséges, de a korábbi verzióknál esetleg nem elérhető. Helyette törölheted az ad ID-t és kérheted az alkalmazásokat, hogy ne kövessenek.



Forrás

iOS alatt

Az Apple-nél az alkalmazásoknak engedélyt kell kérniük, mielőtt hozzáférnének az IDFA-hoz. Amikor új alkalmazást telepítesz, kérhet engedélyt a követésre.

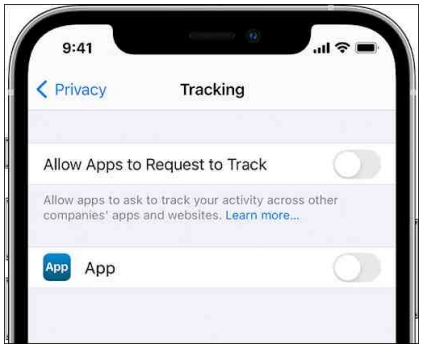
Forrás

Válaszd az „**Ask App Not to Track**”-et az IDFA tiltásához.

Hogy lásd, mely alkalmazások kaptak engedélyt a hozzáférésre, lépj a **Beállítások → Biztonság → Követés**-re. Valami ilyen menüt kell kapnod.

Itt lehet visszavonni a követési engedélyt azoktól az alkalmazásoktól, amik korábban kaptak. Csak az engedéllyel rendelkező alkalmazások érhetik el az IDFA-dat.

Hirdetési nyomkövetés kikapcsolása iOS és Android alatt hogyan és miért kell most megtenni



Az „**Allow apps to Request to Track**” kapcsolót teheted „**off**” (ki) állásba (a csúszka balra van és szürke hátterű). Ennek hatására az alkalmazások többé nem kérnek engedélyt a követésre. Ha korábban pár alkalmazásnak engedélyezted a követést, akkor engedélyt kér azok követésének letiltására is. Lehetőség van a követési engedély alkalmazásonkénti kiadására, vagy letiltására.

Az Apple-nek van saját célzott hirdetési rendszere, az IDFA-val harmadik félnek engedélyezett követésen kívül. Ennek kikapcsoláshoz **Beállítások → Adatvédelem → Apple Advertising**-hoz kell belépni:

Forrás.

Állítsd a „**Személyre szabott hirdetések**” kapcsolót „**ki**” (off) állásba annak kikapcsolásához.

Előzmények

Az okos telefonok őskorában a követők fix eszközazonosítót használtak – iOS-nél „Unique Device Identifier" (UDID) és „Android ID-t Androidon” – az alkalmazások segítségével követéshez. Ezek egyedi, állandó azonosítók voltak és harmadik felek gyakran használták a felhasználó tudta, vagy beleegyezése nélkül.

Adatvédelmi szempontból joggal tartották problémának. A Wall Street Journal egy 2010-es vizsgálata feltárta ezt a problémát és 2011-ben, több amerikai kongresszusi képviselőtől kapott egy sor megkeresés hatására az Apple elkezdte az UDID-hez hozzáférést letiltani.

Az ipar már kezdett berendezkedni az UDID-re alapuló adatgyűjtésre és a követőket a változás összezavarta. Ezután, 2012-ben az Apple csendben bevezette az Identifier for Advertisers-t (IDFA). Az IDFA majdnem teljesen azonos volt az általa lecserélt UDID-val: teljeskörűen egyedi azonosító, amit az alkalmazások alapból elértek. A legnagyobb különbség, hogy az IDFA törölhető volt – már ha a felhasználó tudta, hol keresse. Az Apple elérhetővé tett a felhasználónak egy „Limit Ad Tracking” (követés korlátozása) beállítást. Ez az alkalmazásokatkérte, hogy nem kövessék, de nem korlátozta hozzáférésüket az IDFA-hoz.

Az Android 2013-ban, per nyomán, bevezette az Android Advertising Identifier-t (AAID). Akár az Apple, a Google is alapból elérhetővé tette az alkalmazások számára, külön engedély nélkül. Az azonosító megújítását lehetővé tette, de a törlés, vagy a hozzáférés letiltásának lehetősége nélkül.

2016-ban az Apple frissítette a korlátozott követést azzal, hogy az IDFA-kulcs nullákra lett cserélhető – gyakorlatilag törölve azt. Ezzel először vált lehetővé technikailag az IDFA-követés kikapcsolása.

2021-ben az Apple bevezette az App Tracking Transparency-t (ATT), ami megkövetelte az alkalmazásoktól a felhasználó kifejezett beleegyezését kérjék, hogy követhessék az IDFA, vagy más azonosító segítségével. A követési rendszerekre hatalmas hatással volt. A bevezetése előtt csak a felhasználók 20%-a tiltotta (5-ből 4 engedélyezte), a váltást követően a döntő többség a követés letiltását választotta. Alap az engedély hiánya.

Eközben, az Android is végre elkezdte az azonosító felhasználó általi kikapcsolása módjának kidolgozását. A 2022. április 1-jei állás szerint a fejlesztőknek külön engedély kell az ID eléréséhez. Ugyanakkor ez egy „normál” engedély, nincs felugró ablak, a felhasználó engedélyét kérve az azonosító elérésére. A hirdetési azonosító követésben betöltött alapvető szerepe ellenére a fejlesztői dokumentumok szerint ez az engedély olyan információra vonatkozik, ami „a felhasználó adatai védelme szempontjából nagyon alacsony kockázatot jelent”. Más szóval, az Android azonosítója letiltásos rendszerű, a felhasználóknak kell megtalálni az adataik védelmének módját a platformon.

Februárban a Google bejelentette, hogy végső soron teljesen kivezetheti az azonosítót. A Privacy Sandbox (izolált környezet) keretrendszer egy változatának mobilokra bevezetésével viselkedés alapú hirdetéseket támogatja „az applikációs azonosítókra támaszkodás helyett”. A Google biztosította a fejlesztőket arról, hogy „még legalább két évig” nem lesz lényeges változás az ID-nél.

Ez miért fontos

Azad ID egy betűkből és számokból álló, a telefonodat, tabletedet vagy más okos eszközödet beazonosító egyedi karaktersor. Egyetlen célja, hogy segítse a cégeket a követésedben.

A harmadik fél követői adatokat gyűjtenek a készüléked alkalmazásain keresztül. Az ID lehetővé teszi az adatok

személyedhez kapcsolását. Emellett, mivel az összes alkalmazás egyazon ID-t lát, az adatkereskedők feljegyzéseket készíthetnek rólad. A kereskedő vehet B-től adatokat, az azonosító alapján a két adatsort összekapcsolhatja. Egyszerűen, az ID lehetővé tesz egy sor adatbiztonság-sértést: agresszív profilozást Facebook és Google által; tudományközeli pszichografikus célbavételt a Cambridge Analytica-hoz hasonló, politikai kutatók által, illetve a helymeghatározást az USA hadsereg számára.

Az adatcsatorna részvevői néha azzal érvelnek, hogy az ID névtelen, vagy közel anonim, „nem személyi azonosító" adat és alkalmazása nem jelent komoly veszélyt a személyiségi adatok szempontjából. Ez nem igaz. Először is az ID elterjedten alkalmazott olyan, személy azonosítására alkalmas adatok gyűjtése elősegítésére, mint a helyadatok. Ha látod, hogy az illető hol dolgozik, alszik, tanul, szórakozik, imádkozik és gyógyíttatja magát, nem kell az e-mail-címe az azonosításához. Emellett, teljes iparág rendezkedett be arra, hogy az ID-ket olyan sokkal konkrétabb azonosító információkkal kapcsolja össze mint, az e-mail-cím és telefonszám. Önmagában az ID lehet anonim, de a követői iparági környezetben ez egy állandóan jelen lévő és hatékony azonosító.

Az ID kikapcsolása határozottan megnehezíti a legtöbb hirdetőnek és adatkereskedőnek a követést. Ezek az iparágak milliónyi és milliárdnyi felhasználó adatait dolgozzák fel naponta és az ID-hez hasonlók teszik kényelmessé számukra az ilyen nagyságrend kezelését. Kiragadva ezt az eszköztárukból, lényegesen kevesebb adathoz jutnak hozzá, amit a személyedhez kapcsolhatnak. Ez nem csak az adatbiztonságod szempontjából hasznos, hanem a hirdetéskutató iparág jövedelmezőségét is csökkenti. És nem csak mi mondjuk ezt: a Facebook állította, hogy az Apple App Tracking Transparency bevezetése nyomán a cég bevételei kb. 10 Milliárd USD-vel csökkenhettnek.

Noha az ID eltávolítása jó kezdet, nem szünteti meg a követést. Ha egy adott, téged, vagy környezetedben bárkit fenyegető adatbiztonsági kérdés érdekel, nézd meg a többi forrásunkat, benne a „Digitális biztonsági és személyiségi jogi tippek azoknak, akiket abortusz-kérdés érint".

Érdemes lehet megnézni az EFF felderítés elleni önvédelmi útmutatóját, benne az egyéni biztonsági tervvel, tüntetésen részvétel esetén és az adatbiztonsággal mobiltelefonokon. Ezeket az anyagokat olyan tematikus gyűjteményekbe rendeztük, mint a „for reproductive healthcare providers, seekers, and advocates".

Posted by tbschommer, April 30, 2022, running KDE.