Dr. Johnny Ryan jelentése - Viselkedésalapú reklámozás és személyes adatok

A jelentés kivonatának fordítása, a teljes szöveg itt található:
https://brave.com/Behavioural-advertising-and-personal-data.pdf

Hogyan használják fel a személyes adatokat a viselkedésalapú online reklámozásban.

Valahányszor "viselkedési alapon" célzott reklámot juttatnak el valakihez, aki egy weboldalra látogat, a rendszer, amelyik kiválasztja, melyik hirdetést mutassa neki, több száz vagy több ezer cégnek szórja szét az illető személyes adatait. Az ilyen rendszert "valós idejű licitálásnak", olykor "programozáson alapuló" (egyszerűbben: automatizált) hirdetésnek nevezik. A továbbadott személyes adatok között szerepel a felhasználó által megtekintett valamennyi weboldal URL-je, az illető IP-címe (amelyikből kikövetkeztethető a tartózkodási helye), az általa használt eszköz tulajdonságai és számos egyedi azonosító, amelyeket esetleg régebb óta tárolnak róla a célból, hogy hosszabb távon megalkotható legyen a profilja.

Hiába volt egy türelmi időszak a GDPR bevezetése előtt, a technikai háttértámogatást nyújtó AdTech ipar nem hozott létre megfelelő ellenőrzési módszert annak érdekében, hogy a rengeteg cég, amelyik megkapja az adatokat, képes legyen végrehajtani az adatvédelmi rendeletet.

Hogyan "szórják szét" a személyes adatokat.

Az online média és reklámipar jelentős része alkalmazza az ún. "RTB", avagy "real time bidding" (valós idejű licitálási) rendszert. Ennek két típusa van.

- "OpenRTB" - az online médiában és reklámiparban gyakorlatilag az összes jelentős cég él vele.
- "Authorized Buyers" (Jogosult Vevők) - a Google saját RTB rendszere, nemrég nevezték át "DoubleClick Ad Exhange"-ről (azaz "AdX"-ről) "Authorized Buyers"-re.

A Google mind az OpenRTB-t, mind pedig a saját "Jogosult Vevők" rendszerét alkalmazza.

Mindkét rendszerhez tartozik nyilvánosan elérhető termékleírás. Ezekből kiderül, hogy valahányszor valaki feltölt egy oldalt egy valós idejű licitálással reklámozó weboldalra, több tíz vagy több ezer cég kapja meg a személyes adatait. Íme egy példa arra, milyen személyes adatokat szórnak szét:

● Mit olvasol vagy nézel?

● Hol tartózkodsz (az OpenRTB-nél a teljes IP cím szerepel)

● Az általad használt eszköz tulajdonságai

● Egyedi nyomkövető azonosító vagy "süti azonosító", amelynek segítségével a hirdetéstechnológiai cégek legközelebb megpróbálhatnak beazonosítani, hogy hosszabb távon létrehozzák vagy interneten kívüli adatokkal megerősítsék a profilodat

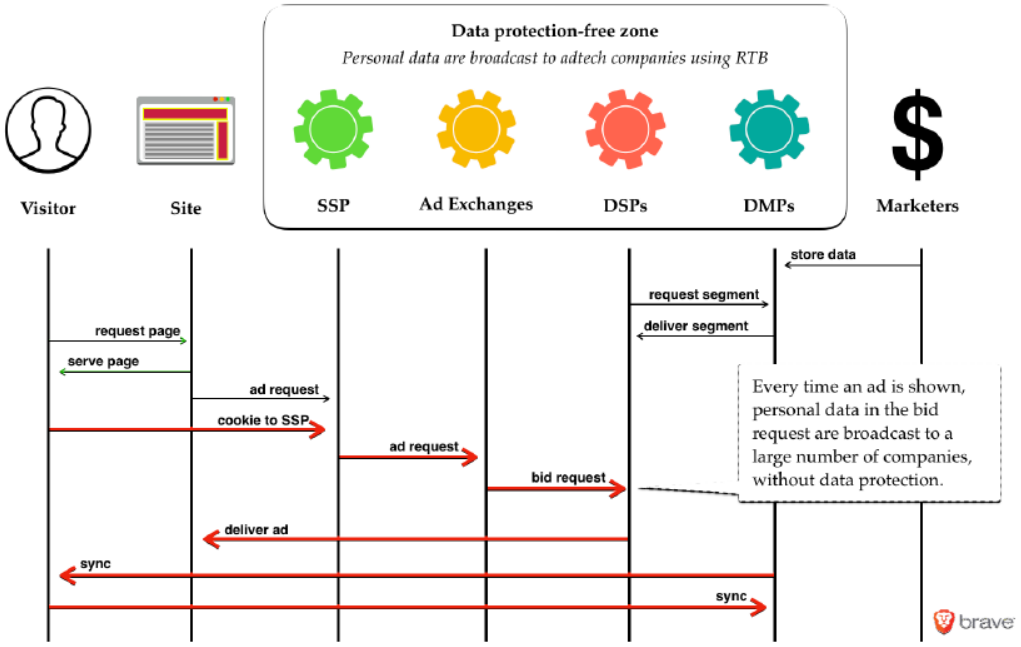
● Az IP címed (az "RTB"-rendszer típusától függően)

● Az adatközvetítő szegmens azonosítója, ha van. Idetartozik a személy jövedelemszintje, életkora, neme, szokásai, közösségi médiafogyasztása, etnikuma, szexuális orientációja, vallása, politikai beállítottsága stb. (az "RTB"-rendszer típusától függően)

Az eredeti angol nyelvű jelentés 1. és 2. mellékletében található egy teljeskörű tájékoztató a licitfelhívásokhoz felhasznált személyes adatokról. A termékleírások vonatkozó részeit a 3. és a 4. melléklet tartalmazza.

Működési elvek

Az alábbi ábra az információáramlás mikéntjét mutatja.



A személyes adatok szórására az RTB rendszerben az "RTB licitfelhívás" (RTB bid request) kifejezés utal. Általában széles körben szórják az adatokat, hiszen olyan cégektől próbálnak meg ajánlatokat begyűjteni, amelyek azt szeretnék, hogy ha valaki feltölt egy weboldalt, az mindjárt meglássa a hirdetésüket. Az RTB licitfelhívásokat a weboldalak részéről "kínálati oldali platformoknak" (*supply side platform*, SSP), valamint "hirdetéscserélőknek" (*ad exchange*) nevezett cégek terjesztik, és megannyi "keresleti oldali partner" (*demand side partner*, DPS) kapja, amelyek azután megfontolják, licitáljanak-e arra, hogy a hirdetést megmutathassák az adott személynek. A DPS a hirdető nevében jár el, ő dönti el, mikor teszi meg az ajánlatot annak a személynek a profilja alapján, akit a hirdető számára meg kell céloznia. Előfordul, hogy az "adatkezelési platformok" (*data management platform*, DMP) az adatok felhasználásával "egyeztetnek" az illető személy meglévő profiljának gazdagítása végett.

Az RTB nem ellenőrzi, mi lesz a személyes adatok sorsa azután, hogy egy SSP vagy egy hirdetéscserélő továbbította a "licitfelhívást". Még ha biztonságos is a licitfelhívás útja, akkor sincsenek olyan technikai intézkedések, amelyek elejét vehetnék annak, hogy aki megkapja a licitfelhívást, az, mondjuk, más adatokkal kombinálva profilt alkosson valakiről, vagy tovább értékesítse az adatait. Miután egy DSP hozzájutott a személyes adatokhoz, szabadon, kénye-kedve szerint kereskedhet velük újabb üzleti partnerek bevonásával.

Különösen súlyos gyakorlat ez annak fényében, hogy a szóban forgó adatok minden bizonnyal "különlegesnek" minősülnek. Elárulják, mit néz valaki az interneten és gyakran azt is, pontosan hol

tartózkodik. Felfedik, milyen az illető szexuális orientációja, vallásos meggyőződése, politikai beállítottsága, etnikai hovatartozása. A “szegmens azonosító” továbbá azt is jelzi, hogy az adatkereskedő vagy más, hosszú távú profilalkotással foglalkozó közvetítő által talált személy milyen kategóriába tartozik.

Összefoglalva, ebben a hirdetési rendszerben tökéletesen megoldatlan a személyes adatok védelme. Széles körben elterjedt és igen aggasztó jelenségről van szó. Az iparág működése gyakorlatilag minden európai internetező alapvető jogait veszélyezteti.