

Panopticlick: mennyire biztonságos a böngésződ?

PCLinuxOS Magazine – 2016. június

Írta: Paul Arnote (parnote)

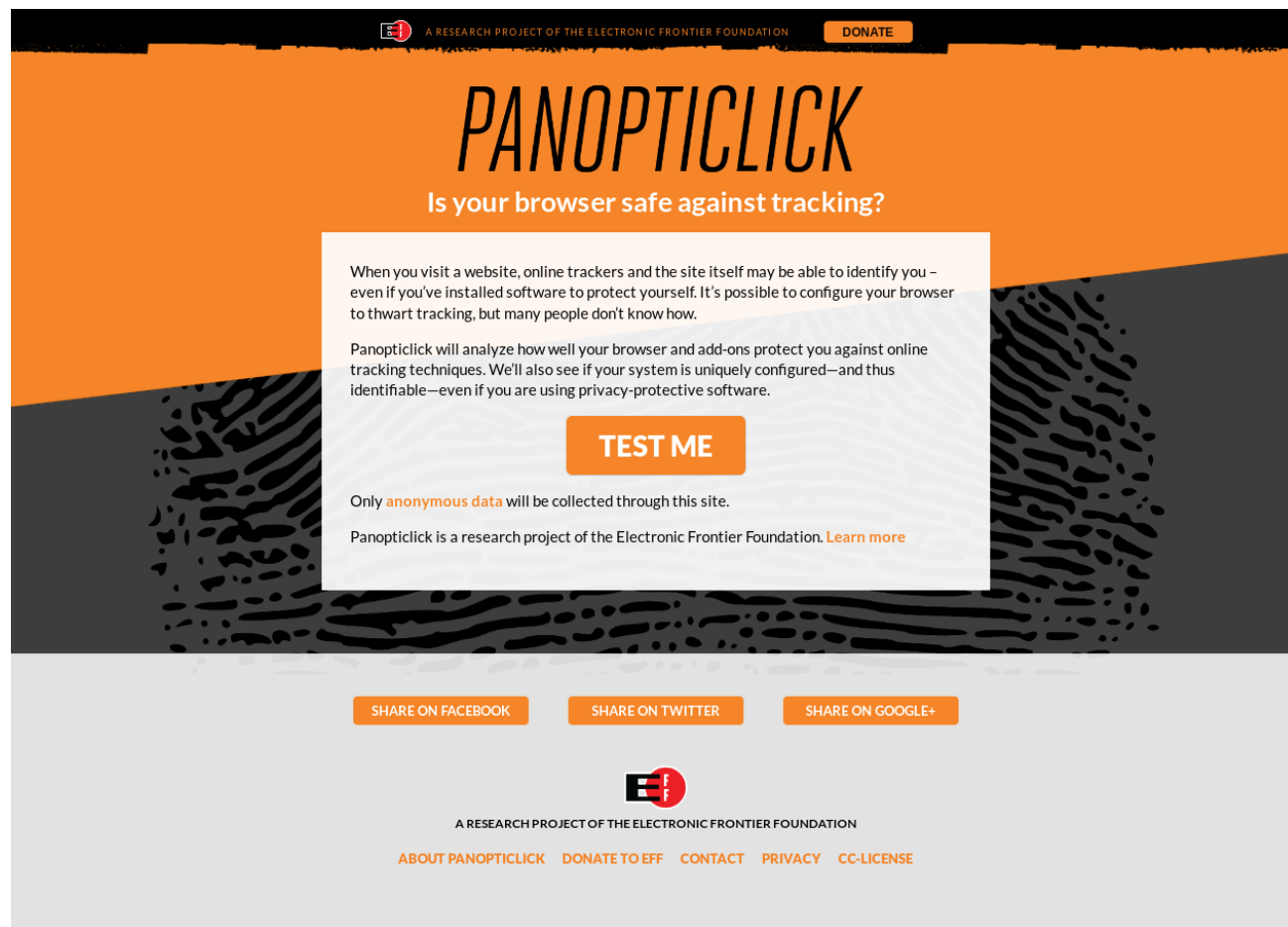
Manapság sok felhasználó fokozottan törődik a személyes adatai fokozott védelmével. Vonatkozzék az akár a Kormány, akár annál sokkal rosszabb szándékú egyedek részéről személyes adataink gyűjtésére. Személyes adataink biztonságban tartása nagy jelentőségű kérdés. Még a különféle honlapok által alkalmazott nyomkövetés is számos dolgot felfedhet az érdeklődési körünkről, vásárlásainkról és tevékenységünkről.

De mennyire biztonságos az az eszköz, amit az online tevékenységed során többnyire használsz: a webböngésző? Meglepő, mi minden derülhet ki. Az [Electronic Frontier Foundation \(EFF\)](#) egy kutatási projektjének köszönhetően könnyen megállapíthatod, hogy mennyire védett a böngésződ a nyomkövetéssel szemben. Ki más vezethetné a magánélet fenntartásáért folytatott küzdelmet, mint az a szervezet, ami mindig is és most is e kérdésben az első vonalban harcol. A kutatási projekt a [Panopticlick](#).

A Panopticlick céljait legjobban az EFF nyilatkozata összegzi:

A Panopticlick kutatási projekt célja jobban megismerni az online nyomkövetési eszközöket és technikákat, valamint vizsgálni a személyes biztonságra való kiegészítők hatékonyságát.

A Panopticlick nem teljesen új. Az EFF 2010-ben indította a Panopticlick-et az egyes böngészők egyediségének vizsgálatára. Anonim módon gyűjt adatokat az operációs rendszer, a böngésző, illetve kiegészítői beállításairól és verziószámáról. Ezután összeveti a beállításaidat más felhasználók adatai alapján felállított adatbázissal, és ad egy egyediségi „osztályzatot”. Az osztályzat felfedi, hogy a web-et



böngészve mennyire (vagy mennyire nem) vagy azonosítható. 2015-ben az EFF kiegészítette a projektet nyomkövető-blokkolás ellenőrzésével is. Az új kiegészítés méri, mennyire hatékonyak az olyan nyomkövetést blokkoló kiegészítők, mint az AdBlock Plus, a Ghostery stb., amik segítenek megvédeni a tolakodó adatgyűjtéstől.

A Panopticlick oldalára látogatva kattints a „TEST ME” gombra, a böngésződ ablakának közepén. Ne félj, anonim adatgyűjtés történik (hiszen ez az EFF, és ha ők azt mondják, anonim az adatgyűjtés elhiszem...állhatatos küzdelmük és kivitt hírnevük a tét). Ezután megvizsgálja, hogy a böngésződ és kiegészítői mennyire védettek a követési eljárásoktól és a személyes és magán adataid gyűjtésétől.

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

DONATE

PANOPTICCLICK

Is your browser safe against tracking?

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Yes! You have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.

Help us defend the Web against tracking:

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting ?	✗ your browser has a unique fingerprint

Show full results for fingerprinting

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticklick does not measure all forms of tracking and protection.

RE-TEST YOUR BROWSER

Thanks to **Fingerprint2** for various fingerprinting tests, **Aloodo** for portions of the tracker test, **browserspy.dk** for the font detection code, and to **breadcrumbs** for supercookie help. Send questions or comments to panopticklick@eff.org.

SHARE ON FACEBOOK

SHARE ON TWITTER

SHARE ON GOOGLE+

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

[ABOUT PANOPTICCLICK](#)
[DONATE TO EFF](#)
[CONTACT](#)
[PRIVACY](#)
[CC-LICENSE](#)

Néhány tesztelő képernyőt megjárva a Panopticklick megjeleníti az eredmény-összefoglalót. Mivel én többnyire Firefox-ot használok, az itt bemutatott eredmény arra a böngészőre vonatkozik. Én az Adblock Plus-t használom vele. Régebben a Privacy Badger-t (EFF), a Ghostery-t és néhány más ilyen kiegészítőt is használtam, de azóta kikapcsoltam azokat, mivel tapasztalataim szerint nagyon visszafogták a számítógépet, vagy túl sok engem érdeklő tartalmat blokkoltak. Amennyire szeretném a böngészési szokásaim és adataim gyűjtését blokkolni, legalább annyira fontos egyensúlyt tartani a böngészés során. Amikor az eszközök a böngészésedet nehezítik, akkor azok az eszközök gátolnak és utadban állnak, hogy elvégezd a dolgodat és élvezd a munkát.

A táblázat alatt a „Show full results for fingerprinting” hivatkozásra kattintva megmutatja, mennyi információt adsz ki egy weblapot meglátogatva. Valószínűleg legalább annyira meg fogsz lepődni, mint én. Nem mutatom meg az eredményeimet itt, két okból. Először is túl hosszú. Másodszor az eredményeid mások, mivel valószínűleg más betűket használsz (igen, a betűtípusnak szerepe van az azonosításban) és valószínűleg más kiegészítőket telepítettél.

Miért a Panopticlick?

Amikor egy weblapot meglátogatsz, a számítógéped beállításairól rengeteg adat válik elérhetővé és kerül megosztásra. Az információk (op. rendszer, böngésző, verziók, telepített betűkészletek, kiegészítők stb.) alkalmasak egyedi „ujjlenyomat” készítésére, amik később felhasználhatók személyed és géped azonosítására.

NAGY izgalmat váltott ki, amikor pár éve a nagyobb webböngészők alkalmazták a Do Not Track-et (Ne Kövess). Helyes alkalmazás esetén megszabadítja a felhasználót a web-en történő követéstől. Ugyanakkor ez nem következett be, mivel a Do Not Track tiszteletben tartása teljesen önkéntes. Ez azt

eredményezte, hogy azon weblapok [listája](#), amelyek figyelembe veszik, elég rövid. Ne okozzon csalódást, ha a kedvenc honlapod nincs a listán. Valószínűleg nem felel meg a feltételeknek.

Amikor bemutatták, azzal kecsegtetett, hogy a felhasználókat ugyanúgy védi majd, mint ahogy a népszerű Do Not Call (Ne Hívj) lista védi az amerikai telefonhasználókat. Ugyanakkor az internetes hirdető cégek többszöri ígéretei ellenére ebben nem történt előrelépés. Valójában a haladás lényegében teljesen érzékelhetetlen, mivel a Do Not Track szabványosítását a World Wide Web Konzorcium megakadályozta annak ellenére, hogy amerikai és európai politikai döntéshozók több ízben is kérték.

Így vannak olyan weboldalak, mint a PCLinuxOS Magazine-é, amik nem érdekeltek a weblapjukat látogatók követésében. Bárcsak ilyen egyszerű lenne a dolog.

2015 novemberében az Egyesült Államok Szövetségi Hírközlési Bizottsága (FCC) [elutasította](#) a Do Not Track figyelembe vételének kötelezővé tételét. A Hivatal petíciót alapján járt el, ami azt követelte, hogy néhány a legnagyobb webes cégek közül – például a Google, a Facebook, a Netflix, a Pandora, a YouTube és a LinkedIn – vegye figyelembe a nem-követési kérést.

Nem minden böngésző egyforma

Mint sok felhasználónak, a számítógépemen több böngésző van. Kíváncsiságom kielégítésére betöltöttem a Panopticlick weblapot mindegyikkel, hogy lássam az eredményt. Az eredmény meglepő lehet.

A Firefox, a Chrome és a Slimjet egyformán szerepelt, azonos eredményt értek el a korábban bemutatottal. Mind védett a követő hirdetésektől és blokkolta a láthatatlan nyomkövetőket, de képtelen volt azok blokkolását feloldani, akik a Do Not Track tiszteletben tartását jelezték és nem védett az ujjlenyomatkozás ellen.

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track ?	✗ no
Does your browser protect from fingerprinting ?	✗ your browser has a unique fingerprint

A Midori és az Opera csak a nyomkövető hirdetésektől védett. Engedték a láthatatlan követőket, képtelen voltak azok blokkolását feloldani, akik a Do Not Track tiszteletben tartását jelezték és nem védtek az ujjlenyomatkozás ellen.

Vélhetően, a legjobb, amit az ujjlenyomat-készítés elleni védelem érdekében tehetsz, hogy a Tor böngészőt használd. Működési jellemzői jóval túlmutatnak az ujjlenyomat elleni védelmen. A Tor böngésző használatának árát avval fizeted meg, hogy sokkal lassabb, mint bármelyik másik böngésző.

Összefoglalás

Az EFF a Panopticlick projektben megnyilvánuló erőfeszítésért tapsot érdemel. Remélhető, hogy az adatgyűjtésük következményeként a felhasználók információkat kaphatnak arról, hogyan tudják legjobban megvédeni magukat a nyomkövetéstől és így védeni adataikat.

Kétséges, hogy a Do Not Track, a tiszteletben tartására vonatkozó kötelező érvényű (technikai, illetve jogi) szabályok nélkül valaha is eléri a fogyasztók és felhasználók által remélt célt. Valójában jogi és technikai szabályok nélkül a Do Not Track elég haszontalan, hatástalan és halott.

Addig is az internet-felhasználók csak abban reménykedhetnek, hogy vannak olyan szervezetek – mint az EFF –, amik a legjobb védelmet nyújtó böngészőkről és kiegészítőikről adatbázist vezetnek. Tehát a részvételed (a kutatási projekt számára adatot szolgáltatva) segíti az EFF-t, hogy megbízható információkat adhasson a többi felhasználónak segítve a személyes adatai és a böngészési szokásai védelmét.

