Fekete Bálint

-

Privacy az interneten

0.9.6.0

2021-05-07

fekete.balint @protonmail com

Tartalomjegyzék

fekete.balint @protonmail com

1. Bevezető

„Több, mint negyven oldaaal??!

Nincs ebből valami rövidebb kivonat? Tudod, olyan infografikás izé.”

**Ha kizárólag a privacyval kapcsolatos gyakorlati tippek érdekelnek,
akkor lapozz rögtön a 7. fejezethez.**

Miről szól a szöveg?

Röviden összefoglalva ez egy „Privacy 1x1” az informatikában nem jártas átlagembereknek – olvasmányos formában. Szabadságjogok, személyes adatok védelme, mentális hatások, tech óriások.

Mire ad választ?

Például arra, hogy milyen egyszerű, bárki által elvégezhető gyakorlati lépéseket tehetek, ha nem akarom, hogy személyes adataim és netes tevékenységeim nagyvállalatok profilozó adatábázisait gazdagítsák és úgy adják-vegyék, akár krumplit a piacon.

Hogy készült?

Nos, ez az írás eredetileg havi bontásban jelent meg a Kaméleon magazin virtuális felületén – részenként jellemzően 2-3 oldalon. Nem vitás: akkora mennyiségben könnyebben emészthető lehetett, hiszen pár metrómegálló alatt elfogyasztható egy-egy ilyen hosszúságú cikk.

Ugyanakkor szerettem volna egy dokumentumban összeszedni, összecsiszolni a szöveget, aztán bővülni kezdett, új fejezetek, aktualitások, képek kerültek bele, a jellege is kezdett lassan megváltozni.

Mostanra leginkább oktató célú kézikönyvvé vagy tanulmánnyá nőtte ki magát. Sok hasonló témájú cikk született az utóbbi időben (szerencsére), két területen viszont véleményem szerint mind hiányt szenvednek: a „**Miért** fontos ez?” kérdésre adott, mélyebb elemzésen alapuló válasz, illetve az egyéni szabadságjogok nézőpontja úgy vélem csak igen érintőlegesen jelenik meg a publikusan elérhető szövegekben.

Hol érhető el?

A dokumentum mindenkori legfrissebb verziója az alábbi állandó linken érhető el:

https://github.com/kaktusztea/tudatosonlinejelenlet/raw/master/FeketeBalint_Privacy_az_interneten.pdf

2. Alapfogalmak, „miért kéne ennek érdekelnie egyáltalán”?

A két nő belépett a kávéházba. Maga a tulajdonos sietett eléjük és hellyel kínálta őket az emeleti teraszon, ahonnan remek kilátás nyílt a belvárosra. A vendégek kávét rendeltek majd beszélgetésbe merültek.

Pár perc udvariaskodás után a magasabb nőből hirtelen kiszakadt, hogy elveszítette az állását, ráadásul igen megalázó körülmények között. Beszéde sírással keveredett – barátnője együttérzően hallgatta.
Megérkeztek a kávék – némi aprósüteménnyel díszítve... és velük a kávéház tulajdonosa is, aki kényelmesen letelepedett az asztal harmadik székére. Kezében egy vaskos jegyzetfüzetet tartott. Kinyitotta, ráérősen fellapozta az első üres oldalt, a tetejére odabiggyesztette a dátumot és időt, majd várakozóan vendégeire tekintett, akik megütközött tekintettel bámultak rá.

– Nyugodtan folytassák, kérem. A kávéjuk és a kiszolgálás mind ingyen volt, cserébe leiratot készítek a beszélgetésükről, amelyekből a legtanulságosabb részeket publikálom hamarosan megjelenő könyvemben, a többit marketing cégek számára értékesítem. Továbbá engedelmükkel a beszélgetés tartalma alapján célzott reklámokat küldök majd ki önöknek, amelyekből én is pár százalék részesedést kapok – így mindenki jól jár: önök, a hirdetőcég és én is.
– Mégis mit képzel?! Hogy gondolhatja, hogy így megsértheti a személyes beszélgetésünket..., a privát szféránkat? Hogy gondolhatja, hogy valaha is beleegyezünk ilyesmibe?!" – kérdezte feldúltan a balján ülő nő. A tulajdonos arcán értetlen zavar suhant át.
– Nem teljesen értem a problémát... Önök használnak Gmailt, vagy Facebook Messengert? – mutatott az asztalon fekvő mobiltelefonokra.
– Igen... de hogy jön ez most ide?
– Akkor már most is használják ezt az üzleti modellt, amit az imént felvázoltam. A személyes adataikért, beszélgetéseik tartalmáért (csevegés, email, esetünkben szóbeli beszélgetés) cserébe szolgáltatást nyújtok. Önök jóravaló embereknek tűnnek, gondolom ***nincs titkuk, nincs mit titkolniuk****, nem?*

A fenti fiktív történet egy analógiát próbál vonni korunk egy igen fajsúlyos problémájával, amellyel manapság leginkább az internetes térben találkozunk. Amiről most szó lesz, arra az angol nyelvben a „**Privacy”** kifejezést használják – magyarban (még?) nem találtunk megfelelő szót, kifejezést rá, csak körülírni tudjuk, nagyjából így: „Személyes adatok birtoklásának joga”, „Adatvédelem”, „Magánélethez való jog”, „Digitális biztonság joga”.

Először is oszlassunk el egy alapvető félreértést: a privacy (a cikkben jobb híján ezt a szót fogjuk használni) NEM a rejtőzködésről szól.

Privacy
Az ember alapvető szabadságjoga ahhoz, hogy rendelkezhessen saját személyes adataival..
Vagy másképp: "Privacy is a basic human right"

Gondoljunk a nők szavazati jogára, a kötelező pihenőnapra, a törvény előtti egyenlőség fogalmára: mind olyan alapértékek, amelyeket ma alapvetésként élünk meg, de egyik sem volt evidencia a saját idejében: időbe telt, míg kiharcoltuk őket, és szükségességüket mindenki megértette és elfogadta. „Miért fontos ez?” – merült fel akkor is, csak a téma változott. Ahogy a fenti szabadságjogok kiharcolásának idejében is, a legnagyobb próbatétel most is a téma elmagyarázása – sokan egyszerűen nem értik, miért is van erre szükség, vagy hogy „mi ez az egész”, minek kell?

A cikk első fejezetében ezen kérdések megválaszolására teszünk kísérletet, későbbi részekben a rólunk gyűjtött adatokról és kereskedelmükről, személyes profilok építéséről lesz szó, végül pedig bemutatjuk azokat a gyakorlati – hétköznapi fejjel is jól érthető – konkrét, tudatos megoldásokat, amelyeket bárki könnyen alkalmazhat internetes jelenlétének védelme érdekében.

„Nincs titkom, nincs mit titkolnom” – ezzel a klasszikus hárító mondattal mi is sokat találkozhattunk, mikor a személyes adatok biztonságáról esett szó egy társalgásban – talán már mi is mondtuk párszor. Azonban jóval összetettebb okok rejtőznek a kijelentés mögött, mint elsőre hinnénk.

Vegyük sorra, hogy privacy témában milyen külső/belső mentális hatások érnek minket, amelyek nagyban meghatározzák a témához való viszonyulásunkat:

1. Külső befolyás – jellemzően a média által. Ezzel a témával foglalkozni nem „menő”, inkább „ciki”, senki nem akar ciki lenni.
2. Külső befolyás – közösségi oldalak nárcizmus-gerjesztése: a privacy ellene megy a folyamatos posztolásnak, minden apró életpillanat megosztásának.
3. Mély, belső félelmek: „Kikerül minden privát adatom”, „Nem értek hozzá, nem tudok védekezni”.
4. Információhiány: mi ez a privacy egyáltalán? Nem értem, mi a probléma, amiről beszélnek.

A fenti hatásokban közös, hogy a végső eredményük valamilyen belső szorongás, amit az agyunk természetesen megpróbál feloldani, hiszen szorongani senki sem szeret. Ilyenkor jönnek a különböző…

fekete.balint@protonmail.com

Megküzdések és reakciók

a) Menőzés: „*Tőlem aztán mindent láthatnak, kit érdekel”* (menő vagyok, hiszen gondtalannak tűnök).
b) Paranoid rettegés: az illetőnek nem sikerül feldolgoznia a személyes adatai szivárgását, mindenhol megfigyeléstől tart, de mivel szakmai ismeretei hiányosak, rettegésbe merül.
c) Kognitív disszonancia redukció: az agyunk nehezen bírja a nyomást, de gyorsan feltalálja magát, kitalál valami egyszerű magyarázatot, miért is jó, ha nem teszünk semmit. Ilyen mondatok bukkannak fel ilyenkor:

- „Nincs titkom, nincs mit titkolnom!”
- „Ezek úgy is mindent tudnak.”
- „Nem vagyok paranoid, én ezzel nem foglalkozom!„
- „Ez csak titkolózás, üldözési mánia!„
- „Már húzom is az alufólia-sisakot, haha!„ (humor, mint hárító stratégia)

A privacy valójában fontos téma, de sokszor sajnos jó szándékkal rossz üzeneteket közölnek a szakértők az ismeretterjesztés során. Legtöbbször félelemkeltést alkalmaznak, ami után magára hagyják az olvasót, aki – mivel nem kapott javaslatokat a megoldásokra – hárító megküzdési stratégiákhoz nyúl.

Az értelmes megközelítés ezzel szemben az lenne, hogy ismertessük a szituációt, oszlassuk el az általános, túlzó félelmeket, mutassuk be a privacy morális fontosságát személyes és globális társadalmi szinten. Ezek után mutassunk be az átlagember számára is megvalósítható, kézzelfogható, mindennapi megoldásokat és erősítsük a hitét, hogy lehetséges és érdemes egyszerű lépéseket tenni az adatvédelemmel kapcsolatban.

Talán furcsa lehet a hosszú bevezető, de világnézeti alap és meggyőződés nélkül nincs mire építkeznünk – ezek nélkül nincs motiváció a tudatos cselekvésre sem.

fekete.balint @protonmail com

3. Össztársadalmi hatás, adatgyűjtési 1x1

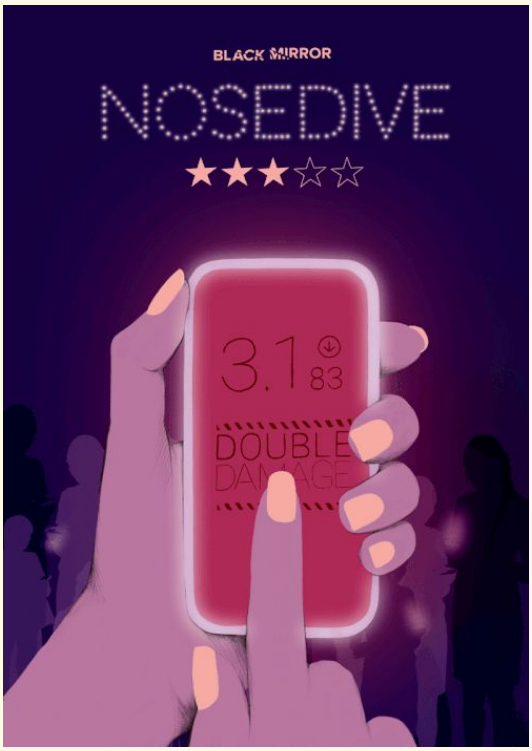
Az előző részben átvettük, hogy mit is értünk privacy alatt és miért fontos, még akkor is, ha épp most nem érezzük pillanatnyilag, hogy hátrányunk származna a figyelmen kívül hagyásából.

Globális felelősség

Fontos gondolat, hogy ezek az elvek nem csak rám – az egyénre – vonatkoznak, ez egy egyetemes szemléletmód, amely magába foglalja a szolidaritást is olyanokkal, akiknek jogaival szemben – bárhol a világon – személyes adataikat felhasználva visszaélnek.

Lehet, hogy nekem „épp nincs titkom”, de ne kizárólag a saját országunk épp aktuális erkölcsi és törvényi szabadságát tartsuk szem előtt. Azzal, hogy otthon nem emelünk szót személyes adataink korlát nélküli gyűjtése ellen, legitimáljuk ezt a jelenséget, és ezzel hatalmas mozgásteret biztosítunk a technológiai cégeknek. Így például előfordulhat, hogy a szabályozatlan módon begyűjtött adatok segítségével egy elnyomó rezsim az emberi jogokat súlyosan sértő tetteket hajthat végre.

Erre jó példa a nemrég bevezetett kínai társadalmi pontrendszer, ahol az arcfelismerő kamerákkal telepakolt országban minden személyt egy egyedi pontszámmal értékelnek – attól függően hogyan viselkedik. Sokat vagy mértékkel iszik -e alkoholt, mit vásárol a boltban, figyel -e a tanórán, vagy bambul, szorgalmas -e, vagy lusta... kritizálja -e az államhatalmat... Az alacsony pontértékű állampolgárok nem juthatnak hitelhez, gyerekeik nem járhatnak egyetemre, extrém esetben kizárják őket a távolsági közlekedésből. Digitális börtön. Az alábbi linken két konkrét kínai személy szempontjából láthatunk bele a fentiekbe, egy interaktív cikk keretében: link.



Forrás: imdb.com

A fenti kínai megoldás ismerős lehet az utóbbi idők egyik legelgondolkodtatóbb sorozata, a Black Mirror, Nosedive (Fekete Tükör, Szabadesés) című részéből, amelyben szintén személyes pontrendszer fon át egy látszólag idilli világot. A fenti sorozat további részei is erősen ajánlottak, mindegyik egy-egy önálló történet lehetséges, közeli jövőképekről, amelyekben a technológia hatására társadalmunk, személyes kapcsolataink lényegesen megváltoznak.

Örülhetnénk, hogy ez azért nem Kína, de a Magyarországon nem is olyan rég elfogadott megfigyelési törvény (T/15054. számú törvényjavaslat, kihirdetés után: 2017. évi XCIII. törvény, amely 2018. július 1. dátummal lépett hatályba), illetve az ország minden köztéri kamerájának képét központi adatbázisba szervező *Szitakötő projekt* nem sok optimizmusra ad okot. Ez utóbbihoz arcfelismerő szoftverek beszerzését is megkezdte a magyar állam. Némi korlátot csak az EU által 2018 májusában elfogadott GDPR rendelet ad.

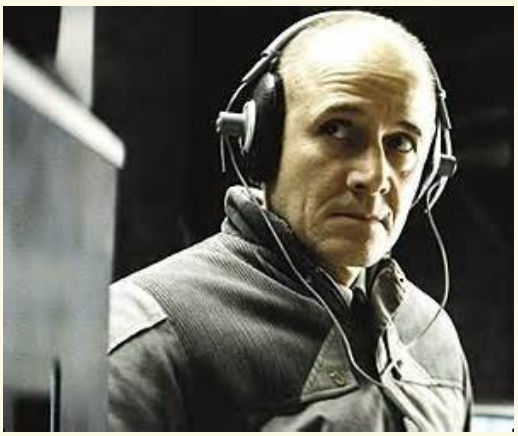
Most lássunk pár alapvetést, hogy miért is fontos a személyes adatok védelme és megfelelő kezelése.

Evidenciák

A privacy lényege, hogy mindenki saját maga kell birtokolja és irányítsa a róla szóló információkat. Másképpen: a rólad szóló adat a TE tulajdonod, nem fizetőeszköz. Angolban elterjedt formában: *“Don't pay with your data!”*

Ha úgy gondolod, hogy "nincs titkod", fontold meg az alábbiakat:

- A lakásod ajtaját is bezárod, mert tisztában vagy vele, hogy nem ideális világban élsz.
- Az adatlopás, internetes bűnözők, zsaroló vírusok sem az ideális világ részei.
- Az az élmény, hogy... bőgtél a vizsgád után, szerelmes lettél, majdnem elütött a villamos, a gyereked autista, vagy tegnap kórházba került, megszerezted a diplomádat, megcsalt a párod, külföldre költözöl, depressziós vagy, és így tovább... ezek mind csak rád tartoznak és azokra, akiknek úgy döntesz, hogy ezt elmondod. A való életben ez evidencia, de a netes térben nem látjuk saját szemünkkel a (jelenleg legálisan!) hallgatózó harmadik felet, ezért könnyebben hitetjük el az agyunkkal, hogy ez nem olyan nagy ügy.
- Egy társalgásban egy mondatnak van feladója és címzettje. Jelenleg viszont elfogadottá vált, hogy egy hallgatózó harmadik fél is ellenvetés nélkül végighallgat mindent, cserébe a *“teraszért, ahol ültök és a kávéért, amit isztok”* azaz a szolgáltatásért (lásd az első fejezet bevezetőjét). Így aztán a fenti példákhoz hasonló személyes gondolatokat lazán elküldjük ismerőseinknek mondjuk egy Facebook Messenger üzenetben, ahol ez automatikusan mind kielemzésre kerül és profilunk építését szolgálja a Facebook és partnercégei számára.



Érdekes kontraszt, hogy míg a Kelet-Német (NDK) kommunista rezsim alatt a Stazi mikrofonokat rejtett a lakásokba és erre elborzadva gondolunk mind vissza, ma önként telepítünk Alexa és Google Home személyi asszisztenseket a nappalinkba, 0-24-ben bekapcsolt mikrofonokkal.

Kellemetlen ezekre rágondolni, de az ingyenesség és a kényelem simogató flow élményt nyújt és ez minden másnál jobban segít ignorálnunk a kellemetlen gondolatokat.

Ingyenes internetes szolgáltatások telepítésekor a pár másodpercre felugró, majd olvasás nélkül azonnal elfogadott felhasználói feltételekben (EULA) felhatalmazzuk a szolgáltatókat, hogy nagyjából bármit megtehetnek személyes adatainkkal, tartalom elemzést végezhetnek mindenen – a Google minden levelet, a Facebook minden Messenger üzenetváltást automatikusan “elolvas” és kielemez.

Lehet, hogy ez először zavar minket, de mivel "mindenki használja", lassan elhisszük, hogy ez nem is olyan nagy dolog – "megfő a béka", ahogy mondani szokás a kártékony, de lassúsága miatt alig észrevehető változásokról.

fekete.balint @protonmail com

Meglepő fordulat, hogy mikor munkahelyünk céges információi kerülnek lehetséges veszélybe, azonnal az adatvédelem bajnokaivá válunk – hogy lehet, hogy ilyenkor felfogjuk a jelentőségét és mindenek előtt: hogyhogy a céges információk fontosabbak számunkra, mint saját személyes adataink..?

Álljon itt egy idézet *Edward Snowdentől*, amerikai volt NSA alkalmazott és etikus kisziárogtatótól:

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say"

azaz:

"Azt állítani, hogy a magánélethez való jog fölösleges annak akinek nincs rejtegetnivalója olyan, mint azt állítani, hogy a szólásszabadsághoz való jog felesleges annak, akinek nincs mondanivalója."

fekete.balint @protonmail com

Netes szolgáltatók üzleti modellje

Évekkel ezelőtt megköttetett egy kimondatlan megegyezés, felépült egy új, bizarr üzleti modell, amiről nem folyt semmilyen diskurzus, vagy megelőző egyeztetés – csak úgy kialakult: adatért cserébe szolgáltatást, kényelmet biztosítanak egyes tech cégek és ezt "ingyenesnek" kommunikálják. A csavar, hogy itt “*Te vagy a termék*”, nem valamilyen árú vagy pénz. Egy ilyen üzleti modell elsőre felháborító lenne, de mostanra már természetesnek tűnik, hiszen megszoktuk. A modell jellemzője, hogy önként átadjuk minden – használat során keletkező – digitális adatunkat a szolgáltatásért cserébe, beleértve annak elemzését is, hogy hogyan, mikor, mire használjuk a szolgáltatást.

Groteszk hatás, de az "ingyenes" szolgáltatások pont egy társadalmi szegregáció elindítói lettek, hiszen a gazdagok tudják megfizetni a privacyt fizetős szolgáltatások keretében, ahol (jó esetben) a fizetség egyik előnye, hogy nem gyűjtik az adataikat – csak hogy ennek nem extrának, hanem alapvetésnek kéne lennie.

De kik is gyűjtik az adatainkat? Jellemzően tech és szórakoztató cégek, valamint kormányok (lásd: Five Eyes, Nine Eyes, Fourteen Eyes), a kereskedő, szolgáltató szektor és persze a bűnözők.

A következő fejezetben adatkereskedelemről és a profilépítésről lesz szó, de már közeleg a megoldásokról szóló rész is, hiszen a cél nem a félelem keltése, hanem a tudatos viselkedés megteremtése az online térben, ami nem is olyan nehéz, mint hinnénk.

fekete.balint @protonmail com

4. Adattermelés, nárcizmus, szabályozás

Legutóbb a privacy globális felelősségét érintettük, illetve hogy mennyire könnyen ignorálunk egy olyan belehallgatást beszélgetéseinkbe, ahol a harmadik fél nincs jelen fizikailag, illetve nincs köztünk közvetlen ismerettség.

Felületesen belepillantottunk az internetes szolgáltatók üzleti modelljébe, innen folytatjuk most. Ismét fontos kihangsúlyozni, hogy a cél nem a rettegés keltése, hanem a megismerés – esküszünk, pár fejezet és már az egyszerű és hatékony megoldásokról fogunk írni. Előtte viszont szükséges a világkép felépítése, hogy értsük, milyen közegben mozgunk és miért fontos tudatosan viselkedni benne.

A közösségi média adattermelése

Az előző részben bemutattuk, hogy a nagy netes szolgáltatók ingyenessége látszat csak – valójában a saját adatainkkal fizetünk, mi vagyunk a termék.

Értelemszerű tehát, hogy ezen cégeknek a nagyobb bevétel érdekében minél több és több nyers adatra van szüksége. Például a Facebook esetében minél több tartalommegosztást végzünk, annál hasznosabbak vagyunk számára, hiszen főleg ránk szabott, célzott reklámok értékesítéséből él. Minél pontosabban tudja, milyen reklámok érnek el bennünket, annál több pénzért adhatja el a megbízóinak hirdetéseit. Például ha egy hirdető cég 20 és 39 év közti, budapesti, elektronikus zenét szerető, jó anyagi körülmények közt élő, liberális, egyedülálló, nagy médiafogyasztású, egészséges, sport iránt érdeklődő emberekre szeretné szakkifejezéssel „targetálni” a reklámjait, akkor a Facebook tud ilyen felhasználókból álló csoport listát generálni (és eladni) számára, mert van annyira részletes a felhasználóiból épített profil-adatbázis, hogy ezt könnyen megteheti. Ez után a megbízó cég reklámjai csak a fenti csoport tagjai számára jelennek meg a Facebook felületen, várhatóan nagyobb elérést, kattintást generálva, mintha csak random levélszeméttel szórtak volna meg pár millió embert.

Viszont a hatékony és nagy mennyiségű profil felépítése olyan mint egy búzaföld gondozása: a bőséges aratáshoz nagy terület, sok és jól táplált kalász (személyes profil) kell.

A szolgáltató célja tehát, hogy rávegyen minket a rendszeres tartalomgyártásra. Az “ingyenesség” és a végtelen tárhely is ezt az impulzust erősíti, a felhasználó még hamis öntudatosságot is érezhet: “*Én aztán nem fizetek semmiért, minden ingyen van! Nehogy már lehúzzanak pénzzel.*”

Hatékony eszköz a tartalomgyártás felpörgetésére a *nárcizmus* gerjesztése is. A közösségi média felületei folyamatosan posztolásra bíztatnak, arcunkba tolják ismerőseink legidillibb képeit, ezzel

szorongást váltva ki: “*Az ő életük milyen idilli, nekem is meg kell mutatnom, hogy nem vagyok szerencsétlen, én is tudok napozós képet posztolni a tengerpartról koktéllal és keresztbetett lábbal ((még akkor is, ha a szívem mélyén sokkal inkább lennék valahol máshol, ami kevésbé “idilli”, de jobban érzem magam ott)).*”

Abba bele se gondolunk, hogy ismerőseink idillje legtöbbször hazugság, hosszas állítgatás áll a “tökéletes” fényképek elkészítése mögött és mindennapi lelki problémáik, szorongásaik sem jönnek át a szépia szűrővel felturbózott képeiken át.

A nárcizmus ilyen fajta gerjesztése sokakat arra sarkallhat, hogy be kelljen mutatniuk életünk minden pillanatát – idealizált formában természetesen. A közösségi médiában mindenki saját bulvármagazinjának főszerkesztőjévé válik, az önvédelmi reflexek kikapcsolnak, végtelenül kitolódik az “*ezt azért már nem*” határa.

Az *érzelmi inkontinencia* is erős tünet, sokan minden lelki gondjukat – annak felbukkanásának pillanatában – kiírják az üzenőfalakra, (részben) elkerülve ezzel a probléma feldolgozását, átnyomva a szorongást az ismerőseikre, akik a huzamosabb terhelés után általában diszkréten az ismerős posztjainak elrejtését választják.

A lájkvadászat ugyancsak brutális ösztönző – hamis önbecsülést merítünk a lájkok számából, azt hisszük (rosszul), hogy a lájkok száma posztunk (ezen keresztül saját magunk) értékét becsüli fel, komoly szorongást keltve, ha számuk alacsony és újabb posztolásra csábítva, ha magas – egyfajta mentális drogként hatva agyunk jutalmazó központjában. Jól látható, hogy a közösségi média ösztönös használata számos mentális probléma megjelenéséhez és elfajulásához vezethet.

A fent taglalt poszt-viharban szinte észrevétlenül válik áldozattá az *adatvédelem*. Ki gondolkozik saját gyereke személyiségi jogain, amikor keble épp büszkeségtől dagad, miközben kiposztolja utódai fürdőruhában pancsoló, viháncoló képeit? Ez a szülői viselkedés írja le az ún. „*sharenting*” fogalmát. Mostanában kezd felnőni az a nemzedék, akinek tagjai tinédzserként azzal szembesülnek, hogy a közösségi háló tele van gyerekkori félpucér, vagy születésük pillanatát megörökítő, vérben úszó képeikkel és ők erre – a mostani fejükkel – lehet, hogy semmilyen felhatalmazást nem adnának szívesen. És akkor még nem beszéltünk a sokkal, sokkal kényelmetlenebb aspektusról, amikor beteges hajlamú idegenek töltik le és osztják meg sötétebb csatornákon ezeket a publikusan megosztott képeket gyerekeinkről…

fekete.balint @protonmail com

(Itt említenénk meg a hintalovon.hu oldalt, amely szülők számára készít gyermekeik online életével kapcsolatos tanácsokat, cikkeket. A fent említett „sharenting” témában is remek cikk érhető el oldalukon: link. Lazán kapcsolódik, de szintén hiánypótoló a yelon.hu chat-weboldal, ahol felkészült önkéntesek válaszolnak tiniknek gyakorlatilag bármilyen kérdésre – mindezt névtelenül.)

Újabb kellemetlenségre adhat okot a címkék („tag”-ek) alkalmazása, mikor ismerősök a csoportképeken megjelölnek, beazonosítanak minden rajta szereplő személyt. Ezzel tudtukon kívül a közösségi oldalak arcfelismerő neurális hálózatát tanítják – így egy random képen később már címkézés nélkül is felismeri az illetőt a rendszer.. Nem beszélve azokról az esetekről, amikor mondjuk egy politikai aktivista teljes ismerős-hálóját barátai önkéntesen – de tudtukon kívül – címkézéssel feltérképezik, tálcán nyújtva azt így át a hatóságoknak.

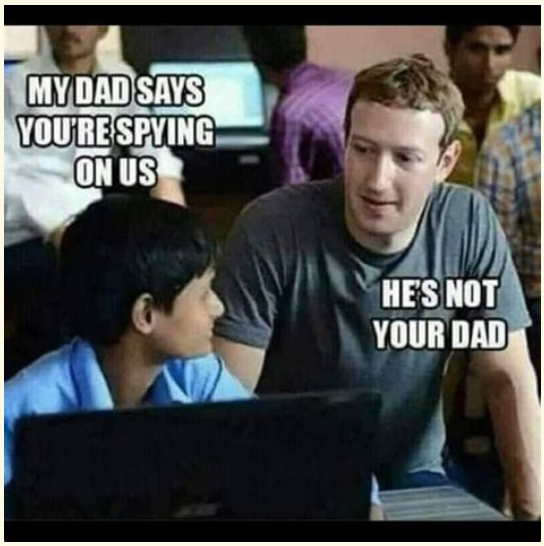
Adatkereskedelem

Az adat az új arany és mi “gombokért” adjuk oda, mint anno az amerikai őslakosok a gyarmatosítóknak kincseiket. Bele se gondolunk, de 1 hétnyi friss, nyers közösségi médiából kinyert adat, amely több millió (néha milliárd) személy tevékenységét tartalmazza, dollár tíz/százezrekbe kerül a hirdetési/kutatási piacon. Ilyen hatalmas adatmennyiséget hívunk “big data”-nak, amelyen ún. “adatbányászatot” folytatnak hirdető, kereskedelmi cégek, kormányügynökségek. Az adat hatalmas mennyisége és sokszínűsége miatt egészen hihetetlen összefüggéseket, statisztikákat képesek kinyerni belőle.

Vadnyugat

Az ember úgy érezheti, hogy ez az egész szabályozatlan és bizony jól érzi – ezért a “vadnyugat” hasonlat. A kormányok el nem végzett munkáját (szabályozás hiánya) magunknak kell megoldanunk – ez az iromány is ezért készült. Amíg nincs hatékony jogi környezet, ami védi személyes adatainkat, addig ez a személyek egyéni feladata marad – ehhez viszont ismeretek, oktatás és tudatosság kell.

A rólunk szóló információk adásvételét nyugodtan hívhatjuk információs “szervkereskedelemnek”. Evidencia, hogy amint a szerveid, úgy a rólad szóló információk is a te tulajdonod kéne hogy legyenek.



A szabályozatlan jogi környezetben vannak azért reménysugarak – a sokak által átkozott EU direktíva, a korábban már említett GDPR jó első lépés erre. Sok vállalkozás számára kényelmetlen, nyűg, mégis jó és hasznos alap, amire lehet építkezni.

Ne legyenek illúzióink: egy világcég jellemzően addig megy el, amíg a szabályozás engedi – tekinthetünk rá úgy, mint egy pszichopátiás viselkedéssel bíró személyre, aki az erkölcsöt legfeljebb mint kommunikációs eszközt ismeri. Szükséges a szigorú

szabályozás, a cégek maguktól nem fognak tiszteletben tartani semmilyen személyes adatot érintő szabadságjogot.

Jó – és végtelenül gátlástalan – példa az *Onavo Project*, ami egy fedőcégen keresztül valójában a Facebook által fejlesztett mobilalkalmazás. Az alkalmazás üzleti modellje: a felhasználó beleegyezésével, havi 20$-ért minden tevékenységet rögzít a felhasználó mobilján a legutolsó érintésig bezárólag. A célcsoport a tizenéves korosztály, mivel ők rengeteg tartalmat gyártanak, általában pénzszűkében vannak és legtöbbször nem is értik az adatvédelmi aggályokat – hiszen már ebben a "mindent posztolok" környezetben nőttek fel. Az alkalmazás által termelt rengeteg adat segít a Facebooknak a felhasználói szokások elképesztő mélységű megismerésével minél hatékonyabban célozni reklámozási technikáit, illetve addiktívabbá tenni termékeit (Facebook, Instagram, Whatsapp).

A nagy trió – Google, Facebook, Apple – profitorientált cégek és ahogy fent említettük, nincsenek etikai megfontolásaik, miközben már gyakorlatilag államszerű működéssel bírnak. Tevékenységük, például a moderálás, annak jellege és mértéke is önkényesen, általuk eldöntött formában zajlik – törvényi keretek, vagy előzetes társadalmi konszenzus nélkül. És míg egy kormányt általában le lehet váltani, egy nagyvállalatot nem.

Felmerült korábban és rendszeresen napirendre kerül, hogy közszolgáltatássá kéne tenni a Facebookot, így a bevételi kényszer megszűnése miatt nem lenne szükség a tartalomgyártás erőszakos hajszolására.

Nehéz ügy a fent említett moderálás témája is. Szükség van -e törvényi kereteket vonni a moderálásra, és ha igen, milyet? Nagyon könnyen a szólásszabadság feláldozásának kapujában találhatjuk magunkat, viszont az álhírek, trollok közben elpusztítanak mindent. Nehéz ügy.

A következő fejezetben a profilépítésről és annak felhasználásáról, valamint a metaadatokról lesz szó.

fekete.balint@protonmail.com

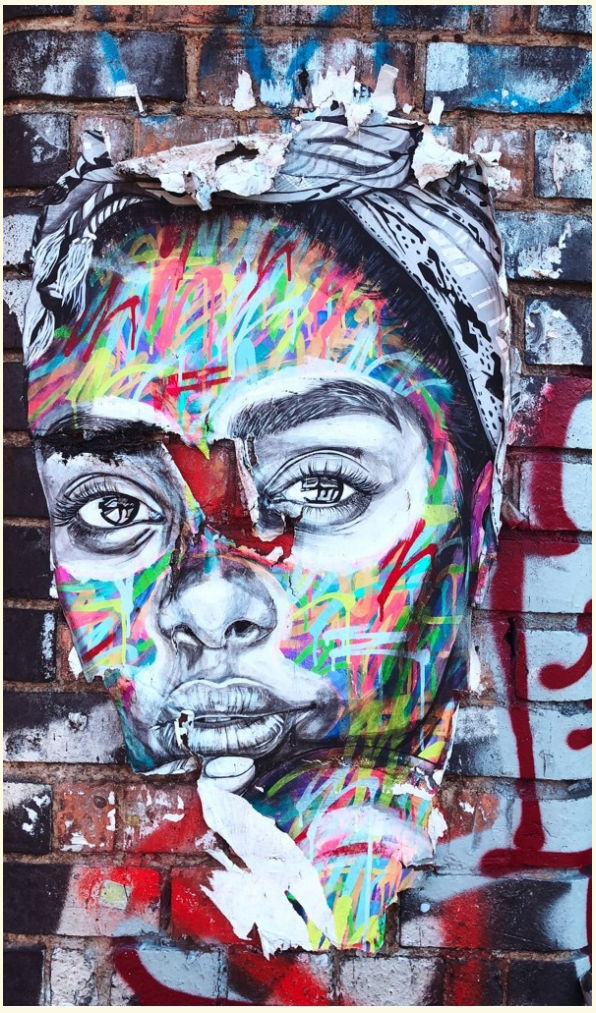
5. Profilépítés, metaadatok, kényelem

Az előző fejezetben a közösségi oldalak különböző trükkjeiről ejtettünk szót, amelyekkel tartalomgyártásra, megosztásokra vesznek rá bennünket, például a nárcizmusunk megpiszkálásával, vagy ismerőseink idillinek hazudott életpillanatainak felvillantásával.

Profilépítés

A fent említett adatok gyűjtése nem ész nélkül, hanem személyekhez rendelve történik. Képzeljünk el egy fiktív filmsorozat szereplőjét, akit mi alkotunk meg, akinek személyiséget, háttértörténetet adunk, fényképeket, videókat készítünk róla, majd elindítjuk a történetét, amely minden epizód eseményeivel árnyalja, mélyíti a karakter jellemét, lelki és fizikai tulajdonságainak megismerését. A harmadik évadra már ismerjük apró gesztusait, rezdüléseit, ismerettségi körét, szokásait.

Hát nagyjából így – fokozatosan – épít rólunk hasonló karakterprofilt a Facebook, a Google és a többi közösségi oldal. Az adatot ehhez pedig mi szolgáltatjuk – folyamatosan frissen tartva azt újabb megosztásainkkal, tartalomgyártásunkkal.



Megdöbbentő, de kutatások szerint a Facebook – amennyiben már legalább pár hónapja rendszeresen használjuk – jobban és mélyebben ismer bennünket, mint bármelyik rokonunk – beleértve a szüleinket is. Ismeri fizikai, lelki, mentális egészségi állapotunkat, politikai, világnézeti beállítottságunkat, szerelmi életünket, szexuális irányultságunkat, családi státuszunkat, baráti körünket, lelki egyensúlyunk mértékét, félelmeinket, hobbijainkat.

A profil összeállítását egyrészt a közösségi portálokon végzett tevékenységünk segíti, mint oldalak kedvelése, kommentelés (és annak gyakorisága), kommentek tartalma, sőt hogy hány másodpercig időzünk egy cikk felett míg – akár megnyitás nélkül – továbbgörgetünk a hírfolyamban. Másrészt gazdag profil információkat adnak megosztásaink (szöveg, fényképek, videók), ismerősök, helyszínek megjelölése, illetve csevegéseink tartalma, valamint... a nemrég kipattant sokadik botrányból kiderült, hogy esetenként hang- és videóhívásaink tartalma is: a gépi algoritmusok által generált hangról-szövegre készült leiratok egy részét emberi operátorok dolgozták fel, így pontosítva és javítva a gépi elemzést.. A kifogás, mint oly sokszor, itt is „felhasználói élmény” javítását hozza fel, mint megkérdőjelezhetetlen végső, nemes cél.

fekete.balint @protonmail com

Rendkívül kényelmes, de annál károsabb a "*Bejelentkezés Facebookkal”*, "*bejelentkezés Google azonosítóval*" funckiók használata internetes híroldalakon, online áruházakban, ételrendelő és egyéb szolgáltatásokat kínáló oldalakon. Ilyenkor még ezeket a különböző tevékenységeinket is bekötjük az említett közösségi cégek adatgyűjtő tevékenysége alá, így még komplexebb profil készülhet rólunk – akár már táplálkozási, hírfogyasztási, vásárlási, hobbi és egyéb szokásainkkal kiegészülve. Úgyanígy a Facebook „Piactér” használata is bőséges táptalaj egy kis „adatszüretre”.

Kereskedelem

A jól felépített profilokat lehet – a korábbi fejezetben már említett – célzott reklámokat vásárló cégek számára értékesíteni, vagy mint friss adatbázist egyszerűen eladni – ez utóbbi nem mindig legális, de talán emlékszünk 2016-ra: a Facebook a Cambridge Analytica elemzőcég számára adta el nagy mennyiségű, Egyesült Államokban élő felhasználó adatait, akik aztán azt az elnökválasztási kampányban felhasználták és a profiljuk alapján összeesküvésre hajlamos, könnyen befolyásolhatónak ítélt embereket célzott álhírekkel árasztották el hirdetés formájában, így jelentősen befolyásolva a választás kimenetelét. A Facebook rekord összegű büntetést fizetett, de a csontvázak szinte havonta potyognak azóta is, újabb és újabb botrányok rázzák meg a céget.

Jó példa erre a 2021. áprilisi brutális adatszivárgás, mikor 533 millió (!) felhasználó profilja és személyes adatai szivárogtak ki, bárki által megtekinthető formában (cikk).

Vagy vehetjük a szintén nagy port kavart 2021 elején kitört botrányt, mikor a Facebook az általa megvásárolt WhatsApp adatkezelési szabályait próbálta erőszakkal megváltoztatni (cikk).

A megvásárolt profil-adatbázisok egyik kellemetlen tulajdonsága, hogy néha elég jól össze is kapcsolhatóak. Például egy telekom cég adatbázisa híváslistákkal és a Facebook profil adatbázisa, amennyiben van közös „kapocs”, mint például a telefonszám, amit sokan olyan természetesen írnak be a Facebook adatlapjukra, mintha egy hivatalos okiratot töltenének ki. Még súlyosabb, mikor a Facebook mobilalkalmazás számára hozzáférést adunk a telefonkönyvünk összes kontaktjához. Ilyenkor jó, ha tudjuk, hogy a Facebook ismerősök nevei és a telefonkönyvben tárolt nevek összepárosításával azok telefonszámát is megszerezhetik, akik amúgy szándékosan nem adták azt meg profiljukban a közösségi oldalon..

De nem csak a közösségi oldalakat „etetjük” adatokkal, amelyek utána kereskedelmi forgalomba kerülnek – gondoljunk a DNS vizsgálatot végző családfakutató oldalak adatbázisaira, ahova önként adja be minden kíváncsi egyén a DNS mintáját, amit aztán magáncégek, vagy kormányzati szervek boldogan átvesznek.

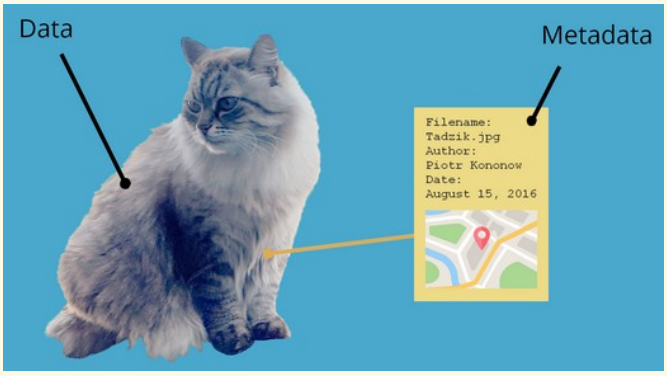
Az összekapcsolt adatbázisok egyik kellemetlen példája mikor diktatórikusabb államok civil aktivistákat tudnak vegzálni a róluk begyűjtött rendkívül részletes adatokkal, egészségi problémáik kihasználásával, célzott adóellenőrzések végzésével, rokonok, családtagok szürke ügyeinek felhasználásával.

Gondolati szabadság

Említettük az előző részben a cenzúrát és hogy a közösségi szolgáltatók egyéni döntése, milyen keretben használják. Kvázi önkéntes rendőrként tevékenykednek egy amúgy közös kommunikációs térben és ennek sokszor súlyos szociális következményei vannak: az öncenzúra kialakulása, mikor a szerző – feladva saját gondolati szabadságát – elküldés előtt átfogalmazza mondandóját, hogy az ne essen áldozatul a legtöbbször automatikus cenzúrának, ami nem érti a kontextust és iróniát – így pont szabad gondolkodását szorítja korlátok közé. A rebellis gondolatok születésük pillanatában karanténba záródnak, elhalnak, ez pedig megöli a progressziót, hisz ami új és forradalmi gondolat, az a múltban is sokszor a legalitás határán kívül esett.

Metaadatok

Sokszor előkerül a fogalom, de mik is ezek? A titkosított kommunikáció (erről lesz még szó) örvendetes előtörésével nem oldódott meg minden problémánk. Például nyomozó hatóságoknak sokszor nincs is szükségük a kommunikáció (pl. beszélgetés vagy csevegés) valós tartalmára, mert az ún. metaadatok kellő információt, kontextust nyújtanak. Lássunk pár példát:



Hagyományos telefonhívás metaadat: ki a hívó fél, ki a hívott fél, mi a hívás időpontja, mekkora a beszélgetés időtartama, hívások gyakorisága (napi/heti/havi). Ezeket az adatokat a telekommunikációs szolgáltató törvényben rögzített kötelessége minden előfizetőről 5 évig tárolni.

Csevegés metaadat: ki, mikor, kinek/kiknek, milyen gyakorisággal küldött üzenetet, mekkora adatmennyiséget forgalmazott. Kapcsolati hálóból személyek közelségére következtetés. Például a WhatsApp (Facebook tulajdona) már pár éve titkosítást használ, mégis gyűjt rólunk adatot – metaadatok formájában, ami megint csak személyes adatainkkal való durva visszaélés.

Internet szolgáltató metaadatai: az előfizető mikor milyen oldalt látogatott meg, milyen szerverhez / eszközhöz kapcsolódott, mennyi adatot forgalmazott, mennyi ideig.

Amerikában egyes metaadat-adatbázisok kereskedelmét 2017-ben monetizálták (!), megvehetőek bizonyos szolgáltatók (pl. netszolgáltatók) így begyűjtött adatai..

Kényelem és a Nagy Kérdés

Furcsa lezárása lesz a cikk elméleti részének, de ezen áll vagy bukik, hogy az olvasóban cselekvést is kivált -e amit megértett (remélhetőleg), vagy az első részben taglalt kognitív disszonancia redukció valamelyik technikájával meggyőzi magát, miért nem is olyan fontos ez. Ezért volt a hosszú felvezetés, a technikai háttéren kívül a társadalmi, közösségi – egyéni érdekeken átnyúló – szemlélet bemutatása is. Mert, ha hiszünk benne, hogy ez fontos, akkor... **talán képesek leszünk lemondani a kényelmünk egy kis részéről, hogy a személyes adatainkhoz, magánéletünkhöz való jogunkat érvényesítsük**.

És a cikk szerzőjének tapasztalata szerint EZ (a kényelem**)** – az, amihez egészen elképzelhetetlenül erősen ragaszkodunk. A kényelem minden más szempontot túllicitál. Az őskortól a jelenkorig vezető út során nagyjából folyamatosan emelkedett az átlagember kényelmi szintje… és nagyon úgy tűnik, visszafelé senki nem hajlandó tenni egy tappodtat sem. Aki élt a 80-as, 90-es években, visszatekintve, a mostanihoz képest sokkal „kényelmetlenebb” életet élt, de mivel még nem birtokoltuk a jelen luxusát, ezért mégsem volt zavaró.

A homályos célozgatásokat félretéve olyanokra gondolhatunk, mint hogy *átváltanánk -e egy olyan csevegőalkalmazásra a telefonunkon, ami titkosítottan kommunikál, nem gyűjt metaadatokat sem rólunk, viszont... mondjuk nincs benne „Online” állapotjelző.* Vagy váltanánk -e olyan levelezőre, amiben nincs benne minden kényelmi funkció, nincs összekapcsolva az azonos szolgáltató felhőtárhelyével, cserébe nem elemzi minden email tartalmát és azért elég jól össze van rakva? Banális kérdések, a válasz viszont döbbenetesen sokszor „nem”.

A váltás a megszokottról azért is tűnik nehéznek mert sokszor ismerőseinket is át kell állítanunk az új platformra és ez néha átmenetileg körülményes lehet, energiát/időt igényel, vagy félünk, hogy paranoidnak, bénának tűnhetünk, nem tudjuk elmagyarázni, hogy miért is kéne ez.

Viszont amennyiben a válasz „**igen**”, akkor a következő résztől kezdve megismerkedünk a gyakorlati megoldásokkal, amelyek nagyságrendi minőségi ugrást okoznak majd privacy terén és az átlagember számára is könnyen elvégezhetőek.. néha némi kényelemről lemondást vagy időt kérve cserébe – amely legtöbbször csak átmeneti kellemetlenség. Vágjunk hát bele.

6. Online csevegés

Eljött hát a pillanat: a hosszas alapozás után végre a gyakorlati megoldásokat mutatjuk be személyes adataink és magánéletünk védelme érdekében.

Rövid összegzésként: emlékezzünk, hogy a tudatos online jelenlét egy komplex világnézet alapját alkotja, amely nem a titkolózás, hanem az alapvető emberi jogok talaján áll. Egy cég, vagy kormány sem jogosult magánéletünk darabkáiból személyes profilt alkotni pénzszerzés, vagy kontroll gyakorlása céljából – akkor sem, ha az számunkra rövid távú előnyökkel kecsegtet. Emlékezzünk, hogy ezen alapelvek sértése nem kizárólag a saját életünket, hanem a miénknél rosszabb, kiszolgáltatottabb helyeken élő emberekét is erősen érinti. A rólunk szóló információ a mi tulajdonunk, továbbá nem fizetőeszköz. Mivel ezen alapjogaink eddig nem foglaltattak törvénybe, ezért egyelőre magunknak kell megvalósítani a szükséges kereteket.

Az előző fejezetben már említettük a cselekvés legnagyobb gátját: ez nem más, mint az ember személyes kényelmi igénye és annak maximális szinten tartása. „*A kényelem mindent más szempontot túllicitál*”.

Viszont ha a cikk előző fejezetei képesek voltak kellő hatást gyakorolni, akkor *talán* egy rövid, átmeneti időszakra képesek leszünk némi átmeneti kényelmetlenséget bevállalni, hogy tudatosabban mozogjunk az online világban.

Nem véletlenül kezdünk a csevegőprogramok tárgyalásával – az online térben talán ezek a legkedveltebbek az összes alkalmazás közül, a rövid üzenetküldés napjainkban szinte már kizárólag ezeken keresztül történik, az sms használata ma már közel anakronizmusnak számít.

Whatsapp, Instagram, Messenger, Viber, Skype, Snapchat

A sor még folytatható, de kétség kívül a fenti csevegőprogramok szállítják a legtöbb üzenetet a mindennapokban. Mindegyikük próbálja valami egyedivel megragadni a felhasználóit, meglepően apró nüanszok teszik kedvelhetővé őket (egyedi emojik, háttérkép). Privacy szempontból viszont komoly probléma van velük. Nézzük, mik a főbb szempontok, mikor egy csevegőprogramot próbálunk megítélni.

1. Végpontok közti titkosítás (E2EE)

Az első szempont, hogy az alkalmazás használ -e úgynevezett végpontok közti titkosítást (E2EE = End To End Encryption), ami meggátolja, hogy akár az alkalmazás üzemeltetője, akár más külső személy „belenézzen” üzeneteinkbe mikor elküldjük azt ismerősünknek és az interneten áthalad. A fenti technológia használatakor az üzenet tartalmát csak a feladó és a címzett láthatja – a kriptográfia elmélete igazi mélyvíz, ennek a cikknek a kereteibe semmiképp nem fér bele, legyen elég annyi, hogy két végpont (pl. mobiltelefon) között jelenlegi technológiával könnyen és számos módon megvalósítható törhetetlen titkosítással „becsomagolt” üzenetek küldése. Ez a technológia

az utóbbi évek botrányai után jelentős lökést kapott, „divatba jött”, még Mark Zuckerberg is ezzel reklámozta a megújult Messengert nemrég, illetve azzal mutatta be a Facebook újdonságait, hogy „The future is private”, ami valljuk be, elég mulatságos szlogen egy cégtől, ami személyes adataink felhasználásából él.

A végpontok közti titkosítás elve szerint a küldő és a címzett alkalmazása a háttérben legyártanak egyedi titkosító „kulcsokat”, amellyel lekódolják a küldendő üzeneteiket, majd azok megérkezéskor a címzett oldalon „visszaalakítják” őket, így ha bárki megpróbálná elolvasni őket miközben „áthaladnak” az interneten, csak zavaros katyvaszt, értelmetlen karaktersorozatokat láthatna. A kulcsok a két fél készülékein tárolódnak, így senki, még az alkalmazás szolgáltatója sem képes az üzenetekbe betekinteni. Ha valakit jobban érdekel a téma, akkor tudjuk ajánlani az alábbi Youtube videót, amely konyhanyelven, egy jól érthető, látványos hétköznapi példával (bár erősen leegyszerűsítve) bemutatja a titkosítás egy gyakran alkalmazott módját: „*How asymmetric (public key) encryption works*”.

Hogy a fenti technológia (E2EE) működőképes arra kellő bizonyíték az egyes kormányok által (USA, Ausztrália, Anglia, a sor hosszan folytatható) időről időre kezdeményezett törvénymódosítások erőltetése, amelyek betiltanák, vagy rejtett hátsó kaput (backdoor) építtetnének az alkalmazásokban használt titkosítási algoritmusokba. Az érvek rendszerint a nemzetbiztonságot emlegetik, pedig meglepően kevés bűnözőt kapnak el üzeneteinek tartalma alapján. Az Európai Unió például egy gyermekbántalmazás elleni törvénybe csomagolva próbálja a fentieket átnyomni.

Törvénytervezet: *Ref. Ares(2020)7284226 – 02/12/2020*

EU online vitaoldal a törvénytervezetről: link

További probléma a technológiában nem igazán jártas jogalkotók elképzeléseivel, hogy ha bármely biztonságos rendszerbe hátsó ajtót építenek, az többé már nem számít biztonságosnak – nem csak a kormányzat, hanem a bűnözőkkel, ellenséges államokkal szemben sem, akik szinte biztos, hogy megtalálják ezeket a gyenge pontokat és sebezhetőségként használva olyan adatokhoz juthatnak, amik aztán már tényleg nemzetbiztonsági kockázatot rejthetnek. Zárójelben: min fognak kommunikálni például a szenzitív adatokkal dolgozó állambiztonsági alkalmazottak, ha minden titkosítás kijátszható lesz..?

A címben említett csevegő alkalmazások közül a Messenger, Instagram, Viber és Snapchat titkosításban pocsékul teljesít. Előbbi kettő alapbeállítása szerint nem is használ ilyesmit (lásd később), a szolgáltató (Facebook) bizonyítottan „elolvassa” üzeneteinket – ennek fontos szerepe van személyes profilunk építésében, a Viber pedig ugyan alkalmaz valamilyen szintű titkosítást, de nem valós végpontok közti megoldást, mivel a titkosítás „kulcsait” a szolgáltató

szerverén tárolják, nem pedig a felhasználók mobilkészülékein – ahogy az elvárható lenne, így a tárolt üzenetek ismét csak visszafejthetőek a cég által. A Snapchat a küldött képeket titkosítja, semmi mást nem. A Whatsapp (már) modern titkosítást használ, de bőven van vele baj (lásd metaadatok fejezet), főleg mióta pár éve megvásárolta a Facebook..

Ha még vannak kétségeink, hogy miért baj, ha bárki belenézhet üzeneteink tartalmába, gondoljunk a hongkongi, iráni, iraki tüntetőkre, vagy Szaúd-Arábiában a rabszolgakörülmények közt tartott nőkre, akik közvetlen fizikai fenyegetettségnek vannak kitéve amennyiben az államnak/férjüknek nem tetsző üzeneteket küldenek, fogadnak.

A fenti probléma „finomabb", hétköznapibb formája a korábban már említett öncenzúra, mikor – tudván, hogy az alkalmazás elolvassa üzeneteinket – küldés előtt inkább átfogalmazzuk nyers, vagy esetlegesen félreérthető üzeneteinket. Ez a szólás- és személyes szabadság brutális (ön)korlátozása, ami lelkünk mélyén pusztít el valami nagyon fontosat, azt sugallva, hogy multinacionális vállalatok vagy államok „engedélyezett" szóhasználatának, „jóindulatának" vessük alá magunkat. Ahogy szóban, úgy írásban is azt mondunk, amit akarunk, annak tartalmi megítélése kizárólag a címzett fél joga.

2. Metaadatok gyűjtése

Az előző fejezetben már beszéltünk a metaadatok fogalmáról. Nos, az említett hat nagy csevegőalkalmazás mind szorgosan végzi a metaadatok gyűjtését és ezek alapján személyes profilt alkotnak rólunk, amelyeket nyomozó hatóságoknak, kereskedelmi partnereknek, nagy gazdasági erejű, de a demokráciát sajátosan értelmező államoknak időről időre kiadnak.

3. Megismerhetetlenség, permanent record, future secrecy

A *megismerhetetlenség* fogalmának megértéséhez dióhéjban felvázoljuk hogy jut el egy üzenet az egyik mobilkészülékről a másikra. Az üzenet a feladó készülékéről először a szolgáltató (pl. WhatsApp) saját kiszolgáló szerverére érkezik, ami aztán – mint egy postás – megpróbálja kézbesíteni azt, amennyiben a fogadó oldali készülék elérhető éppen. Ha nem, akkor várakozik, míg a címzett telefonja feljelentkezik az internetre és „lekéri" a szervertől új üzeneteit.

Egyes alkalmazások minden múltbéli üzenetről tárolnak másolatot kiszolgáló szerverükön, így ha újratelepítjük az alkalmazást mondjuk egy új telefonra, nem kell előtte mentést készítenünk korábbi csevegéseinkről, mert az új készülék rögtön lekéri azokat a kiszolgálótól. Ez komfortos, ugyanakkor privacy szempontból erősen aggályos. Az a bizonyos kényelem.. már megint bizony. A Facebook Messenger jellemzően így működik – bárhol beléphetünk – akár egy webes böngészőn keresztül is – az üzenetek ott lesznek.

A másik iskola mikor a kiszolgáló tényleg csak „postás", azaz miután továbbította az üzenetet a címzettnek, nem tárol belőle semmit, számára megszűnik. Ennek hátránya, hogy kézbesítés után az üzenetek csak a küldő és fogadó telefonján/tabletjén/számítógépén vannak meg – új telepítés előtt mentést kell készíteni. Előnye viszont, hogy a szolgáltató nem képes „beleolvasni" az üzenetekbe, de ami fontosabb, azt még bírósági végzés teljesítése esetén sem képes kiadni harmadik félnek – így a *megismerhetetlenség* elve érvényesül.

***Permanent Record*:** nem véletlen az angol kifejezés, eddig ugyanis nem fordították még le Edward Snowden, amerikai volt titkosszolga és etikus kiszivárogtató (whistleblower) új könyvének címét. A

névadás arra utal, hogy amit a közösségi médiában, csevegőüzeneteinkben, illetve más internetes platformokon írunk, az az esetek nagy részében véglegesen, kitörölhetetlenül megmarad, megőrzésre kerül – ha akarjuk, ha nem – és az bármikor a jövőben, mondjuk egy mainál kellemetlenebb rendszerben visszakereshető és bárki ellen felhasználható lehet. Az is, amit mondjuk tegnap, félig részegen küldtünk el egy személyes csevegő üzenetben egy barátunknak, vagy volt szerelmünknek – és aminek tartalma ma még nem bűn, de mondjuk 20 év múlva lehet, hogy már annak számít.

Mit jelent a megismerhetetlenség elve a csevegőalkalmazások esetében? A fent taglalt kézbesítés módját: az a szolgáltatás, ami csak „postás” – tehát nem őrzi meg az üzenetünket – biztosítja, hogy az üzenet tartalma nem csak most, hanem bármikor a jövőben is – akkor is, ha a ma használt titkosítás a jövőben törhetővé válna – a küldő és fogadó félen kívül más számára nem lesznek megismerhetőek. Ez az ún. „***future secrecy***” elve. Az a szolgáltatás viszont, amely megőriz egy példányt az üzenetből kiszolgáló számítógépén, – és így megőrzi azt „örökre” – nem biztosítja az üzenet megismerhetetlenségét. Fontos kiegészítés, hogy az a „jó postás”, amelyik nem csak az üzeneteket, de a metaadatokat sem tárolja (ki, kinek/kiknek, mikor, milyen gyakran írt).

Nem csak a csevegésben, de a közösségi médiában is felmerül a fenti a probléma. Gondoljunk a heti rendszerességgel beütő botrányokra mikor média vagy filmes személyiségek 10 évvel ezelőtti pillanatnyi hülyeségének előásása után (mint egy-egy vitatható bejegyzésük a Twitteren) az internetes tömegek háborgásától megijedve a stúdiók forró krumpliként dobják el az illetőt – sokszor véglegesen páriát csinálva belőle. Irtózatos büntetés ez, ráadásul nem a törvény, hanem random, interneten lincselő tömegek nyomásának eredménye. Képzeljük el, hogy mondjuk 10 év múlva olyan világnézet lesz a kizárólagosan elfogadott, amibe a ma leírt hülyéskedéseink, – amiket kiteszünk valamelyik profilunk alá – már nem férnek bele. És mivel ezek a bejegyzések „örökre” ott maradnak, bármikor előáshatóak. Hiába változtunk meg mi is közben, vagy értékeltünk át sok mindent, a „bűnjel” a múltból kitörölhetetlenül ott maradt.

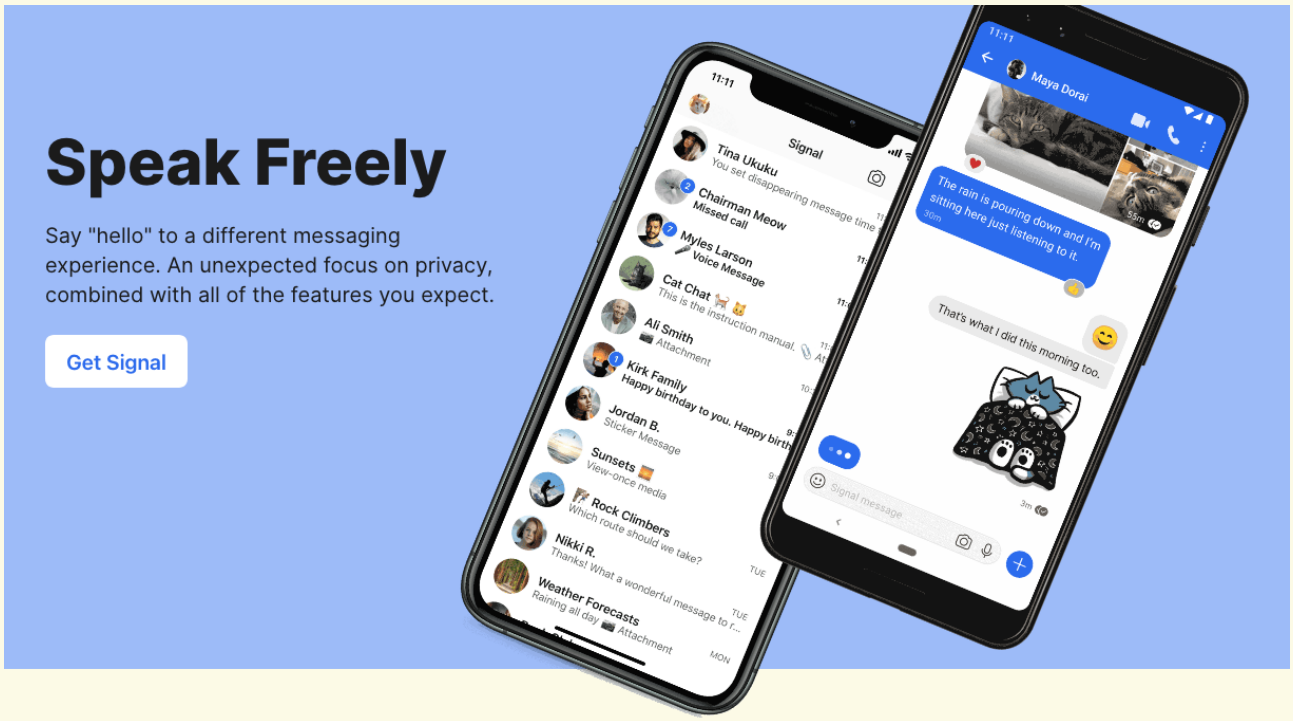
A fentiek társadalmi szempontból is aggasztóak, mert terepet adnak a kimondottan rosszindulatú embereknek, akik nem valamilyen valós erkölcsi sérelem miatt, hanem szórakozásból ássák elő ezeket a régi bejegyzéseket, amiken az utólagos törlés sem segít sokszor, mivel nem egyszer képernyőkép, vagy az archive.org alól előtúrt, weboldalak korábbi állapotát rögzítő mentéseket tárnak mindenki elé.

Nem jobb ennél egy személyes üzenet, ami alapból nem kerül ki sehova és elküldés után pár nappal, vagy héttel mindenhol megsemmisül?

4. Üzleti modell

Nem mindegy, hogy a csevegőalkalmazást fejlesztő cég milyen üzleti modell szerint működik. Amennyiben ez reklámok értékesítése, gyanakodhatunk, hogy valamilyen szintű adatgyűjtés készül kommunikációnkról – akár csak metaadatok szintjén –, profilt építenek rólunk, hogy a hirdetések megfelelően célzottak legyenek. Ha viszont egy nonprofit alapítványról van szó, annak nem áll érdekében magánéletünk részleteiben turkálni.

Alternatíva: Signal Private Messenger (signal.org)



Ahogy ígértük, konkrét javaslatokat, megoldásokat ajánlunk, legyen ez hát az első.

A ***Signal*** működésében a Whatsapp/Viber alkalmazásokra hasonlít, tehát a telefonunkban tárolt ismerőseink telefonszámai alapján építi fel kontaktlistáját, ami a kapcsolati háló alapja. Az utóbbi években jelentős felhasználói köre épült, egyre elterjedtebb, főleg az olyan jellegzetességei miatt, mint a nyílt forráskód, azaz a program működése részleteiben bárki által megismerhető, vagy hogy egyedi „cenzúra kikerülő funkciót” tartalmaz: azon kevésbé demokratikusabb országokban, ahol használatát államilag blokkolják, speciális technikai trükkökkel sokszor képes a tiltást megkerülni.

A Signal természetesen végpontok közti titkosítást (E2EE) alkalmaz az – egyénileg fejlesztett, de más cégek, alkalmazások által is adaptált – *Signal protokoll* segítségével. A szolgáltató nem gyűjt, nem tárol sem üzeneteket (csak a kézbesítés végéig), sem metaadatot a kommunikációról, ezen kívül fontos szempont, hogy nem is képes kiadni semmilyen információt külső félnek a felhasználókról – mivel vagy nincs mit, vagy ami van, az számukra is visszafejthetetlen, mivel a feloldó kulcsok a felhasználók készülékein pihennek.

Az üzenetek csak a küldő és a fogadó fél készülékein kerülnek tárolásra, sőt maga a kézbesítés folyamata is rejtett, a kiszolgáló úgy továbbítja az üzenetet, hogy nincs tisztában a feladó, de még a címzett személyével sem!

Google Play Store: Signal letöltése

App Store for iOS: Signal letöltése

A Signal használata szerencsére hasonlóan gördülékeny és felhasználóbarát, mint társaié, az alábbi kényelmi funkciókat nyújtja:

- Csevegés, csoportos csevegés, egyéni és ***csoportos hang/videóhívás***, valamint kép, videó, hangüzenet, GIF, sima- és animált matrica, emoji küldése/fogadása – természetesen mind titkosítottan, továbbá csoport admin funkciók.
- Eltűnő üzenetek funkció: bekapcsolása esetén 5 másodperctől 1 hétig állíthatjuk, hogy meddig éljen elküldött üzenetünk. Az idő lejárta után a saját és a fogadó készülékéről is törlődik az üzenet/kép/videó.
- Mobilra, tabletre (Android, iOS), asztali számítógépre/laptopra (Windows, Linux, Mac) is elérhető, egy azonosítóhoz több eszköz is csatolható. Letölthető a mobil alkalmazásboltokból, vagy a **signal.org** weboldalról.

A Signal fejlesztője eredetileg az Open Whisper Systems cég volt, de a fejlesztés 2019 körül egy nonprofit alapítvány – a Signal Foundation – keretében folytatódott azonos gárdával. Az alapítványi forma (501c3) biztosítja, hogy a céget és a fejlesztést ne lehessen felvásárolni. A Signal Foundation jelentős adományokat kapott az elmúlt években, így fejlesztése és jövője biztosított, az alkalmazás ingyenes, nem szorul rá az ellentmondásos személyes adatgyűjtési gyakorlatra és természetesen semmilyen reklámot nem tartalmaz.

Érdeklődőknek a Signal protokoll működéséről íme két „mélyvíz” jellegű cikk a készítőktől: link1, link2, de a Wired nevű internetes újság közérthetőbben mutatja be online cikkében: link, bár ez sem könnyű olvasmány.

Csevegőprogramok mentális függőségei

A **for-profit** cégek legfőbb célja, hogy a felhasználók minél többet használják a terméküket, a lehető legjobban addiktív legyen – hisz így az emberek több adatot „termelnek” magukról, a bőséges „szürethez”, pedig ez kell. Ennek eléréséért a beépített képességek és a felhasználói felület dizájn elemei is úgy vannak megtervezve, hogy mentális függőséget alakítsanak ki. Színes, tudat alatt táplálkozással összekapcsolható elemek is helyt kapnak, mint például a kis piros bogyók amelyek valamilyen újdonságra, értesítésre, új üzenetre utalnak. Ezek a kis, piros, bokrokon növő bogyókra hasonlítanak, amelyek leszedése fontos feladat volt még az ősidőkben. Rá akarunk nyomni, zavar, ha ott marad, de magunk se tudjuk, miért. De beszélhetünk a „*Stories*” vagy a „*Last online*” státuszjelzőkről, amelyek nemcsak az internetes zaklatás egy enyhébb, de kellemetlen formáját valósítják meg, de szorongáskeltő hatásuk is bizonyított. Egy másik példa: Indiában több, erőszakba torkolló tömeges felkelés volt a WhatsApp-on korlátlanul terjedő álhíreknek köszönhetően. A cég ezután külső nyomásra korlátozta a „Továbbítás” funkció egy időben kiválasztható maximális címzettjeinek számát.

Egy non-profit cég viszont megengedheti magának, hogy a felhasználható mentális egészségét szem előtt tartva etikus tervezéssel készítse el a felhasználói felületet és kihagyjon, vagy korlátozott formában vezessen be olyan funkciókat, amik bár kedveltek, de egyértelműen szorongáshoz, mentális zavarokhoz vezetnek. Szerencsére a Signal fejlesztése ezek szem előtt tartásával történik. Például egyszerre maximum 5 címzettnek tudunk egy üzenetet továbbítani.

Másik példa a csak olvasható csoportok, vagy más néven „*hírcsatornák*”, ahol a tulajdonoson kívül más nem képes bejegyzést közzétenni. A Telegram felületén például elérhető ez a funkció, de magas taglétszám esetén ez is alkalmas lehet tömeges manipulációra. Fontos eltérés, hogy az elérés sebessége sokkal nagyobb, mint a hagyományos közösségi médiás felületeké, hiszen „élőben” érkeznek az újabb és újabb üzenetek egyszerre akár több százezer embernek is. A Signal tudatosan hagyta ki ezt a lehetőséget eszköztárából.

Ezek a korlátok okozhatnak csalódottságot azoknál, akik megszokták a fenti funkciókat, de attól, hogy valami kedvelt, még lehet nagyon káros..

A Signal titkosítása

Ahogy korábban említettük a Signal – saját fejlesztésű, nemzetközi szakmai elismerésnek örvendő – végpontok közti titkosítását (*Signal protokoll*) beépítették más alkalmazásokba is, lassan kvázi iparági standard lesz. Bizony ezt a technológiát használja pár éve a WhatsApp is, sőt egy kellően kényelmetlenül eldugott beállítás aktiválásával az új Facebook Messengerben is bekapcsolható, de csak erősen korlátozott módon. A fentiek sajnos nem jelentik azt, hogy ezek az egyéb alkalmazások ne tudnának adatot gyűjteni a használóikról. Ugyan az üzenetekbe a titkosítás miatt alapesetben nem tudnak belenézni (a mentésekbe már igen), de a metadatok (kapcsolati háló, ki, kinek, mikor, milyen gyakran üzen) begyűjtését továbbra is hörcsög módjára űzik. A Signal a metaadatokat is titkosítja, így nem képes azok gyűjtésére.

Említettük, hogy a cég nem képes adatokat kiadni a felhasználóiról. Ennek éles „próbája” már meg is történt egy amerikai bírósági eljárásban pár éve, ahol a bíró kötelezte az akkor még „Open Whisper Systems” néven futó céget egy felhasználó adatainak átadására – ők ezt meg is tették: az összes információ, amit ki tudtak nyerni az általuk – a működéshez szükséges – minimális tárolt adatokból, az egy nagyon általános megállapítás volt: „Igen, ez az ember ezzel a telefonszámmal valóban használja a Signal alkalmazást”. Semmi mást.

A Signal (gyerekkori nevén TextSecure) akkor kapta az első nagy pozitív lökést, mikor Edward Snowden – a korábban említett híres amerikai kiszivárogtató – megjegyezte, hogy ő is ezzel kommunikál ismerőseivel, valamint az újságírókkal, akiknek a titkos kormányzati lehallgatásokról szóló bizonyítékait 2013-ban eljuttatta. További érdekesség, hogy 2016-ban mind a Demokrata-, mind a Republikánus párt kampánystábja annyira félt a lehallgatástól, hogy Signalt kezdtek használni belső kommunikációra – egyedül ezt az alkalmazást ítélték megbízhatónak. 2019 decemberében pedig a titkosítást nyíltan betiltani kívánó brit Konzervatív párt képviselői tértek át Whatsappról Signalra – ami talán nevezhető képmutatásnak annak fényében, hogy előtte mit szorgalmaztak az ország „védelme érdekében”.

Magyarországi publikus példa is akad: a *Telex.hu* fenntart egy telefonszámot, amire Signal üzenetet küldhet bárki, amennyiben érzékeny információkat akarna eljuttatni az újság számára (+36 70 640 0003).

Átszokás…?

„Na jó, de akkor most töröljem le a Whatsappot, ne máár…!?”

Nem, nem kell rögtön letörölni, a jó módszer itt is a lassú átszokás. Kezdjük el használni párhuzamosan a Signalt a többi alkalmazással, kérjük ismerőseinket, hogy inkább azon kommunikáljanak velünk, aztán... ha elértünk egy kritikus tömeget és képesek vagyunk elszakadni a régi platformoktól, akkor törölhetjük magunkat egy-egy, vagy több régi alkalmazásból is. Ilyenkor tudassuk ismerőseinkkel, hogy ha továbbra is el akarnak érni, akkor ezt az alkalmazást telepítsék – ez működni szokott. A WhatsApp „Stories” funkciójába kitett közlemény az átállásról, vagy a Signal csoportmeghívó link funkciója nagyban megkönnyítheti ezt.

Nehéz pár szóban megválaszolni az ilyenkor sablonszerűen jövő megszokott kérdéseket („*Minek váltsak? Nem vagyok paranoid, nincs titkom, nincs mit titkolnom*” – lásd az első fejezetet) – ilyenkor segíthet pár kulcsmondatot akár ebből a cikkből is. Ez az az említett ideiglenes kellemetlenség, amivel meg kell küzdenünk – a saját kényelmünk és megszokásunk után másokéval is szembesülhetünk. De ne adjuk fel, mert fontos az ügy, a kellemetlenség pedig nem tart soká.

Pikáns adalékként érkezett 2021 januárjában a WhatsApp alkalmazásban felugró jogi beleegyezést sürgető értesítés, mely ahhoz kér engedélyt, hogy a felhasználó egyezzen bele minden WhatsAppból származó személyes adatának átadásába a Facebook számára – akkor is, ha nincs Facebook azonosítója (ilyenkor egy "árnyék profil" készül róla). Ha nem fogadja el, pár héten belül törlik a regisztrációját.

A felháborodás meglepően elsöprő volt, tömegek kezdek alternatívát keresni. A Facebook lépése a saját szempontjából érthető volt, elérkezettnek láthatta az időt, hogy a WhatsApp 2014-es bekebelezésére kiadott pénzt (**19 milliárd** dollár) valahogy elkezdje visszahozni. Ez pedig a

felhasználói adatok „leszüreteléét” és a profil alapú célzott reklámok WhatsAppba való beillesztését jelenti.

A Signal felhasználói bázisa pár nap alatt növekedett a többszörösére (valahol 50 és 100 millió között járt 2021. január végén). Úgy tűnik lassan kezd megjelenni az átlagemberek gondolkodásában is a tudatosság és kezd gyökeret verni az eddig elhesegetett privacy fontossága.

Mitől véd és mitől nem?

A továbbított adatok (*Data-in-Transit*) és a tárolt adatok (*Data-at-Rest*) védelme két külön dolog.

A Signal csevegőprogram *Data-in-Transit* szinten nyújt védelmet a végpontok közti titkosítás (E2EE) segítségével. Ez azt jelenti, hogy a védelem onnan kezdve él, hogy üzenetünk elhagyja a telefonunk és ott ért véget mikor megérkezik a címzetthez. Menet közben, míg áthalad az internet sok-sok szerverén és netszolgáltatóján, addig a jelenleg törhetetlen titkosítása miatt nem lehetséges belenézni, sem metaadatot gyűjteni belőle (ki küldte kinek, stb).

Viszont a telefonunkon levő üzenet-adatbázis (*Data-at-Rest*) ugyan titkosítva van, de a nyitó kulcsa is magán a fizikai telefonon van (hiszen valahogy vissza kell fejteni hogy lássuk). A jobb telefonok háttértára – amin minden program, adat és adatbázis van – titkosított (ilyen minden iPhone) és csak a jelkódunk, arcképünk, vagy ujjlenyomatunk oldja fel. Így tehát csak akkor tudnak hozzáférni az adatokhoz, ha fizikailag megszerzik a telefont ÉS feloldják (tudják a jelkódot, vagy rányomják erőszakkal az ujjlenyomatunk). Az Androidos telefonok közül még nem mindegyik háttértára titkosított – ezeknél ha megszerzik fizikailag a telefont, akkor elvileg hozzá lehet férni megfelelő kütyükkel.

Tehát: használjunk E2EE üzenetküldőt ÉS vigyázzunk fizikailag telefonunkra, mert a fizikai hozzáféréstől a cevegőprogram nem véd – nem is arra lett kitalálva. Viszont a paranoia nem indokolt: egy átlagember telefonját nem fogják ellopás után adatokért hekkelni, ez iszonyú idő és energia, továbbá szakértelemet is igényel, meg minek ugye... Inkább törlik és eladják a Blaha aluljáróban..

fekete.balint @protonmail com

Gyakorlati tanácsok Signal használatához

Asztali kliens

Nem kell kizárólag mobilunkra szorítkozzunk, a Signal elérhető minden asztali platformra is (Windows, Linux, Mac), amelyek letölthetőek innen: https://signal.org

Letöltés után az asztali klienst párosítanunk kell mobilunkkal. Ennek menete:

1. Telepítsük a letöltött állományt laptopunkra, vagy asztali számítógépünkre, majd nyissuk meg a Signalt. Első indulásnál felugrik egy QR kód.

2. Telefonunkon a Signal beállításokban a "Társított eszközök" alá lépjünk be, majd válasszuk az "Új készülék társítása" menüpontot.

3. Olvassuk be telefonunk megnyíló kamerájával a monitoron látható QR kódot

4. Pár perc míg a két kliens szinkronizál. Ezek után kontaktlistánk és csoportjaink átkerülnek az asztali kliens alá. Fontos, hogy maguka az üzenetek kerülnek szinkronizálásra – ez szándékos, lásd „future privacy” elve.

Csoport csevegéssel kapcsolatos tudnivalók

- Csoportot létrehozni (egyelőre) csak mobilon lehet, de ezt követően már az asztali kliensen is lehet bennük irogatni.
- Kontakt személy vagy csoport beállítások: a beszélgetésen belül (mobilon) felül rányomunk a kontakt vagy csoport nevére, ott számos egyedi beállítást találunk, amit az adott személyre/csoportre szabhatunk mint a némítás, eltűnő üzenetek, egyedi csengőhang, stb.
- Csoportban működik a más csevegőkből is ismert *@említés* funkció.
- A csoport létrehozója lesz alaphelyzetben a csoport admin, de mást is felruházhat ezzel a szerepkörrel. A csoport beállításokban megadhatjuk, hogy bármely tag vagy csak adminok változtathassák a csoport jellemzőket (háttérkép, cím, stb), illetve adhassanak hozzá új tagot a csoporthoz.
- Csoport tagok kezelése: nyissuk meg a csoportot, majd az adott tag avatárjára nyomjunk, ekkor feljön egy menü, ahol admin jogot adhatunk/elvehetünk, vagy eltávolíthatjuk az adott tagot a csoportból és még pár apró műveletet végezhetünk.
- ***Emberek meghívása a csoportba***: ha nem akarjuk egyenként hozzáadogatni ismerőseinket egy új, vagy már meglevő csoporthoz, vagy még nem regisztrált embereket csábítanánk át Signalra, akkor küldhetünk csoporthivatkozást, ami gyakorlatilag egy internetes link (URL). Erre rányomva ismerőseink egy csatlakozási kérést küldenek a csoport admin számára, aki ezt jóváhagyhatja, vagy elutasíthatja. Ezt az admin jóváhagyás funkciót ki is lehet kapcsolni, ilyenkor az új tagok automatikusan tagságot nyernek – ezzel csak óvatosan. Az alábbi twitter bejegyzés pár képen bemutatja, a fenti lépéseket: link

Signal hívás

- Csoporthívást a csoport jobb felső sarkában lévő kamera ikonnal lehet indítani, amely az „előtérbe” (lobby) visz, ahol a kamerát, hangot ki/bekapcsolhatjuk, megviselt ábrázatunkon igazíthatunk, majd beléphetünk a hívásba. A csoporthívás "meeting" jellegű, tehát nem fog kicsörögni senkinél, mindössze megjelenik a csoport csevegésben egy zöld ikon, amely jelzi, hogy valaki a tagok közül hívást indított és lehet csatlakozni. Egy időben maximum 8 fő tud a csoporthívásban részt venni.
- Az 1:1 telefon/videóhívás viszont már kicsörög, olyan, mint egy sima telefonhívás és mobilunk híváselőzményeiben is megtalálható lesz (ha ezt engedélyeztük).
- A csevegés beszélgetés közben is elérhető. Mobilon a „vissza” nyíl használatával (bal fent), asztali kliens esetén a jobb felső sarokban találjuk a „kicsinyítő” ikont.

Vegyes tanácsok

- Eltűnő üzenetek: egy adott beszélgetésre a korábban már említett kontakt/csoport beállításokban lehet beállítani, konkrét üzenet lejárati idő megadásával. Használatakor a küldő és fogadó összes készülékéről eltűnnek a beállítás után küldött üzenetek a megadott idő leteltével.
- Képet, annak csatolásakor lehetséges „egyszer megtekinthető” módon küldeni: a "végtelen" jelre nyomjunk a kép alsó részénél, ami így átvált „1x” módra.
- Mobilunkon a főmenüben beszélgetéseken jobbra-balra húzva ujjunkat sok extra funkció érhető el, mint az *olvasatlannak jelölés*, *kitűzés*, *archiválás*, vagy a *törlés*.

fekete.balint @protonmail com

7. Internetes védelmünk felépítése

Végre elérkezett a cselekvés pillanata, a sok elmélet után a gyakorlati megoldások felé vesszük az irányt. Mit tehetünk, hogy a sokat emlegetett, egyelőre szabályokba nem foglalt alapjogunkat adataink birtoklásához és kommunikációnk személyes jellegének megőrzéséhez megfelelően gyakorolhassuk? Praktikus használatra először egy tömör táblázatban összefoglaljuk a lényeget, majd utána ennek kifejtése következik.

Böngésző: Firefox + Firefox Multi-Account Containers + Facebook Container + DuckDuckGo Privacy Essentials + uBlock Origin + Privacy Badger + ClearURLs + Decentraleyes + Cookie Autodelete

Videókonferencia: Jitsi Meet, Signal Private Messenger

Facebook adatvédelem: link és link, FB alkalmazásokat, videó/hanghívást ne használjunk

Google adatvédelem: link

Email: Protonmail

VPN: ProtonVPN

Keresők: duckduckgo.com, ecosia.org, Brave search

Online jegyzetelés: Standard Notes

Cloud tárhely: sync.com, valamint 2021-ben várható a ProtonDrive bevezetése

Fájl tárolás titkosított konténerben: Cryptomator

Rövid jegyzet küldése: Privnote

Fizikai védelem: kamerákat, laptop mikrofont takarjuk le

Internetes böngészés

A csevegés mellett az internetes böngészés ez egyik leggyakoribb online tevékenység. Sajnos ha simán elindítunk egy böngészőt, akkor „ernyő nélkül megyünk az esőbe”, a látogatott oldalak adatgyűjtés, követés és profilépítés alapjaira épülő modelljei ellen védtelenek leszünk. Szerencsére pár egyszerű trükkel egész radikálisan lecsökkenthetjük a rólunk „lenyúzható” információk mennyiségét.

Korábbi fejezetekben szó volt róla, hogy ha egy böngészőlapon megnyitunk egy weboldalt, esetleg bejelentkezünk egy szolgáltatásba, azzal nem csak azon a lapon, hanem az „egész” böngészőben be leszünk jelentkezve. A lapok – korlátozottan ugyan – de „átláthatnak” más lapokra. A tartalmukat nem tudják kiolvasni, tehát ne féljünk, hogy netbankos belépésünket megszerzik, ennél kevésbé durva a helyzet, de igen kellemetlen információgyűjtésre képesek.

A legtöbb cég, szervezet, híroldal önként építi be külső szolgáltatók, közösségi média elemeit weboldalába. Ilyenek például a Google Analytics láthatatlan komponensei, amelyek a

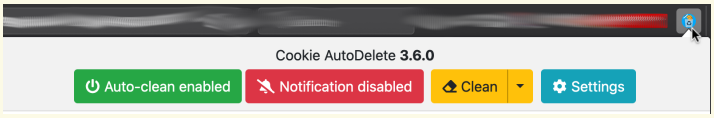
látogatásszámot és felhasználói viselkedést mérik (melyik oldalról érkezett, honnan hova kattintott, mennyi időt töltött az oldalon, melyik másik oldalról kattintott át ide, stb). De ilyenek a Facebook „Like” gombai is például egy híroldal cikkjeinek alján. A híroldal üzemeltetője így nagyobb elérést nyerhet és ha akarja még Facebook komment szekciót is könnyen applikálhat a cikk alá. Cserébe viszont ha be vagyunk jelentkezve a Facebookba az – a like gombon keresztül – begyűjti személyes profilunk alá az eseményt, hogy az adott oldalon látogatást tettünk. Akkor is, ha nem nyomtunk rá a gombra egyáltalán… elég, hogy az oldallal együtt betöltődött.

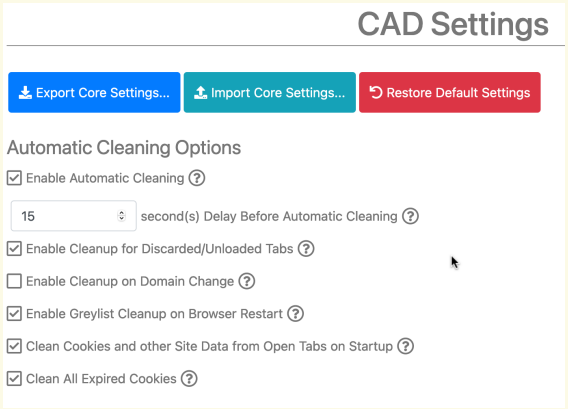
Böngésző felvértezése

Először is: milyen böngészőt használjunk? Jó szívvel jelenleg csak a Mozilla Firefoxot tudjuk ajánlani, amely az utóbbi években hangsúlyosan ráfeküdt a privacy támogatására. Az alap verzió is ad bizonyos fokú követés elleni védelmet, de remek kiegészítők telepíthetőek alá, amik sokszorosára növehetik képességeit. Ezeket a ***kiegészítőket*** (Firefox addons) ajánljuk telepíteni, a nevek alább mind kattinthatóak, a telepítő oldalra visznek, ahol csak a „Telepítés” gombra kell nyomni és a felugró engedélyezési kérdést elfogadnunk. Értelemszerűen csak Firefox böngészővel működnek. Gyorsbillenytűk: CTRL+SHIFT+A (Windows), CMD+SHIFT+A (Mac).

- Firefox Multi-Account Containers: A Mozilla által fejlesztett – tehát hivatalos – kiegészítő, jó kérdés, miért nincs alapból telepítve – valószínűleg az egyszerűség megtartása miatt. Definiálhatunk egyedi ***konténer típusokat*** például ***Bankolás***, ***Vásárlás***, ***Google***, stb. – a felosztás logikája teljesen ránk van bízva, a nevek csak tetszőleges elnevezések, tehát nem „kötelező” a ***Bankolás*** alatt megnyitni a webbank oldalakat. Az elv: használatukkal a különböző konténer-típusú füleken megnyitott oldalak nem „látnak rá” egymásra egyáltalán, csak konténeren belül. Tehát ha mondjuk egy „Google” típusú konténerfülön megnyitjuk a Gmailt és bejelentkezünk, utána pedig mondjuk egy ***Zene*** típusú konténerfület indítunk és megnyitjuk a Gmailt, akkor úgy látszik majd, hogy ott egyáltalán nem is vagyunk bejelentkezve. Ennek előnye, hogy ha így „karanténba” vonjuk például a Google alapú weboldalakat (Gmail, Youtube, Google Maps, stb), akkor a Google nem lesz képes a mi azonosítónkhoz rendelt adatot gyűjteni más konténerben megnyitott oldalakról.
    - Oktatóvideók a fentiekről, példákkal: link1 és link2 (angol nyelven)
- Facebook Container: az előző kiegészítő telepítése ennek előfeltétele. Ez az okosság specifikusan a Facebook ökoszisztéma karanténba helyezésére lett kitalálva. Automatikusan létrehoz egy ***Facebook*** nevű konténer típust és minden Facebook által birtokolt oldalt (Facebook, Instagram) automatikusan ilyen típusú fülön nyit meg. A Facebook nem lesz képes kilátni belőle. További képessége, hogy automatikusan blokkol minden más weboldalon minden Facebook gombot és láthatatlan 1x1 pixeles „követő” kép betöltést, amiket a közösségi oldal használ más oldalakba ágyazva.
- DuckDuckGo Privacy Essentials: a méltán elismert duckduckgo.com keresőoldal szakemberei által készített követés elleni kiegészítő. Az oldalak megnyitásakor automatikusan letiltja a tracker-eket és egyéb követést megvalósító elemeket.
- uBlock Origin: reklámblokkoló
- Privacy Badger: Szintén tracker és reklámblokkoló

- ClearURLs: mikor elképesztően hosszú URL-eket látunk, olyankor a „?” karakter utáni rész legtöbbször követési információt tartalmaz: melyik oldalról érkeztünk, stb. A Facebook a **?fbclid=** rész után tesz egy kódolt, számára hasznos követési karaktersorozatot. Ez a kiegészítő megtisztítja linkjeinket ezektől a parazitáktól.
- Decentraleyes: bonyolult követési technikákat hatástalanító kiegészítő
- Cookie Autodelete: haladó szint! A böngészés során a weboldalak által gépünkre letárolt sütiket törölhetjük velük az oldalak bezárása után automatikusan. Hozzáadhatunk kivételeket a „**whitelist**”-hez, ezek az oldalak mentesülnek a cookie törlés alól. Ajánlott beállítás: az oldal bezárása után 15 másodperccel törlődik minden hozzá kapcsolódó cookie. Nyomjunk a kiegészítő ikonjára, majd a „Settings” gombra és állítsuk be a lentieknek megfelelően.
  Fontos: ha egy oldalt nem tettünk whitelist-re és törlődnek a hozzá köthető sütik, akkor az az oldalra való bejelentkezéseinket is törli!





Követésblokkolás

A Firefox az 2020-as év során beépítette a böngésző alapváltozatába a követésblokkolás képességét. Ennek erősségét magunk is szabályozhatjuk a lenti menüben:

`Eszközök menü → Beállítások → Adatvédelem&Biztonság → Követésblokkolás`

Ajánlás: válassszuk a „*Szigorú*” (Strict) lehetőséget az opciók közül..

Böngészési adatok törlése

Időnként nagyon érdemes elvégezni, a fenti védelmek ellenére is. A látogatott oldalak által gépünkön tárolt ideiglenes állományait tisztíthatjuk el a lenti módon. Firefoxban a felső menüsort az "Alt" gombbal tudjuk megjeleníteni.

```
Eszközök menü → Beállítások → Adatvédelem&Biztonság
        → Előzmények → Előzmények törlése
```

"Time range": "Everything". Minden négyzetet kattintsunk be, majd "Clear Now" gomb. Megjegyzés: ez minden oldalról kijelentkeztet minket.

Ajánlás: mielőtt belevágunk a taglalt kiegészítők használatába végezzünk el egy fent említett teljes, böngészési adatokat érintő törlést, hogy „tiszta lappal” tudjuk megkezdeni új netes életünket.

Böngészési előzmények

A fenti menüben található szintén a böngészési előzmények megőrzését szabályozó két opció is. „*Böngészési és letöltési előzmények megőrzése*”, illetve „*Keresési és űrlap előzmények megőrzése*”. Ha nincs szükségünk rájuk, kapcsoljuk ki, különben csak felesleges „naplóként” szolgálnak minden meglátogatott oldalunkról. Elérésük szintén itt található:

```
Eszközök menü → Beállítások → Adatvédelem&Biztonság → Előzmények
```

Videókonferencia alkalmazások

Ugyan elképesztő mértékben elterjedt, a mára mindenki által ismert **Zoom** számos aggályt vet fel nem csak privacy, de etikai téren is. Gondoljunk csak az azóta eltávolított facebookos beépülő adatgyűjtő komponensre, vagy a szemmozgást figyelő funkcióra, amivel a menedzserek az elkalandozó figyelmű kollégákat szúrhatják ki.

Ha személyes célokra használnánk csoportos videóhívást, ahol munkahelyünk nem írja elő a használt szoftvert, válasszunk etikus megoldást.

Jitsi Meet

Böngészőben futó, nyílt forráskódú, ingyenes alkalmazás, sőt bárki telepíthet saját Jitsi szervert, akár maga, akár egy szervezet számára. Ugyanakkor a fejlesztők gondoltak az átlagemberre is és üzemeltetnek egy mindenki által elérhető publikus példányt saját szoftverükből.

A Jitsi alapesetben böngészőben fut, de mobilra elérhető külön alkalmazás is („Jitsi Meet” néven). A szoba létrehozása tetszőleges – nem foglalt – néven történhet, utána a linket megoszthatjuk ismerőseinkkel például egy csevegőprogram segítségével. Ajánlott jelszót is beállítani a belépéshez, hogy elkerüljük a kéretlen trollok véletlenszerű felbukkanását, akik jó eséllyel testük olyan részeit tárják fel előttünk, amire minden bizonnyal kevéssé vagyunk kíváncsiak. A publikusan üzemeltetett Jitsi Meet itt érhető el:

https://meet.jit.si

Signal Private Messenger

2020 ősze óta már a Signal is képes csoportos videóhívásra. Ehhez egy csevegőcsoportot kell létrehozni, vagy egy meglevőt használni. A csoporthívás inkább egy meeting indításhoz hasonlít: nem csöng ki egyik csoporttagnál sem, mindössze egy értesítő jelenik meg, hogy egy tag csoporthívást kezdett és aki akar, csatlakozhat. 2021 elején egyelőre 8 fő a felső limit egy hívásban.

A hívásba asztali és mobil kliensről is becsatlakozhatunk – sőt lehetséges mindegyikről külön-külön is egy időben, ha valaki egyszerre több szögből szeretné megvillantani arcélét.

Facebook adatgyűjtés szabályozása

Nem csupa szívjóságból, hanem leginkább az európai szabályozások miatt (helló GDPR!) a nagy tech cégek is rákényszerültek, hogy a felhasználónak nagyobb kontrollja legyen saját adatai felett. Így 2020 vége óta a Facebook felületén is megnézhetjük, illetve ki is kapcsolhatjuk a tevékenységeink követését az alábbi linken:

https://www.facebook.com/off_facebook_activity/

Az "*Események leválasztása*" opcióval lehet törölni az eddig begyűjtött adatokat, illetve jobb oldalt található a "*A jövőbeni tevékenységek kezelése*" opció, ahol ki is lehet kapcsolni ezt a fajta adatgyűjtést. Persze kapunk ijesztgető figyelmeztetést, hogy nem kapunk majd célzott reklámokat, de ezzel a „borzalmas" körülménnyel talán tudunk együtt élni..

Facebook adatvédelmi beállítások

Nyissuk meg az alábbi oldalt és a bal oldalon látható összes menüponton haladjunk végig. Egyszer kell csak megcsinálni, szánjuk rá azt a 10 percet és tiltsunk vagy szigorítsunk mindent, amire nincs feltétlenül szükségünk. Az ijesztgető megjegyzéseket nyugodtan figyelmen kívül hagyhatjuk, a Facebook nyilván nem szeretné ha letiltanánk, mert így kevesebb személyes adatunkat tudja majd begyűjteni a jövőben.

https://www.facebook.com/settings

Facebook alkalmazások

A Facebookon belül futtatott minialkalmazások (mint a szépemlékű Farmville és társai) valóságos rémálomnak számítanak – személyes adatok védelmének szempontjából. Talán emlékszünk a „*Hogy nézek ki 10 év múlva*" alkalmazásra, amit boldog-boldogtalan osztogatott, gyorsan rányomtunk a beleegyező nyilatkozatra és jót nevettünk a generált képen. Közben az alkalmazás fejlesztője begyűjtötte minden személyes adatunkat, kapcsolati hálónkat és ami elérhető volt a profilunkból, plusz az önként átadott biometrikus azonosítónkat: az arcképünket. És ehhez mi adtuk a hozzájárulásunkat, mikor elfogadtunk a nyilatkozatot. Szóval röviden: hanyagoljuk a Facebook alkalmazásokat.

Facebook mint hang és videóhívás platform

A Facebook nem számít megbízható hang/videóhívás platformnak sem, főleg mióta kiderült, hogy beszélgetéseink tetszőleges részéből leiratot készítenek – hangfelismerő algoritmusuk „okosításának" céljából (forrás).

Facebook csevegés és üzenőfal

Jó, ha eszünkbe véssük: a Facebook nem egy privát csevegőszoba, ahol csak ismerősökkel társalgunk. Az egyéni és csoportos csevegéseink is elolvasásra kerülnek automatikus algoritmusok által. Mikor kiírunk valamit a falunkra, vagy üzenetet küldünk valakinek, gondoljuk át: ez olyan üzenet, amit egy zsúfolt, nyílt utcán átüvöltenénk a túlsó járdán álló ismerősünknek. Ha igen, akkor hajrá.

Facebook és telefonszámunk

A Facebook nem egy hivatali szerv, nem kell kötelezően „kitölteni” adatlapunkat. Az egyik legkárosabb (nem csak magunkra, hanem ismerőseinkre is ható) tett, amit tehetünk, az telefonszámunk megadása. Ez egy nagyon erős, egyedi azonosító, ami kiválóan alkalmas adatbázisok összekapcsolására – akár Facebookon kívüli nyilvántartásokkal is. Ha a főbűnt is elkövetjük, azaz készülékünk telefonkönyvéhez, tehát személyes kontaktlistánkhoz is hozzáférést adunk, akkor olyan ismerőseink számához is hozzájut a közösségi oldal, akik amúgy nem adták azt meg, vagy nem is regisztráltak – sőt, az ismerősök ismerősei és érintettek lesznek. A telefonszámok használatával „kiváló”, Facebookot nem is használó személyeket is tartalmazó kapcsolati háló rajzolható ilyen adatokból. Röviden: ne adjuk meg a telefonszámunkat és főleg ne adjunk hozzáférést személyes telefonkönyvünkhöz.

Facebook profilszennyezés

Mivel a Facebook az aktivitásunkból alkot képet a személyiségünkről, érdeklődési körünkről, ha hamis adattal „etetjük”, akkor a rólunk alkotott profil is használhatatlan lesz. Ezt legegyszerűbben úgy tudjuk megtenni, ha olyan oldalakat, posztokat kedvelünk, amelyek a valóságban igen távol állnak érdeklődési körünktől. Ha például minden magyarországi politikai pártot bejelölünk, vagy hirtelen lelkesen „érdeklődni” kezdünk a horgolás iránt, akkor ezzel összezavarhatjuk a profilalkotó algoritmust.

További jó tanács, hogy minden Facebook által feldobott "ajánlott oldal" esetén nyomjunk "elrejtést" az adott posztra. Ha rákérdez ennek okára, egyszerűen az X-re nyomva zárjuk be az felugró ablakot – válasz nélkül.

Ha érdekel egy ajánlott oldal, akkor se a linkre kattintsunk, hanem nyissuk meg külön ablakban manuálisan az ajánlott weboldalt és annak nyitóoldaláról érjük el a tartalmat. Így nem szolgálunk kattintási statisztikával sem.

A személyes adatainkat (telefonszám, cím, születésnap) sem ajánlott megadni, mert ez kiváló egyedi azonosításra ad lehetőséget. Például sok Kovács István van az országban, de egy pontos születési dátum erősen leszűkíti az egyének számát.

Google adatgyűjtés szabályozása – általános

Az előzőekhez hasonlóan Google azonosítónk jogosultságait is tudjuk korlátozni. Nyissuk meg az alábbi oldalakat és itt is haladjunk végig a bal oldali menükön. Szigorítsunk, tiltsunk.

https://myaccount.google.com

https://myactivity.google.com

Google adatgyűjtés szabályozása – Gmail

A Gmail ugye a felhasználói feltételekben kiköti, hogy a szolgáltatásért cserébe elolvassa minden levelünket és abból profilt építve célzott reklámokat jelenít meg számunkra. Ha ez nem tetszik (még szép), akkor szintén 2020 végén jelent meg ennek az elemző funkciónak a kikapcsolási lehetősége. Egyetlen hátránya, hogy a levelek „szortírozása” (Elsődleges, Közösségi, stb) nem fog működni,

hiszen az is a levelek tartalmának elemzéséből derül ki. A fenti funkció kikapcsolásának mikéntjéről itt olvashatunk egy egyszerű leírást: link.

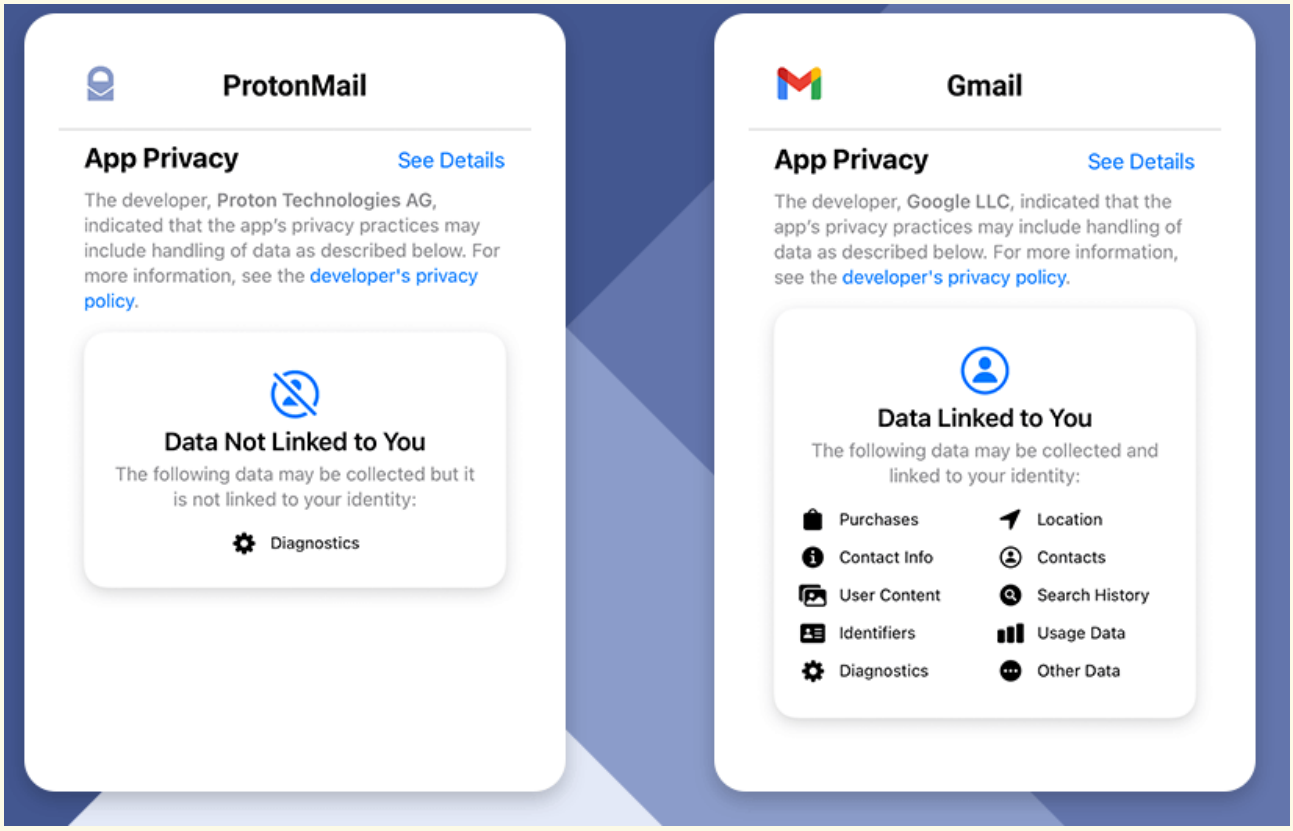
Email szolgáltatók

Lehet korlátozni a Gmailt, de az igazi megoldás egy olyan szolgáltató használata, amely nem akar és nem is képes beleolvasni a leveleinkbe. Ez nem csak saját leveleinkre igaz, de képzeljünk el egy orvost, pszichológust, vagy orvosi labort amely elmailben kommunikál páciensével és így minden egészségügyi és mentális probléma bekerül a Google személyhez rendelt profil adatbázisába.

Jó szívvel tudjuk ajánlani a Protonmail.com szolgáltatót, amely titkosítva tárolja leveleinket, maga a szolgáltató sem képes beleolvasni a levelekbe és metaadatokat sem tud gyűjteni, továbbá teljesíti a szigorú HIPAA – orvosi titoktartással kapcsolatos – követelményeket is. Az alapverzió ingyenes, de ésszerű árakkal nagyobb tárhelyet, több email címet (1 azonosító alá rendelve) és még számos más kényelmi funkciót kapunk. De ami a legfőbb, hogy nem személyes adatainkkal, hanem mint minden más szolgáltatásért úgynevezett *pénzzel* fizetünk – bár lehet, sokaknak ez maradinak hathat. A Proton szerverei fizikailag Svájcban vannak, amely ország az egyik legszigorúbb adatvédelmi törvénnyel védi adatainkat.

Remek hír, hogy van lehetőség Gmailben tárolt leveleink importálására is. Kövessük az útmutatót.

Az alábbi összehasonlító kép két eleme az Apple App Store alkalmazásboltjából származik. Az iOS 14.4 verziójáról kezdve az alkalmazások fejlesztőinek meg kell adniuk adatlapukon, hogy milyen személyes információkat gyűjtenek be a használat során és mi az, ami ezek közül személyhez is rendelt – nem csak általános, anonim statisztika.



Forrás: Proton hírlevél, 2021. április 7

További kiváló alkalmazás a **ProtonVPN** (erről később), valamint 2021 elején már beta teszt állapotban volt az (asztali és mobilos) **Proton Calendar** és a **Proton Drive** szolgáltatás is – természetesen mindkettő titkosított adattároláson alapul, tehát rajtunk kívül senki, még a szolgáltató sem képes belelátni adatainkba. Látható tehát, hogy egy privacy szempontból remek, teljes platform, ökoszisztéma épül ki.

Regisztrációs trükk emaillel

Mikor egy random weboldalon regisztrációkor email címünket alkalmazzuk mint felhasználói azonosító, olyankor bevethetünk egy apró trükköt, ami jól jöhet, ha később valakik elkezdenek levélszeméttel bombázni és nem tudjuk, vajon melyik weboldal adta el profil információinkat egy hirdetőcégnek. Tegyük fel, hogy email címünk *gipszjakab@protonmail.com* és a „Kedvenc Áruház” oldalon regisztrálunk. Email címünkbe a „+” jelet beszúrva regisztrálhatunk így is:

gipszjakab+KedvencAruhaz@protonmail.com

Az így küldött email rendesen megérkezik eredeti címünkre, a „+” jel utáni rész csak „megjegyzésként” marad rajta (szóközt ne használjunk). Így viszont mikor kéretlen levelet kapunk, megnézhetjük a **címzett** mezőt és rögtön látjuk, hogy ha ott a fenti email címet találjuk (gipszjakab+KedvencAruhaz@protonmail.com), akkor a Kedvenc Áruház volt az, aki talán nem bánik olyan jól az adatainkkal.

VPN (Virtual Private Network)

Röviden: egy VPN kliens alkalmazás segítségével laptopunkkal, mobilunkkal **titkosított csatornán** kapcsolódunk egy VPN szolgáltató szerverére és onnantól **minden adatunk, ami elhagyja gépünket, vagy beérkezik rá, ezen a közbeiktatott szerveren át közlekedik az internet felé, felől.**

A magyarországi törvények szerint az internet szolgáltatók kötelesek meghatározott ideig tárolni (néhány évig, de változó a jogi környezet) az internetezési metaadatokat, azaz hogy milyen oldalt, milyen szervert mikor nyitott meg a felhasználó. Ennek elfedésére (is) alkalmas a VPN, amely nem egy konkrét termék, hanem egy technológia. Sokféle VPN kliens és VPN szolgáltató létezik.

A VPN szoftverek lényege, hogy gépünkön egy titkosított csatornát (VPN tunnel) építenek ki az adatforgalom alsóbb rétegében egy külső, interneten levő VPN szerver felé. Ez a szerver lehet sajátunk (valahol a hálón, akár külföldön), a munkahelyünk saját VPN szervere, vagy jellemzően egy konkrét, általunk megbízhatónak ítélt, publikus VPN szolgáltatást nyújtó cégé.

Lényegében egy "titkos alagutat" építünk, ami nálunk indul és a VPN szerveren "bukkan ki" a netre. Ugyan a mi netszolgáltatónkon haladnak át az adatok, de titkosítva, ezért mindössze annyi látszódik – és naplózható számára – hogy egy darab adott szerverrel (a VPN kiszolgálóval) folytatunk titkosított kommunikációt. Minden netes forgalom ebben a csatornában halad.

A VPN technológia eredetileg táv-adminisztrátori célokra lett kitalálva, így például egy rendszergazda az otthonából bejelentkezve a munkahelye VPN szerverére, úgy dolgozhat, mintha „benn ülne” az irodában, annak belső hálózatára csatlakozva. Újabban viszont otthoni munkavégzés céljából, adatvédelmi okokból, kényelmi szolgáltatások használatáért (csak USA-ban elérhető streaming), illetve elnyomó rezsimek internetkorlátozását megkerülő céllal számos átlagember is használja.

– „Ez elég bonyolult, meg technikai, jó lenne egy példa.”

– „OK, nézzük, hogy érjük el mondjuk a *macskaskepek.hu* oldalt alapesetben, illetve VPN használatával és ilyenkor mit lát tevékenységünkből az internetszolgáltatónk.”

I. Példa hagyományos böngészésre – VPN nélkül

Beírjuk laptopunk böngészőjébe, hogy *macskaskepek.hu*, miközben otthon ülünk a wifi routerre kapcsolódva, amibe kedvenc internetszolgáltatónk kábele csatlakozik. Alapesetben mikor a cím beírása után leütjük az entert, laptopunk kapcsolódik a routerre, az a netszolgáltató szerverére, ami (több ugráson keresztül) eléri a *macskaskepek.hu oldalt*, ahonnan ugyanezen az úton visszajön a kért adat. A szolgáltató látja a forrást (mi) és a célt (*macskaskepek.hu)* és erről dátummal naplóbejegyzést is készít.

Ha az oldal **https** protokollt használ (kis pajzs vagy hasonló ikon a link előtt a böngészőben), akkor a kapcsolat titkosított, így az adat tartalmába nem tud belenézni – viszont nem is feltétlenül kell, a metaadat bőven elég (ki, milyen szerver felé, mikor, mennyi ideig, mennyi adatot forgalmazott). Úgy is ez az az adat, amit elad – ha a törvény lehetővé teszi, mint az Egyesült Államokban – vagy kiadhatja a hatóságoknak, ha a jogi környezet engedi – és újabban egyre könnyebben engedi.

II. Példa böngészésre VPN használatával

Ezúttal kiépítettünk valamilyen VPN csatornát laptopunkon és beírtuk a böngészőbe, hogy *macskaskepek.hu*. Az adatáramlás folyamata ekkor így néz ki:

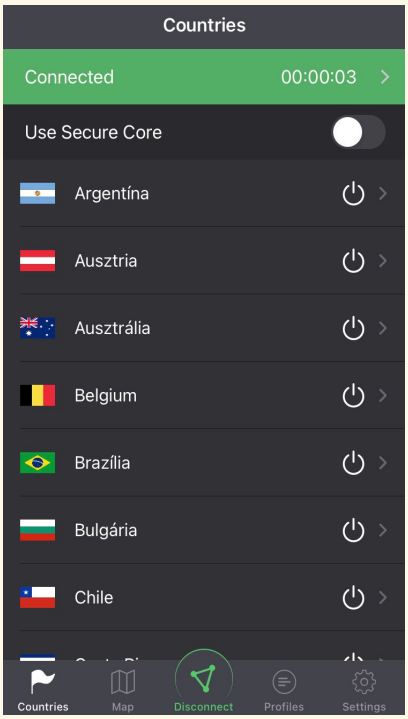
laptop böngésző → VPN csatorna nyit (titkosítás rátesz) → router → netszolgáltató szerveren áthalad a titkosított adat → VPN szerver (titkosítás lebont, adat kibont) → VPN csatorna zárul → *macskaskepek.hu*
Persze olyan VPN szolgáltatót kell találni, amelyik nem naplózza tevékenységünket és megbízható, mert innentől az internet szolgáltató helyett már a VPN szolgáltatónál van netezési statisztikáink kulcsa. Egy megbízható szolgáltató egyáltalán nem gyűjt ilyen adatokat.

Vannak böngészőhöz is VPN kiegészítők, de akkor csak arra a forgalomra vonatkoznak a fentiek, ami a böngészőn belül fut. Vannak operációs rendszerre – pl. Windows, Linux, OSX – telepíthető VPN kliensek, ekkor az adott számítógépről induló minden forgalom a VPN csatornában halad, ha bekapcsoljuk a funkciót.

Rengeteg VPN cég verseng manapság a felhasználók kegyeiért, influenszerek videói indulnak úgy, hogy „*This video is sponsored by Xyz VPN*”. Ezeket általában kerüljük, főleg ha ingyenesek. Ilyenkor elég gyanús, hogy miből csinálnak bevételt… hát nyilván netezési metaadataink értékesítéséből, amit most az ők kezükbe tettünk.

Más, kellemes célra is használhatjuk a VPN szolgáltatást, például magyarországi címről blokkolt külföldi tartalmak elérésére (egyes streaming szolgáltatók), vagy külföldi utazásunkkor itthoni – de külföldi címről nem elérhető – magyar oldalakhoz, szolgáltatásokhoz. Például ha valamilyen perverz, önpusztító okból külföldi nyaralásunk során a magyar közszolgálati tévét néznénk üres óráinkban – ami alapból csak magyar IP címről érhető el – akkor beállítunk VPN kliensünkön egy magyar szervert és már nézhetjük is az elfogulatlan, ... hiteles, ... tájékoztatást..

Az elmélet után a gyakorlati tanács:



ha nem szeretnénk, hogy szolgáltatónk gyűjtse netezésünk és a mobilalkalmazásaink által elért oldalak, szerverek listáját és előfizetői profilunkhoz csatolja, esetleg korlátozott, más országban elérhető oldalakat használnánk, akkor használjunk VPN-t asztali és mobil eszközeinken.

A korábban említett ProtonVPN kliens nagyon egyszerű és megbízható. Android és iOS mobil platformokra, valamint Windows, Mac és Linux asztali platformokra is elérhető, Protonmail azonosítónkkal használhatjuk. Ingyenes verziója a „Basic” szerverek használatára elég, fizetős csomagjaival több, gyorsabb „Plus” kiszolgálókat használhatunk. Lehetséges „bundle” csomagban egyszerre Protonmail és ProtonVPN szolgáltatásra egyben előfizetni.

Használatakor csak beállítjuk, melyik országban levő VPN szerverre kapcsolódjunk és onnan kezdve minden adatforgalmunk azon keresztül éri el az internetet.

fekete.balint @protonmail com

Keresők

Az utóbbi években bevéső dött, hogy „ha keresés, akkor Google”. De mi van, ha nem akarjuk, hogy minden keresésünk személyes profilunk építését szolgálja. Használjunk alternatív keresőket:

https://duckduckgo.com – Jelenleg a legnagyobb, privacy szempontból is kifogásolhatatlan kereső. Nem gyűjt semmilyen személyes adatot. Tipp: ha a keresőkifejezés után beírjuk, hogy „site:.hu”, akkor csak a „.hu”-ra végződő, tehát csak magyar oldalakon keres. Ez egy általános trükk, más keresőknél is működik.

https://www.ecosia.org – Erre is igazak a fentiek, továbbá kereséseinkkel fák ültetését támogatjuk.

https://brave.com

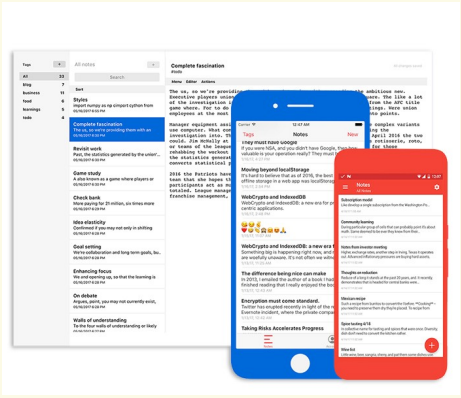
Online jegyzetelés

Kiváló mobil és asztali alkalmazással használható, sőt még böngészőből is elérhető jegyzetelő program a nyílt forráskódú Standard Notes, amit mindösszesen egy ember fejleszt, ráadásul igen intenzíven.

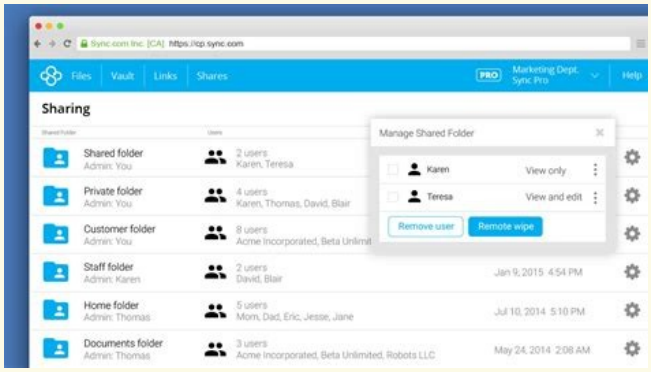
Ingyenesen is használható, a fizetős megoldással szövegeink formázásának lehetőségét kapjuk meg.

Jegyzeteinket kizárólag a mi jelszavunkkal feloldható titkosítással tárolja szerverén az alkalmazás. Biztonsági mentéseinek megadhatunk helyi meghajtónkon levő mappát.

Ha plusz biztonságot igényelünk, egyes jegyzetlapokra külön jelszóvédelmet is beállíthatunk.



Cloud tárhely

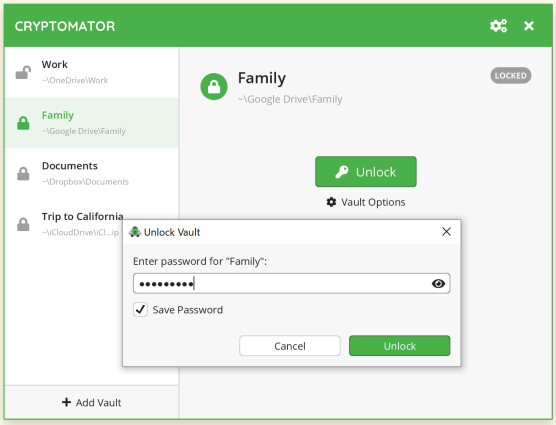


A Google Drive a szolgáltató korábban már részletesen tárgyalt kétes privacy feltételei miatt nem ajánlott. A már említett **Proton Drive** végső kiadásáig a sync.com felhőszolgáltatót tudjuk ajánlani. Itt is alap a fájlok titkosított tárolása, a szolgáltató nem gyűjt semmilyen metaadatot tevékenységünkről, mobil és asztali platformokra egyaránt elérhető.

Fájl tárolás asztali gépen, mobilon – titkosított konténerben

Az otthoni adattárolás a folyamatos internetkapcsolat korában már nem olyan szeparált, mint korábban. Az olyan alapvetésekre, mint hogy minden fontos adatunk minimum 2 példányban legyen meg külön adattárolón most nem vesztegetünk több szót.

Ha személyes munkánk, kutatásunk, szellemi termékünk szeretnénk külön, titkosított, jelszóval védett tárolóban tudni, akkor használjuk az ingyenes és nyílt forráskódú Cryptomator alkalmazást.



Tetszőleges számú tárolót hozhatunk létre abban a könyvtárban, ahol szeretnénk. A tárolót csak a program segítségével tudjuk kinyitni, anélkül mindössze visszafejthetetlen krixkraxokat láthatunk fájljaink helyén. Mikor „kinyitjuk” egy tárolónkat, az hálózati meghajtóként látszik majd a fájlkezelőben. Kevésbé megbízható felhőszolgáltatóval is összekapcsolhatjuk, ilyenkor a szolgáltató csak egy titkosított konténert lát a tárolt állományok között.

Fizikai védelem

A zsarolóvírusok korában már nem számít paranoiának eszközeink kamerájának leragasztása. Az igazat megvallva nem pont az volt eddig nagyon bizarr, hogy önként beengedtük ezeket a szenzorokat a legbelsőbb életterünkbe..? Pár évtizede ez az átlagember egyik legnagyobb félelme volt, mikor az államhatalom erőszakkal próbált a saját állampolgárairól terhelő információkat gyűjteni..

Laptop esetén az alábbi lépések ajánlottak:

- Laptop kamera letakarása
- Laptop mikrofon leragasztása. Érdekes adalék: Mark Zuckerberg laptopján is le van ragasztva a mikrofonnyílás, oh az irónia..

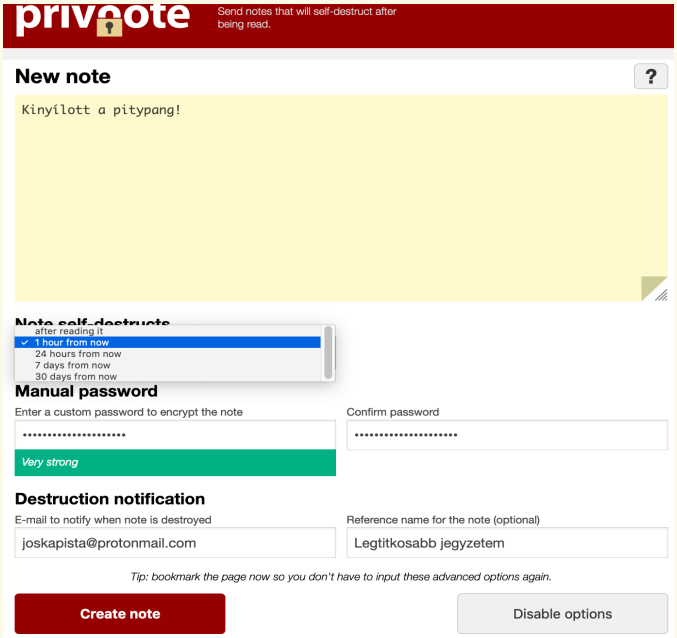
Mobiltelefon esetén is erősen javasolt a front kamera letakarása.

Privnote

Van hogy jelszót, vagy érzékeny szöveget szeretnénk könnyen eljuttatni valakihez úgy, hogy az üzenetnek biztos ne maradjon digitális „nyoma”, vagy másolata az interneten és olvasás után törlődjön is. Ilyenkor használhatjuk a Privnote weboldalt.

A szöveg bemásolása után beállíthatjuk, hogy mikor semmisüljön meg jegyzetünk: rögtön olvasás után, vagy meghatározott idő elteltével. Egyszer használatos jelszót is tehetünk rá, illetve értesítést is beállíthatunk email címünkre, amiben láthatjuk, hogy az üzenetet elolvasták.

A „Create note” gombra kattintás után egy frissen kreált internetes linket kapunk, amit emailben, vagy csevegőprogrammal eljuttathatunk a címzettnek – ha különösen érzékeny a tartalom, akkor a jelszót érdemes eltérő csatornán küldeni, mint magát az URL-t.



Jelszókezelő

Érzékeny téma a jelszavak tárolása. Van, aki a papír alapra esküszik és nem tárol semmit elektronikusan, van aki igen, de csak lokálisan, helyi gépen és van, aki egy kellően megbízhatónak ítélt szolgáltatónál akár a felhőben is tárolja jelszavait.

Papír alaphoz nem tudunk hozzászólni, de talán a félfamentes rajzlap nem a legjobb választás... Lokális megoldás esetén a Password Safe alkalmazást ajánljuk, ha pedig a felhőt választjuk, akkor a Bitwarden megoldását javasoljuk. Nyílt forráskodú, végpontok közti titkosítást (E2EE) használ – tehát a szolgáltató sem tud belenézni –, továbbá minden asztali és mobil platformra elérhető.

Hasznos gyakorlati tanácsok egy helyen

Az alábbi oldalak magyar nyelven adnak további áttekintést, gyakorlati tanácsokat. Tekintsünk el az ijesztgetős stílusuktól, sajnos ezen nehezen lépnek túl általában privacy témával foglalkozó oldalak. A tartalmuk viszont tényleg nagyon hasznos.

- https://maganelet.hu
- https://surveillancematters.com/nyitooldal/
- https://www.youronlinechoices.com/hu/ad-choices: megnézhetjük, hogy a böngészőnk által letárolt „sütik” milyen reklámcégektől származnak és állíthatjuk, hogy mit engedünk nekik. Az egyszerűbb – és ajánlott – megoldás inkább a sütik rendszeres törlése.

8. Mobiltelefon tudatos beállítása

Jön … jön … jön!

A következő hónapokban remélhetőleg ez a fejezet is elkészül. Az 1. fejezet végén található linken mindig a dokumentum legfrissebb változatát tölthetjük le. Érdemes néha ránézni.

9. Zárszó

Reméljük sikerült egy – ha nem is teljeskörű, de – érdekes áttekintést adni a privacy jelenkori helyzetéről és hogy mi, átlagemberként hogyan tudjuk megvalósítani egy egyelőre még törvénybe nem foglalt alapjogunkat. Minden jót és „Víg napot polgár!”

10. Források

Az illusztráció céljául szolgáló képek az unsplash.com weboldalról származnak, illetve egyénileg készített képernyőkép mentések. Az egyes alkalmazások képei azok hivatalos weboldalán láthatóak.

Az unsplash képek felhasználásának alapját adó licenc: https://unsplash.com/license

11. Licenc