Integritetsguide för nätet – del 1/2

> *Den mardröm många människor har […] att folken en gång skall komma att behärskas av tekniken – den var nästan förverkligad i Hitlers auktoritära system. Varje stat löper i dag risken att bli terroriserad av tekniken. […] Därför: ju mer teknisk världen blir, dess nödvändigare är som motvikt kravet på den enskilda människans individuella frihet och självmedvetande.*
>
> — Albert Speer, Hitlers arkitekt och rustningsminister, under Nürnbergrättegångarna.[Slutnot 1]

Scenario: Du känner till Cambridge Analytica-skandalen[2] och Facebooks integritetsproblem[3] (med deras nya valuta Libra som nytt orosmoln[4]). Hur Google närmar sig ett monopol i internets infrastruktur[5] och hur Googles och Facebooks affärsmodell riskerar att reducera demokratin[6]. Du märker att det blir svårare att leva i vardagen utan att ge upp din integritet genom att använda tjänster som säljer sina användares dataanvändning och kan förändra sina användarvillkor och program utan förvarning. Ibland kanske du blir förvånad över hur lite kontroll du har över en tjänst eller enhet som du har betalat för. Kanske du inte är en John Deer-traktorägare, som plötsligt fått veta att det inte är tillåtet att hen själv reparerar, eller själv väljer en tredje part, att reparera sin traktor (utan det får endast göras av en officiell John Deer-reparatör)?[7] Kanske du inte är en fotograf som hotas att bli stämd av Adobe för att du inte uppdaterar, och förstås därmed betalar extra, för den senaste versionen av Photoshop (trots att du betalat för din nuvarande version och personligen inte har något behov av en uppdatering)?[8] Kanske du inte är en Windowsanvändare som blir frustrerad av att din dator uppdaterar sig själv utan ditt samtycke och installerar Candy Crush utan att fråga dig[9] eller uppdaterade till Windows 10 utan lov för att sedan ta bort dina personliga filer?[10] Kanske du inte är en Apple-användare som tvingas köpa en ny iPhone, trots att det inte är något tekniskt fel på din nuvarande iPhone, eftersom Apple med flit slöar ner telefonen i fråga så du måste köpa en ny?[11, 12] Kanske du inte är en företagare som försöker skapa en konkurrerande tjänst till Uber, men blir saboterad av din konkurrents hemliga datainsamling?[13] Kanske du inte är en Hong Kong-bo som skadats under protesterna mot Kinas ökade kontroll över regionen och är nervös över att sjukhuset ger vidare dina uppgifter till myndigheterna.[14, 15]

Nej, inget av det där har lyckligtvis hänt till dig. Du må ha din laptops kamera fasttejpad (men inte din telefons kamera, av någon orsak). Det känns lite löjligt. Men samtidigt får du dig ibland en tankeställare när du läser en ny artikel gällande den minskande integriteten, men samtidigt är väl demokratin ännu tillräckligt intakt?

Men ja, det är lite som att i den digitala världen ska man ha dörren olåst i sin hyreslägenhet. Tredje parter må titta in och snoka lite, göra upp statistik om en, tjäna pengar på en, men det kan man ju bara ignorera? En del argumenterar att att samla data är den nya oljeindustrin, där ett litet antal bolag med oligopol- eller rentav monopolstatus fortsätter att växa och bli mäktigare.[16] Kunskap är makt och vad är inte data, samlad i tillräckligt stor mängd och organiserad, om inte kunskap? Kunskap om vad konsumenterna vill ha, eller vad man kan få dem att vilja ha.

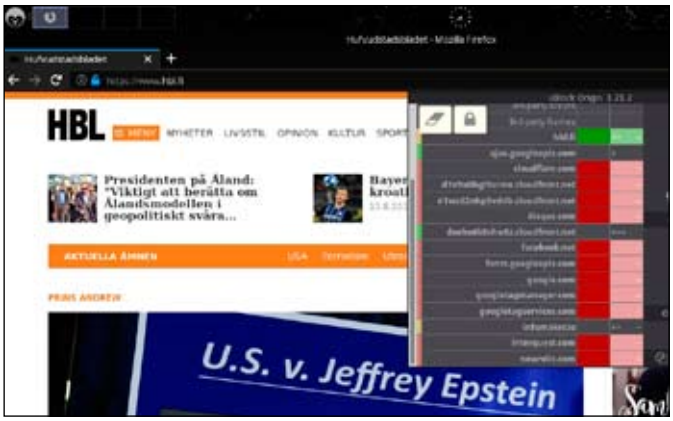
Vad om man får nog? Vad ska en laglydig medborgare som inte har någonting att dölja, men som inte har någonting att visa heller, ta sig till? Finns det alternativ som är mer långsiktigt vettiga utan att man behöver leva under en sten?

Kanske![1]

Webbläsare

Om vi börjar på integritetens mjuka sida. Det finns tillägg (eng. *add-ons*) som det lönar sig att installera i din dators webbläsare. Nio av tio hemsidor är idag fyllda av javascript från tredje parter som enbart har två funktioner: spionera på användarna (antingen dolt genom kod, till exempel genom så kallad *browser fingerprinting*[17] som inte syns på hemsidan, eller genom annonser som även de samlar in data och identifierar användarna, eller i värsta fall laddar in virus i användarnas webbläsare eller operativsystem. **uBlock**

1 Följande guide ger dig inte anonymitet. Den listar snarare tjänster som i mycket högre grad respekterar din integritet. Du undviker, eller åtminstone reducerar, att dina data blir sålda.



Bilden: De flesta hemsidor innehåller idag överflödig kod som spårar användarna. Man kan till exempel blockera 19% av HBL:s kod (röda staplar t.h. på skärmdumpen) utan att det påverkar upplevelsen av deras hemsida. Börjar man använda uBlock Origin i avancerat läge märker man snabbt att Google och Facebook finns överallt, från nyhetssidor till Kela.

Origin blockerar många spårare och annonser utan att förstöra hemsidorna i fråga.[2]

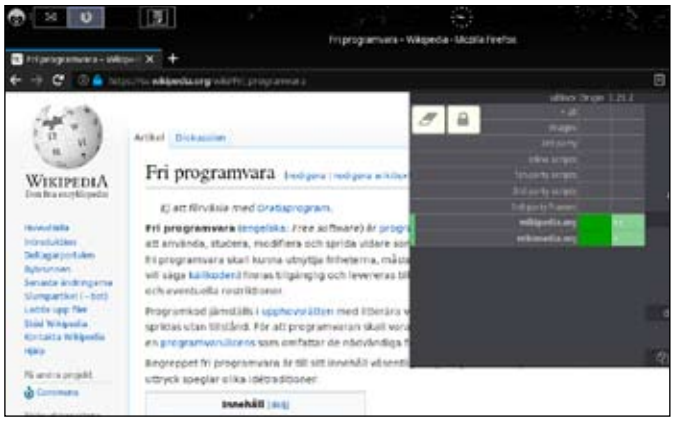
Om du redan använder en annan annonsblockerare än uBlock Origin kan det löna sig att byta. uBlock Origin har öppen källkod (eng. *open source*[3]) vilket innebär att koden är öppen för allmänheten. I praktiken gör detta det möjligt för utomstående att kontrollera att programmet gör vad det utlovar utan att göra andra olovliga saker i bakgrunden. Tänk det som att du köper bröd som listar vilka råvaror som använts till att baka det i jämförelse med att köpa ett bröd utan ingrediensförteckning, där företaget i fråga bara muntligt garanterar, men vägrar att i praktiken visa vad det sist och slutligen innehåller. De allra flesta kan gott köpa sitt bröd utan att bry sig om vad alla namn och e-koder egentligen innebär. Men för det allmännas bästa finns alltid möjligheten för individen att själv ta reda på mer om produktens innehåll, inte bara genom att fråga företaget utan också genom att fråga utomstående experter (eller själv gå in för att lära sig). Många program och tillägg som idag används är proprietära (eng. *proprietary*), det vill säga har låst källkod, vilket i praktiken betyder att användarna inte kan veta vad tillägget gör på sidan om, eftersom koden aldrig visas för utomstående. Många annonsblockerare har åkt fast för att till exempel sälja användarnas data i bakgrunden. En ofta återkommande funktion i proprietära tjänster och appar är att de gör mycket i bakgrunden som användarna inte bett om eller ens känner till, det senaste uppmärksammade exemplet vore hur FaceApp har rätt att sälja användarnas bilder.[19]

Fint! Förutom frihet från annonser och mindre risk för virus har du nu också en snabbare nätuppkoppling, eftersom din webbläsare inte behöver ladda lika mycket innehåll. Andra tillägg som det verkligen lönar sig att installera: **HTTPS Everywhere, Privacy Badger** och **Decentraleyes**. Inga av dessa kräver, precis som uBlock Origin, något underhåll. Installera och surfa med ro.[4]

2 Rent etiskt kan man fråga sig om det är rätt eller fel att blockera annonser på de hemsidor man besöker, eftersom företagen i fråga förlorar sin inkomst (*https://www.independent.co.uk/voices/comment/heres-why-you-should-delete-adblock-right-now-10264083.html*). Det är vars och ens eget val. Personligen svarar jag att så länge dessa företag själva väljer att inbegripa spionerande kod från tredje part samt annonser som per automatik säljer våra data till Facebook, Google m.fl., och dessutom ger användarna risken för virusinfektioner på sina system, kan de gott förlora denna inkomstkälla. Som alternativ till de tjänster och hemsidor du uppskattar kan du ju betala för hemsidan du besöker genom att till exempel prenumerera, om vi pratar om tidningar, eller donera, vilket ett flertal hemsidor gör möjligt.

3 Jag använder uttrycket *open source* (sv. öppen källkod) eftersom det är den mer kända termen och saker är krångliga nog som de är. Öppen källkod ger i de flesta fall goda säkerhets- och integritetsmöjliheter, men rent praktiskt finns det ingen garanti för att något som är open source är etiskt (Chromium är till exempel Google Chromes open source-version och den spionerar inte mindre bara för det). För att ytterligare säkerhetställa att ett program eller en app gör det man tror den gör lönar det sig att använda så kallad fri programvara (eng. *free software*, free som i fri, inte gratis). Free software innebär i stort sett open source-program som förutom att de har öppen källkod följer Free Software Foundations regler, vilket ger användarna rättigheterna att a) använda programmet som användaren själv vill, b) källkoden är fritt tillgänglig och får studeras, c) programmet får kopieras, d) användaren har rätt att göra ändringar i programmet, men dessa ändringar måste även de publiceras öppet som fri programvara (*https://www.gnu.org/philosophy/free-sw.sv.html*). Operativsystemet Linux, mediespelaren VLC samt encyklopedin Wikipedia är tre exempel på open source-produkter som också är free software.

4 Dessa ger dig större integritet på grund av blockeringarna, men ja, samtidigt får du också en mer unik webbläsarkonfigurering. Vilket ironiskt nog gör att du blir i viss



Bilden: Inga spionskript på Wikipedia (enbart gröna staplar). Du märker det bland annat på hur snabbt Wikipedia laddar i jämförelse med de flesta andra hemsidor du besöker (speciellt om du jämför efter att ha rensat dina kakor).

Du kommer kanske ihåg att man inte ska ge ut till exempel sina bankkortsuppgifter till hemsidor som inte stöder HTTPS, men visste du att det trots att en sida har HTTPS inte är sagt att all tredjepartskod har HTTPS, utan enbart HTTP, vilket är okrypterat och därmed sätter dina personuppgifter och de data du ger i öppen dag för vem som nu råkar snoka? HTTPS Everywhere är ett tillägg som ser till att hemsidan man besöker faktiskt använder HTTPS, vilket ger dig större säkerhet och integritet. Detta tillägg förstör heller inte hemsidor.

Privacy Badger skannar på hemsidor efter tredje parter som upprepas men inte har någon funktion på hemsidan, det vill säga spårare (eng. *trackers*). När en sådan tredje part identifieras på en hemsida för tredje gången blockeras den automatiskt. Detta påverkar heller inte hemsidor, eftersom spårare inte bidrar med någonting – förutom att de spårar dig, slöar ner din internetuppkoppling och i värsta fall till exempel kan höja priserna på tjänster, eftersom den vet att det är du som besöker en viss produkt igen (för att garantera att sådant inte sker krävs dock mycket mer än enbart Privacy Badger, men det är i alla fall en början). Privacy Badger blockerar dock inte Google eller Facebook. Man kan lägga till dem manuellt i blocklistan om man så önskar.

Decentraleyes snappar upp en hemsidas förfrågningar efter kod från tredje part och använder (en smula förenklat) istället din webbläsares lokala kodversion. Det är oftast tredje parter på en hemsida som ger större risker.

En annan sak att överväga: om du, likt 66% av internet, använder Google Chrome[20] är det en bra idé att byta till till exempel Firefox. Google Chrome var tidigare den snabbaste webbläsaren, men nuförtiden har den så många extra spårare och extra kod, som bara används för spionage på användarna, att den är en integritetsmardröm.[21] Vill du öka möjligheten för ett fortsatt fritt internet är Firefox ett bra alternativ. Googles hela affärsmodell är att sälja användarnas data. Firefox är open source och tillhör Mozilla, som är en ideell organisation som värnar om ett öppet internet. Idag är Firefox även snabbare än Chrome eftersom det inte har samma mängd extra kod som är gjord för spionieri. Chrome har även blivit fast för att sabotera för andra webbläsare, till exempel genom att kräva dem på en så kallad *captcha* (innan man loggar in på en tjänst måste man välja rätt bilder) eller slöa ner YouTube för dem.[22] Tilläggen jag tidigare listat fungerar både för Firefox och Chrome.[5] Måste man nödvändigtvis använda Google Chrome av x orsak så är ett alternativ **Ungoogled Chromium**, som är Google Chrome men med mycket av Googles spårare borttagna.

Vill du på riktigt reducera spårning bör du dock även installera **Cookie Autodelete**. Så kallade kakor är problematiska eftersom de behövs för att en hel del hemsidor ska fungera på din dator, men de sparas och registrerar ofta vilka hemsidor du besöker. Det räcker inte att tömma kakorna varje gång du

mån lättare att identifiera (du kan själv se på hemsidor som till exempel *https://ipleak.net* att varje hemsida du besöker får ganska mycket information, bland annat ”ser” var du befinner dig fysiskt, storleken på din skärm, ditt operativsystem, webbläsare och så vidare, som läggs ihop med kakor och historik). Det bästa vore att lära sig använda uBlock Origin i avancerat/manuellt läge, men detta gör att i stort sett varje hemsida man besöker ”går sönder” och man måste själv manuellt aktivera de delar av hemsidan man vill komma åt. Detta är förstås i praktiken för tröttsamt för de flesta. Men även om man riskerar ett mera unikt ’digitalt avtryck’ med fler tillägg installerade (om inte majoriteten börjar använda just dessa tillägg), är det sist och slutligen ändå bättre att ta den risken än att ge ifrån sig de data som tilläggen ska hindra att sprids. Utan tilllägg har man också ett unikt ’digitalt avtryck’.

5 I ett skede såg det ut som om Chrome skulle börja förbjuda en del tillägg, till exempel annonsblockerarna. Det har sedan dess dragits tillbaka, men det är ännu en orsak till att det är farligt att låta Google bli ännu mer dominerande.[23]

stänger din webbläsare (fastän det är bättre än att aldrig radera kakor överhuvudtaget). När du besöker någonting Google- eller Facebook-relaterat sparas deras kakor igen och de följer dig tills du stänger webbläsaren. Cookie Autodelete raderar kakor så snart de inte längre behövs. En varning dock. Du måste antingen 'vitlista' (white list) varje sida du litar på, där du vill logga in, eller spara några inställningar, för utan kakor behandlas du alltid som om du besöker sidan för första gången.

Vill du gå längre kan du göra efterforskningar i hur du använder så kallade 'containers' i Firefox, eller varför inte surfa med **Tor**? När du funderar på vad du vill köpa kan du till exempel använda Tor för att reducera att bli förföljd och att till exempel priserna höjs därefter. När du bestämt dig för vad du vill ha byter du till Firefox när du köper produkten ifråga. Du bör dock göra lite efterforskningar innan du använder Tor. Logga till exempel aldrig in till din nätbank genom Tor. Det bästa när det handlar om att använda en nätbank är att använda en annan webbläsare som du inte använder till någonting annat.

RICKY LINDÉN

I nästa nummer del 2/2 av integritetsguiden: om mobil, sökmotor, e-post, sociala media, YouTube, operativsystem.

Slutnoter

1 Speer, Albert (1969). *Memoarer*. Ullstein Verlag, Berlin: ScandBook, Falun 2003. [s. 421]

2 https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [Hämtad 27.6.2019]

3 https://techcrunch.com/2018/02/19/facebooks-tracking-of-non-users-ruled-illegal-again/amp/

4 https://www.thesun.co.uk/tech/9319668/facebook-launch-libra-cryptocurrency/ [Hämtad 27.6.2019]

5 https://www.washingtonpost.com/opinions/2019/06/21/googles-immense-power-threatens-open-internet/ [Hämtad 27.6.2019]

6 https://news.yahoo.com/big-tech-fraud-regulation-090000250.html [Hämtad 23.7.2019]

7 https://twitter.com/BernieSanders/status/1125109464980434955 [Hämtad 27.6.2019]

8 https://www.vice.com/en_us/article/a3xk3p/adobe-tells-users-they-can-get-sued-for-using-old-versions-of-photoshop [Hämtad 27.6.2019]

9 https://www.howtogeek.com/342871/hey-microsoft-stop-installing-apps-on-my-pc-without-asking/ [Hämtad 27.6.2019]

10 https://www.forbes.com/sites/gordonkelly/2018/10/06/microsoft-windows-10-update-lost-data-upgrade-windows-7-windows-xp-free-upgrade/ [Hämtad 23.7.2019]

11 https://www.nbcnews.com/tech/tech-news/apple-slowed-iphones-forcing-owners-buy-new-ones-lawsuit-claims-n832416 [Hämtad 27.6.2019]

12 https://www.theverge.com/circuitbreaker/2017/12/27/16822736/apple-battery-slowdown-iphone-6-6s-se-lawsuit

13 https://www.theguardian.com/technology/2017/apr/13/uber-allegedly-used-secret-program-to-cripple-rival-lyft [Hämtad 27.6.2019]

14 https://www.nbcnews.com/news/worldhttps://www.howtogeek.com/342871/hey-microsoft-stop-installing-apps-on-my-pc-without-asking//hong-kong-protesters-are-deep-fear-about-leaving-digital-footprint-n1020146 [Hämtad 27.6.2019]

15 https://www.reddit.com/r/privacy/comments/c0le4p/hong_kong_government_requires_public_hospitals_to/

16 https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

17 https://restoreprivacy.com/browser-fingerprinting/

18 https://www.avg.com/en/signal/what-is-malvertising

19 https://nakedsecurity.sophos.com/2018/07/26/more-browser-extensions-and-apps-caught-spying-on-users/

20 https://www.netmarketshare.com/browser-market-share.aspx

21 https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/ [Hämtad 27.6.2019]

22 https://www.zdnet.com/article/former-mozilla-exec-google-has-sabotaged-firefox-for-years/

23 https://www.theregister.co.uk/2019/01/22/google_chrome_browser_ad_content_block_change/3/jun/06/us-tech-giants-nsa-data; https://www.dn.se/ekonomi/linus-larsson-apple-slar-till-rejalt-mot-facebooks-betalda-avlyssning/

Ovanstående artikel med länkar kan också läsas på *Nya Argus* nätsidor (http://www.kolumbus.fi/nya.argus/) – som för övrigt inte använder kakor eller annan spårning. — Red.