# Osobe od interesa

Aplikacija za slanje poruka ToTok, koju su koristili milijuni korisnika, zapravo je špijunski alat Ujedinjenih Arapskih Emirata! To je vijest koja je procurila preko New York Timesa iz obavještajne zajednice. Posljedično, Apple i Google su je uklonili iz svojih trgovina, a korisnicima koji su je instalirali preporučuje se da je uklone s pametnih telefona. Blago nama! Otkrivena je još jedna prijevara, besplatna aplikacija koja nas špijunira. Sada smo sigurni, više nas ne špijuniraju neki zakašnjeli outsideri koji se nastoje ubaciti u svjetsku igru prijestolja.

U krimi serijama navikli smo na prizore ispitivanja sumnjivaca u prostoriji s minimalnim namještajem: tu je stol s nekoliko stolica i veliko ogledalo na zidu. Svi već znaju da je to lažno ogledalo, staklo koje propušta svjetlost u jednom smjeru, ogledalo sa skrivenom funkcijom, neka vrsta trojanca. S druge strane ogledala su specijalisti koji čitaju govor tijela i profiliraju sumnjivce, nastojeći otkriti kad lažu, kad govore istinu, gdje ih treba pritisnuti, u kom smjeru voditi razgovor.

Zapravo ne bismo trebali koristiti izraz sumnjivci. Ljude se ispituje i kad se smatra da znaju informacije koje bi pomogle istrazi. Američki izraz za njih je "person of interest". To je politički korektnije. No u fizičkom svijetu ne može se svakoga samo tako dovesti u sobu za ispitivanje, mora postojati valjan povod, a osoba od interesa može odbiti odgovarati na pitanja bez prisustva odvjetnika. Dakle osoba od interesa ima svoja prava, na koja se može pozvati. Pretpostaljamo da ista pravila vrijede i u virtualnom svijetu Interneta, zar ne?

Nedavno je Electronic Frontier Foundation, neprofitna organizacija posvećena zaštiti digitalne privatnosti, slobode govora i inovativnosti, objavila dokument o tome kako tvrtke prikupljaju podatke o nama. U dokumentu se koristi "trojansko" ogledalo kao metafora tog nadzora. Dokument pod nazivom "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance" javno je dostupan i može se skinuti s ove adrese [1].

Doslovno ćemo prenijeti uvodno poglavlje spomenutog dokumenta.

"Pratitelji (trackers) kriju se u gotovo svakom kutku današnjeg Interneta, a to znači u gotovo svakom kutku modernog života. Web stranice dijele podatke s desecima vanjskih tvrtki. Prosječna mobilna aplikacija čini isto, mnoge aplikacije prikupljaju osjetljive podatke kao što je lokacija i zapisi poziva čak i kad ih ne koristimo. Praćenje zahvaća i fizički svijet. Trgovački centri imaju automatske čitače regitracija za praćenje prometa na svojim parkiralištima i zatim ih dijele s policijom. Tvrtke, organizatori koncerata i političke kampanje koriste bluetooth i Wifi odašiljače za pasivni nadzor ljudi unutar svog prostora. Trgovine koriste prepoznavanje lica da identificiraju kupce, otkrivaju krađe i isporučuju ciljane reklame.

Tehnološke tvrtke, data brokeri i oglašivači koji stoje iza ovog nadzora kao i tehnologije koja ga omogućavaju većinom su nevidljivi prosječnom korisniku. Korporacije su izgradile dvoranu jednosmjernih ogledala: iznutra vidimo samo aplikacije, web stranice, oglase i samog sebe kako nas odražavaju društvene mreže. Ali u sjenama iza stakla pratitelji tiho bilježe sve što radimo. Ovi pratitelji nisu sveznajući, ali su široko rasprostranjeni i nisu izbirljivi. Podaci koje prikupljaju i izvode nisu savršeni, ali su svejedno iznimno osjetljivi."

Nakon ovako upečatljivog uvoda, ostatak dokumenta (PDF od 48 stranica) jasnim, razumljivim jezikom objašnjava kako praćenje funkcionira. Dokument bi trebao pročitati svaki korisnik Interneta,

kako bi shvatio razmjere nadzora i pobrinuo se da smanji i ograniči zloupotrebu vlastitih osobnih podataka. Prenijet ćemo, ukratko, nekoliko naglasaka.

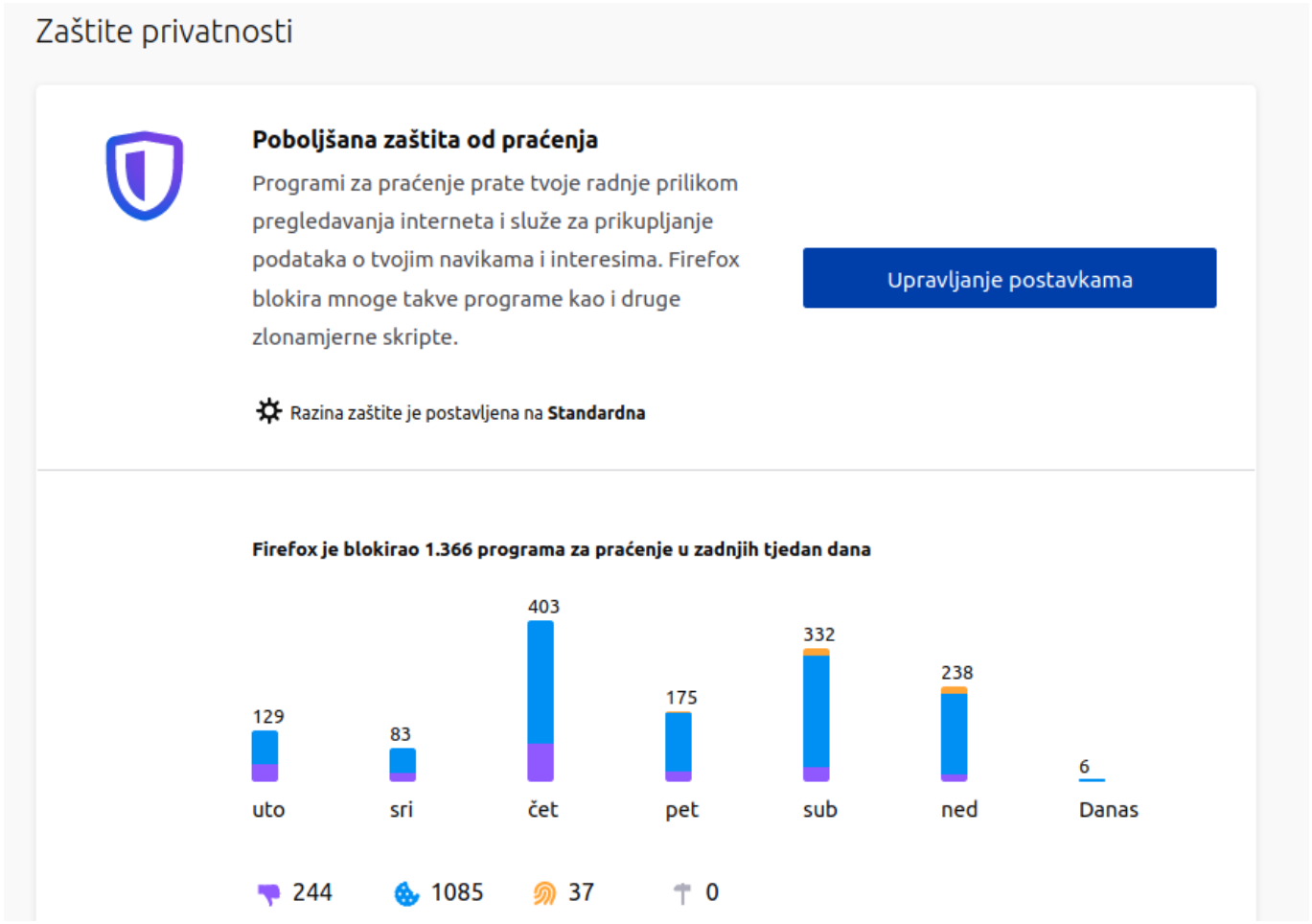
Najprije se objašnjava što je "first-party" odnosno "third-party" praćenje. Kad Facebook ili Google bilježi sve što radite koristeći njihove servise, tu je sve manje više jasno, oni su "first-party". Pristali smo na to kad smo kliknuli, gotovo uvijek bez čitanja napornih detalja, da pristajemo na uvjete korištenja. Osim toga, donekle se možemo zaštiti podešavanjem postavki, ako si damo truda, čime se većina korisnika ne zamara. Google i FB ipak moraju poštivati regulativu koja štiti osobne podatke, makar nevoljko.

No u igru su, zahvaljujući softverskim dodacima koji se aktiviraju na web stranicama, uključene brojne tvrtke "treće strane". Tu korisnici posve gube kontrolu nad time što se događa s njihovim podacima. Data brokers su tvrtke koje žive od prikupljanja podataka iz mnoštva izvora, njihove obrade, odnosno pročišćavanja, organizacije i analize. Te podatke daju na raspolaganje svima koji su zainteresirani. Pri tom se ne koristi izraz "prodaja podataka", jer bi to bilo pravno problematično, s obzirom na činjenicu da brokeri nisu vlasnici podataka koje obrađuju, pa ne mogu prodajom prenijeti vlasništvo nad njima. Zato kažu da svojim klijentima daju licencu za korištenje obrađenih podataka za određenu, ograničenu svrhu. Lukavo, zar ne? Tako se pitanje vlasništva nad podacima ostavlja po strani. Zasad to funkcionira, sve dok mi to dopuštamo. Naime, temeljna je činjenica koju olako previđamo da smo vlasnici osobnih podataka mi, korisnici. Sve dok nas nije briga što se s tim podacima radi, netko će na tim podacima profitirati, a da mi od toga nemamo nikakvu korist. Činjenica je da korisnici Interneta nisu svjesni vrijednosti svojih osobnih podataka, pa se olako odriču svojih prava. Da bi dobili neku sumnjivu mrežnu uslugu, odriču se privatnosti i dopuštaju da netko skriven iza ogledala zarađuje na njihovom vlasništvu, bez njihova znanja, bez traženja privole, a pri tom ne mora s njima dijeliti dobit. Kad bi netko obrađivao njivu koju ste naslijedili kao djedovinu, da li biste tražili za sebe dio dobiti? Pogotovo ako njivu obrađuje na crno, ne tražeći od vlasnika dozvolu?

Najveći dio dokumenta objašnjava različite tehnike praćenja korisnika. Čitatelji koji nisu tehnološki potkovani neće sve shvatiti, ali im svejedno preporučujem da pokušaju izdržati do kraja, ako ništa drugo, zaprepastit će ih mnoštvo načina na koji se pratitelji dovijaju kako doći do informacija, koristeći sve što im tehnogija pruža. Sam web preglednik šalje dosta informacija kad zahtijeva konekciju, na primjer javlja da se radi o Firefoxu na Ubuntu Linuxu. Otkriva se IP adresa s koje se korisnik spaja, pomoću nje se može odrediti država, vremenska zona. Tada slijede različite vrste kolačića, od kojih su najopasniji *local storage cookies*. Kod kriptiranih veza pamti se TLS state, polutrajni podatak koji šalje server da bi se rasteretio zahtjevnog procesa izračunavanja kriptografskih ključeva za svakog klijenta. Složenije su tehnike *browser i canvas fingerprinting* - to će gradivo zanimati radoznale sistemce.

Ono što *trackeri* pokušavaju napraviti jest prikupiti što više naizgled nepovezanih informacija, a onda ih složiti u profil i po mogućnosti taj profil povezati sa stvarnom osobom. Kako koristimo više uređaja, računalo, tablet, pametni telefon, jedan od izazova je sve te uređaje povezati s korisnikovim identitetom. Kad pristupite Googleu ili Facebooku s novog uređaja, dobit ćete mail koji od vas traži da javite da li ste to bili vi. Tu se radi o brizi za vašu sigurnost, upozorenju da je možda netko drugi koristio vaš identitet. Ako ne odgovorite na mail, praktički ste potvrdili da se radi o vama, pa se uz vaš profil veže novi uređaj, na kojeg će se odmah snimiti neka šifra koja potvrđuje vaš identitet i služi za praćenje vaše aktivnosti.

Zapanjujuća je količina veza koje web stranice povezuje s tvrtkama koje spadaju u "treću stranu", a kojih korisnici nisu svjesni. Pratitelji se ne oslanjaju samo na usluge prve strane, već nastoje na naša računala ubaciti svoje idenitifikatore, koristeći na primjer JavaScript. Srećom, Firefox već sa zadanom konfiguracijom blokira mnoštvo takvih pokušaja, a ta mu pravila možemo još i postrožiti. Cijena koju ćemo platiti jest da nećemo moći koristiti neke siteove, ali uvijek možemo postaviti iznimke za stroge blokade. Provjerite imate li istu razinu zaštite s preglednikom koji koristite.




Postoje zakoni koji štite našu privatnost, ali je praksa još u razvoju, u previranju. Griješe korisnici koji misle da su automatski zaštićeni, da će netko drugi sve odraditi za njih. Google na primjer ima svoje poslovne interese i nastoji balansirati između prava korisnika i zahtjeva svojih komercijalnih partnera. Čak je i gđa. Merkel kao granicu zaštite osobnih podataka navela potrebe privrednog razvoja. Kako pronaći tu granicu? Drugo mjesto gdje zaštita osobnih podataka smeta napretku jesu znanstvena istraživanja. U medijima možemo pročitati [2] s koliko je napora mlada istraživačica skupljala podatke o razvodima u Hrvatskoj. Neke analize nije mogla ni provesti, jer nije imala uvid u sve potrebne podatke. S druge strane, kao negativni primjer još nam je pred očima afera s Cambridge Analiticom koja je uz pomoć analize podataka, dobijenih od Facebooka bez privole korisnika, ciljanim marketingom utjecala na rezultate izbora. Dokument EFF opisuje tehnike nadzora koje komercijalne tvrtke koriste u svoju korist, a s Cambridge Analiticom dodirnuli smo se i politike.

Kakve zaključke možemo izvući nakon što osvijestimo ovu situaciju masovnog nadzora? Ako se vratimo na metaforu s početka članka, možemo li reći da je Internet cijeli svijet pretvorio u jednu veliku sobu za ispitivanje? Da smo svi postali "osobe od interesa" iako nismo sudjelovali niti svjedočili nekom kršenju zakona? Nadziru nas a da nismo ni svjesni da smo u sobi za ispitivanje (interogation room) pa i ne tražimo zaštitu odvjetnika. Da li, nakon što smo u prošlom stoljeću preživjeli dva totalitarizma, ulazimo u novi: društvo totalnog nadzora? Ispada da u virtualnom svijetu imamo manja prava nego u fizičkom, iako nas štite zakoni poput GDPR-a. Nismo svjesni razmjera tog praćenja, pa ga olako shvaćamo. Većina će se ljudi odreći svojih prava radi malo komfora i poneke besplatne usluge. Čekaju nas novi izazovi, ako ne namjeravamo samo tako prihvatiti "nužnosti" i prepustiti da nas nosi struja. Slobodu treba definirati na nov način. Dosad smo je definirali kao slobodu mišljenja, govora i udruživanja. Danas možeš misliti što hoćeš, govoriti (manje više) što misliš, udruživati se do mile volje s "prijateljima" koje ne poznaješ i zapravo ne znaš da li su stvarne osobe ili trolovi, a da to nema nekog utjecaja na svijet. **Danas se, možda, sloboda treba definirati pravom na privatnost!** Kao i uvijek, samo najbogatiji si mogu priuštiti takvu slobodu. Najbolje je biti bogati i anoniman, zar ne?

čet, 2020-01-16 11:35 - Aco Dmitrović**Kategorije:** Kolumna [3]
**Vote:** 5

Vaša ocjena: Nema Average: 5 (1 vote)

**story_tag:** zaštita osobnih podataka [4]
tracking [5]

**Source URL:** https://sysportal.carnet.hr/node/1861

**Links**
[1] https://www.eff.org/document/behind-one-way-mirror-deep-dive-technology-corporate-surveillance
[2] https://www.jutarnji.hr/life/obitelj-i-djeca/prva-analiza-takve-vrste-ikad-napravljena-u-hrvatskoj-evo-zasto-kako-i-kada-krahiraju-brakovi-gradana/6757746/
[3] https://sysportal.carnet.hr/taxonomy/term/71
[4] https://sysportal.carnet.hr/taxonomy/term/347
[5] https://sysportal.carnet.hr/taxonomy/term/348