CARNET

Osnove privatnosti na Internetu

NCERT-PUBDOC-2017-12-350

CERT.hr

Sadržaj

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Privatnost je jedno od temeljnih ljudskih prava, no unatoč tome, ona je u današnje vrijeme slabo shvaćena i često narušavana, pogotovo u domeni Interneta i telekomunikacija. Iako svi intuitivno razumiju potrebu da se neke sfere života i neke osobne informacije zadrže dalje od očiju javnosti, prosječni korisnici u pravilu nisu svjesni opsega osobnih informacija koje korištenjem Interneta prepuštaju trećim, često nepoznatim stranama.

1.1 Zašto štititi privatnost?

Srž problematike zaštite privatnosti nije, kao što se to često u medijima predstavlja, apsolutna zaštita identiteta korisnika Interneta kako bi se omogućilo skrivanje iza nepoznatog nadimka. Protivnici zaštite privatnosti pri tome najčešće iznose primjere kriminalaca i terorista kojima privatnost omogućuje nesmetano obavljanje nepoželjnih aktivnosti dok normalni građani ne bi trebali imati ništa za sakriti te se stoga ne bi trebali boriti za zaštitu privatnosti. Ovaj je argument dvostruko promašen i varljiv.

Prije svega, doista postoje brojni represivni režimi koji strogo kažnjavaju svaki javni ili privatni izraz neslaganja, kršeći time slobodu govora i mišljenja i kojima je ovakvo uskraćivanje zaštite privatnosti na Internetu moćno oružje kojim osiguravaju svoju vlast na štetu ljudskih sloboda.

Ali argument je promašen i kad se radi o "normalnim" građanima u slobodnim i demokratskim zemljama. Premještajući naglasak debate na kriminal i terorizam, odvraća se pažnja s činjenice da su sva demokratska društva prepoznala i zaštitila građane od svih oblika diskriminacije. Naše društvo donijelo je zakone kojima se strogo zabranjuje diskriminirati na osnovu rase, vjere, spola, dobi, političkih i ostalih uvjerenja. Tako zakon npr. izričito brani poslodavcima da od kandidata za posao traže podatke o vjerskim i političkim uvjerenjima, spolu, starosti, zdravstvenom stanju i planovima za rađanje djece te na brojne druge načine štiti osobnu privatnost pojedinca kako bi osigurao jednako tretiranje svih građana.

Nažalost, ove i slične informacije čije je izravno prikupljanje zabranjeno moguće je pribaviti okolnim putem od kompanija koje se naizgled bave veoma različitim poslovima i uslugama, ali čiji je glavni posao zapravo prikupljanje informacija o građanima. Poslovni model nuđenja besplatnih usluga ili proizvoda zapravo sakriva bogatu zaradu od prodaje prikupljenih informacija o osobi, njenom kretanju i društvenim vezama, njenom ponašanju i njenom mišljenju.

1.2 Žele li korisnici privatnost?

Jedan od često isticanih argumenata protiv posebnih mjera zaštite privatnosti je da korisnici tvrtkama dobrovoljno stavljaju na raspolaganje svoje privatne podatke i tako zauzvrat dobivaju željene usluge ili proizvode. Činjenica je kako većina tvrtki koje na neki način prikupljaju informacije o korisnicima prethodno od njih ishode barem formalnu privolu, najčešće prihvaćanjem općih uvjeta usluge koju nude. Međutim, problem je u tome što velik broj korisnika nije na odgovarajući način upoznat sa sadržajem ugovora ili uvjeta koje prihvaćaju, tj. kako, tko i za što će koristiti njihove podatke.

Danas je teško pronaći proizvod ili uslugu koji su u potpunosti slobodni od dodatnih uvjeta i pravila, tako da su korisnici preopterećeni dugačkim pravnim tekstovima te redovito prihvaćaju uvjete bez da im posvete potrebnu pažnju ili uopće pročitaju. Industrija je toga vrlo svjesna i koristi ovakvo stanje da bi dodatno zbunila korisnike teško razumljivim sadržajem i poopćenim jezikom ugovora koji ne otkriva istinsku namjeru i način korištenja prikupljenih podataka. Izuzetno su rijetke kompanije koje korisnicima jasno objašnjavaju koji se sve podaci prikupljaju, u koju se svrhu koriste, kako se pohranjuju i kada se brišu.

Istinska zaštita ljudskih i građanskih prava zahtijevala bi jasno i nedvosmisleno upoznavanje korisnika s činjenicom da će se npr. njihovi zdravstveni podaci prodavati osiguravajućim kućama koje će na osnovu toga određivati cijenu police osiguranja ili da će se podaci o njihovim prihodima i prosječnoj potrošnji dijeliti s trgovcima koji će na osnovu toga određivati cijenu u Web trgovini kako bi maksimizirali svoj profit.

Osim što nisu primjereno upoznati sa sadržajem uvjeta na koje pristaju, korisnici su često stavljeni i u podređeni položaj zbog monopolističkog položaja neke kompanije na tržištu i zbog činjenice da gotovo sve kompanije postupaju vrlo slično. Prema slovu zakona korisnik je, doduše, slobodan odbiti uvjete i odreći se usluge, ali u stvarnom svijetu to bi značilo odbiti sve usluge na Internetu i odreći se tehnoloških dobara koja su danas postala nužna.

2 Narušavanje privatnosti na Internetu

Da su osobni podaci korisnika veoma dragocjeni i komercijalno vrijedni, dokazuje i činjenica da ogroman broj kompanija osobne podatke prikuplja i bez znanja ili barem formalne privole korisnika. Ovo poglavlje opisuje neke od najčešćih tehnika kojima se narušava privatnost korisnika Interneta. Svaka od ovih tehnika ograničena je u opsegu podataka koje može prikupiti, ali njihovom kombinacijom lako se stvara iznenađujuće detaljan profil korisnika. Prikupljene podatke kompanije razmjenjuju ili pak prodaju drugim kompanijama koje se bave agregiranjem podataka i izradom profila za daljnju prodaju.

2.1 Narušavanje privatnosti na Webu

Narušavanja privatnosti na Webu često se svode na to da podatke o korisnicima prikuplja treća strana, dakle ne vlasnik stranice. To znači da kada korisnik posjeti Web stranicu, u tom procesu treća strana (netko tko nije ni korisnik, ni Web stranica koju on posjećuje) prikuplja podatke o identitetu korisnika, o njegovim radnjama i slično. To na tehničkoj razini najčešće funkcionira tako da Web stranica koju korisnik posjećuje sadrži program (u jeziku JavaScript) ili cijelu Web pod-stranicu (kao HTML *iframe*) koji pripadaju nekoj trećoj strani. Slika 1 prikazuje primjer programskog koda za funkciju *Google Analytics* (označen crveno) uključenog u izvorni kod neke Web stranice.

```
413
414 </div>
415
416 <a href="#topNav3" class="skipper">preskoči na navigaciju</a>
417
418 <!--[if lt IE 7]>
419 <link rel='stylesheet' href='/img/themes/cn/usluge/ie6fix.css?1235833779' type='tex
420 <script type="text/javascript" src="/img/themes/cn/usluge/js/pngfix.js"></script>
421
422 <script type="text/javascript">window.addEvent('load', function(){ new pngFix(); })
423
424 <![endif]-->
425
426
427 <script>
428   (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
429   (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
430   m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
431   })(window,document,'script','//www.google-analytics.com/analytics.js','ga');
432
433   ga('create', 'UA-57662985-1', 'auto');
434   ga('send', 'pageview');
435 </script>
436
437
438
439 </body>
440 </html>
441
```

Slika 1 - Primjer *Google Analytics* JavaScript koda (označen crveno) uključenog u izvorni kod Web stranice

2.1.1 HTTP kolačići treće strane (eng. *third party cookies*)

HTTP kolačići koristan su mehanizam koji Web stranice koriste kako bi mogle zapamtiti prijavu svojih korisnika, spremiti njihove postavke i slično. HTTP kolačići treće strane su kolačići Web stranice čiji je JavaScript kod ili cijela Web pod-stranica uključena na Web stranicu koju korisnik posjećuje.

Kolačići treće strane mogu biti korisni primjerice ako neki članak na Web stranici omogućuje korisnicima da ostave komentar putem *Facebook* društvene mreže. Primjer takve funkcionalnosti prikazan je na slici 2. U tom slučaju, unutar Web stranice s člankom se nalazi ugrađena *Facebook* Web stranica s komentarima. Ona pomoću kolačića može identificirati korisnika ako je on prijavljen na *Facebook* i na taj način omogućiti mu da ostavi komentar u svoje ime.

Slika 2 - *Facebook* komentari na Web stranici

No zbog toga *Facebook* sada zna da je taj korisnik posjetio tu Web stranicu s člankom. *Facebook* to sazna čim se Web stranica učita – bez obzira na to je li korisnik ostavio komentar. Korisnici su više ili manje svjesni činjenice da *Facebook* i ostale društvene mreže prate svaki njihov korak unutar *Facebook* Web stranice, no manje je poznato da one prate i svaki njihov posjet drugim Web stranicama koje imaju mogućnosti komentiranja, dijeljenja i sličnih radnji preko *Facebooka*, odnosno drugih društvenih mreža.

Facebook komentari samo su jedan primjer korištenja HTTP kolačića treće strane kako bi se pratilo koje Web stranice korisnici posjećuju. Brojne druge usluge to rade, i što su raširenije, tj. na što više Web stranica su ugrađene, to je i njihovo znanje o korisniku veće. Uz društvene mreže, najčešće ovu tehniku koriste usluge Web oglasa, od kojih je *Google AdWords* vrlo vjerojatno najrašireniji.

2.1.2 Praćenje otiska Web preglednika (eng. *browser fingerprinting*)

Ova tehnika primarno se zasniva na uporabi JavaScript programskog koda kako bi se djelomično identificiralo posjetitelje Web stranice preko karakterističnih "otiska prsta" njihovih preglednika. Prilikom učitavanja stranice prikupljaju se podaci o vrsti i verziji Web preglednika, o veličini i dostupnoj razlučivosti ekrana, o podržanim fontovima sustava, HTTP zaglavljima te o raznim drugim detaljima koji zbrojeni mogu vrlo dobro identificirati računalo pojedinog korisnika. Jedna od usluga pomoću koje je moguće dobiti dojam o tome koliko ovi podaci zaista mogu jedinstveno identificirati korisnika je Panopticlick od *Electronic Frontier Foundation* grupe. Slika 3 prikazuje primjer rezultata dobivenih testiranjem otiska Web preglednika na *Panopticlick* usluzi.

Your browser fingerprint **appears to be unique** among the 840,266 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 19.68 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting here.

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
Limited supercookie test	0.4	1.32	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	11.14	2258.78	8c13f487c68166ee1cbd4dccb94fc460
Screen Size and Color Depth	5.31	39.55	1920x1200x24
Browser Plugin Details	9.41	680.38	Plugin 0: Chromium PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chromium PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf).
Time Zone	3.33	10.06	-60
DNT Header Enabled?	1.21	2.31	False
HTTP_ACCEPT Headers	17.36	168053.2	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.9,hr;q=0.8,bs;q=0.7
Hash of WebGL fingerprint	11.73	3388.17	01cc78cfa25bcb24a8f31b5cc4ea98b9
Language	0.91	1.88	en-US
System Fonts	13.93	15560.48	Andale Mono, Arial, Arial Black, Bitstream Vera Sans Mono, Calibri, Cambria, Comic Sans MS, Courier, Courier New, Georgia, Helvetica, Impact, MS Gothic, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.24	9.47	Linux x86_64
User Agent	12.5	5794.94	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/62.0.3202.89 Chrome/62.0.3202.89 Safari/537.36
Touch Support	0.58	1.49	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.19	1.14	Yes

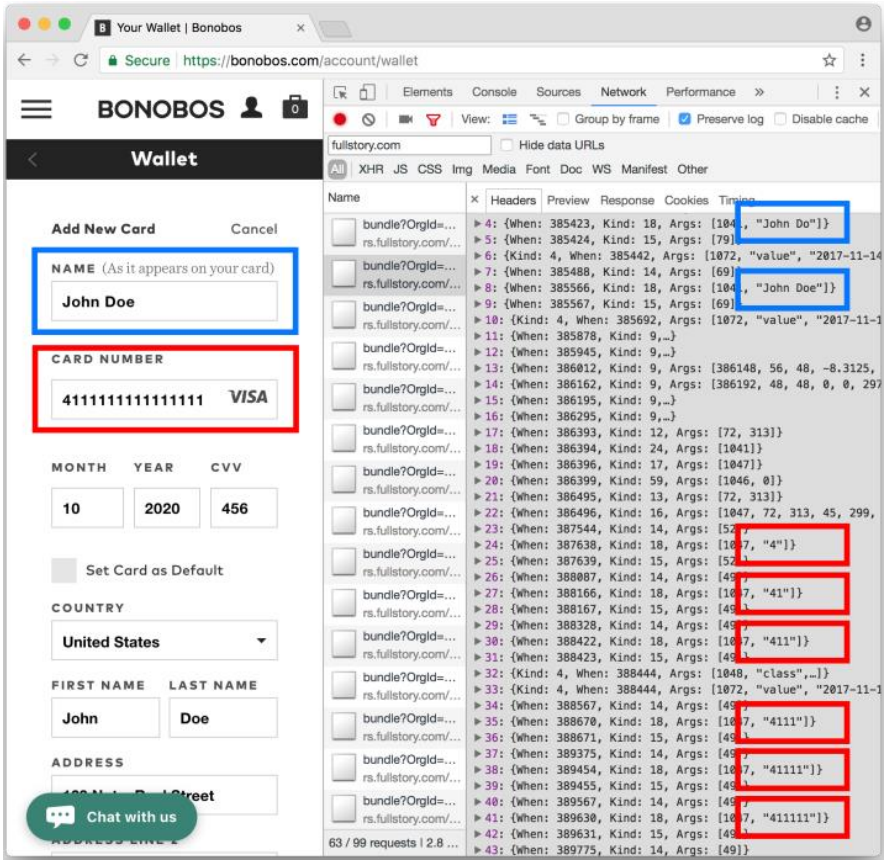
Slika 3 - Primjer rezultata *Panopticlick* usluge

Iako pravi identitet korisnika nije moguće na ovaj način izravno doznati, njega se ipak može jednoznačno povezati s određenim profilom koji će se naknadno popunjavati podacima koji nedostaju. Pomoću IP adrese moguće je geografski smjestiti korisnika u određeni grad ili državu, moguće je pratiti njegove navike i ponašanje na Internetu, a ako se na neku od Web stranica prijavi osobnim imenom, moguće je saznati i njegov pravi identitet.

2.1.3 Reprodukcija Web sjednice i detaljno praćenje korištenja stranice

Istraživanje Sveučilišta Princeton (1) pokazalo je da barem 482 od 50 000 najpopularnijih Web stranica prema rangiranju Alexa koriste skripte za reprodukciju Web sjednice. To znači da se na tim Web stranicama pomoću JavaScript koda snima sve što korisnik radi – uključujući svaku tipku koju pritisne na tipkovnici te svaki pokret i klik mišem. Kasnije, ili čak uživo dok korisnik koristi stranicu, moguće je u potpunosti prikazati kako je korisnikovo korištenje Web stranice izgledalo, odnosno kako ono trenutno izgleda.

Primjerice, korisnik želi obaviti kupovinu preko Interneta i krene upisivati broj svoje kreditne kartice na Web stranici. No, prije bilo kakvog slanja ili klika, korisnik se predomisli, izbriše broj kreditne kartice i ugasi tu Web stranicu. Korisnik možda misli da nije poslao nikakve podatke – no, pomoću skripta za reprodukciju sjednice, sve što je korisnik natipkao će biti poslano i snimljeno, neovisno o tome što je on to izbrisao umjesto slanja i ugasio Web stranicu. Izrazito je zabrinjavajuće to što ti podaci u pravilu nisu dostupni samo Web stranici koju korisnik posjeti, već se oni šalju **trećoj strani** – tvrtki koja pruža tu funkcionalnost reprodukcije sjednice. U ovom primjeru, unatoč tome što se korisnik predomislio i nije obavio kupovinu, broj njegove kreditne kartice poslan je i Web stranici i trećoj strani (tvrtki koja se bavi snimanjem reprodukcije sjednice). Slika 4 iz prethodno navedenog istraživanja Sveučilišta Princeton pokazuje prethodno opisani primjer na stvarnoj Web stranici – plavom bojom označeno je upisano i poslano ime korisnika, a crvenom broj njegove kreditne kartice.



Slika 4 - Snimanje kako korisnik upisuje ime (označeno plavo) i broj kreditne kartice (označeno crveno) prije njihovog eksplicitnog slanja (1)

Konkretno, isto vrijedi i za statuse na društvenoj mreži *Facebook* (korisnik krene upisivati status, no predomisli se i izbriše ga – sve što je natipkao je *Facebook* ipak zapisao) i za brojne Web stranice koje pružaju mogućnosti *chat*-a s djelatnikom (korisnička podrška): korisnik krene upisivati poruku, no predomisli se i ne pošalje ju – s druge strane, djelatnik je u potpunosti vidio sve što je korisnik tipkao, neovisno o tome što on poruku naizgled nije poslao.

Svrha prikupljanja svih podataka o tome kako korisnici koriste Web stranicu obično je unapređenje korisničkog iskustva, no neovisno o primarnoj svrsi, očito je kako takvi postupci predstavljaju izrazito veliku prijetnju privatnosti.

2.2 Narušavanje privatnosti elektroničke pošte

Elektronička pošta postala je de-facto standard komuniciranja, posebno u poslovnom svijetu. Korisnici imaju iluziju intimnosti i privatnosti. No, tehnologija na kojoj se ona zasniva stara je preko 40 godina i krajnje je podložna raznim oblicima zlouporabe, ali i korištenja na rubu legalnosti.

2.2.1 Privatnost adrese elektroničke pošte

Brojne usluge na Internetu reklamiraju se kao besplatne, uz zahtjev da se korisnik prvo registrira ili na neki drugi način ispuni obrazac s podacima o sebi. To često znači da ta usluga nije besplatna, već da ju korisnik zapravo plaća svojim podacima.

Korisnicima je u pravilu jasno da su oni te podatke predali toj usluzi, no često nisu svjesni da se ti podaci kasnije prodaju i dijele s trećim stranama. Jedan od podataka koji se često prodaje i dalje dijeli upravo je adresa elektroničke pošte. Te adrese tako dolaze u posjed raznim marketinškim tvrtkama te čak i organizacijama koje posluju izvan zakona. U konačnici, na ovaj način korisnici često završe kao odredište brojnih *spam* poruka i raznih prevara putem elektroničke pošte.

2.2.2 Slike za praćenje (eng. *tracking image*, *tracking pixel*…)

Jedan način narušavanja privatnosti u elektroničkoj pošti je korištenje slike za praćenje. Pošiljatelj može u poruku ugraditi sliku koju korisnik ne vidi, primjerice prozirnu sliku veličine jedne točke (eng. *pixel*). Ključno je razumjeti da se ta slika ne nalazi u prilogu (eng. *attachment*), već u tijelu same poruke koja je u pravilu tada u HTML formatu.

Sama slika ugrađena je tako da je u HTML kod poruke zapisana poveznica na vanjski resurs: datoteku na pošiljateljevom poslužitelju. Ta poveznica je jedinstvena, tj. napravljena je tako da ju je moguće jednoznačno povezati s porukom jer je različita za svakog primatelja poruke. S druge strane poveznice nalazi se poslužitelj koji, jednom kada netko zatraži taj resurs, zapisuje sve podatke kao što su IP adresa, vrijeme preuzimanja i ostali podaci vezani uz protokol preuzimanja (npr. HTTP zaglavlja).

Rezultat navedenoga je da kada korisnik otvori poruku, njegov program za elektroničku poštu vidi da se u poruci nalazi slika koja treba biti preuzeta sa zapisane poveznice. Zatim program preuzme tu sliku i na poslužitelju se zabilježe prethodno navedeni podaci. U konačnici, pošiljatelj pročita te podatke – primjerice, slika je preuzeta u 8 sati s IP adrese

198.51.100.4. To mu može reći da je korisnik poruku otvorio tada i s te IP adrese, uz sve ostale podatke koji su zapisani.

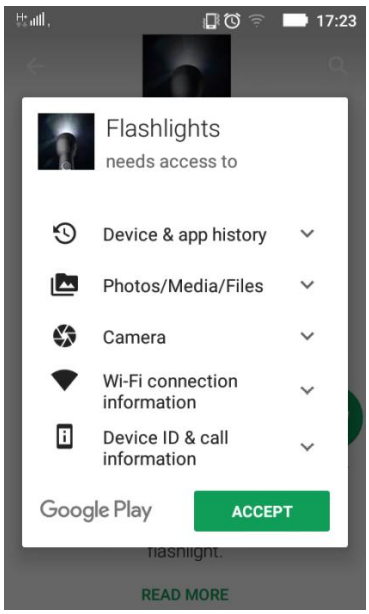
Slika 5 prikazuje odjeljak iz pravila o privatnosti (eng. *privacy policy*) usluge Pandora koji spominje kako oni i njihovi partneri koriste slike za praćenje.

Beacons and tracking pixels: Pandora, its third-party advertising partners, and tracking-utility partners employ a technology known as "beacons" or "tracking pixels" (each, a "**Beacon**"). A Beacon is a one-pixel-by-one-pixel clear image that is embedded in HTML content, and is about the size of a period at the end of a sentence. When HTML content containing a Beacon is rendered, the Beacon transmits anonymous information to a server, such as a numeric count, unique identifier, or IP address. Pandora and its partners use Beacons to help us better manage content on our Service. For example, we may place a Beacon in HTML-based emails to let us know which emails recipients have opened, or on a webpage to count the number of unique visitors to that page. The use of a Beacon may also allow us to gauge the effectiveness of certain communications and of our marketing campaigns.

Slika 5 - Dio pravila o privatnosti Pandora usluge koji spominje korištenje slika za praćenje

2.3 Narušavanje privatnosti kroz pametne telefone

Na pametnim telefonima, narušavanje privatnosti obično se odvija kroz aplikacije koje prikupljaju brojne podatke unatoč tome što oni nisu potrebni za njihovu funkcionalnost. Tipičan primjer su Android aplikacije koje omogućuju uključivanje bljeskalice/svjetiljke (eng. *flashlight*) i ništa drugo, no traže dozvole za pristup datotekama, lokaciji, pozivima itd. Primjer jedne takve aplikacije prikazan je na slici 6.

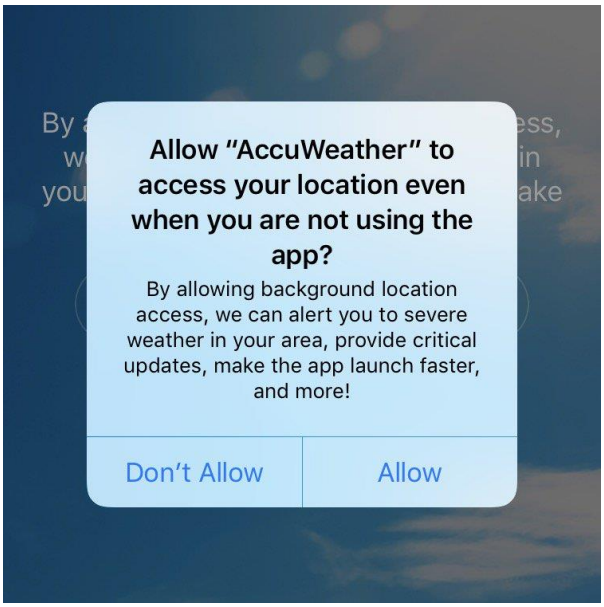


Slika 6 – Primjer aplikacije koja traži brojne dozvole nepovezane s njenom funkcionalnošću

Takve aplikacije zatim znaju prikupljati toliko podataka o korisniku da je to moguće nazvati špijuniranjem. Primjerice, aplikacija AccuWeather za iOS je između ostaloga prikupljala GPS koordinate korisnika te podatke o Wi-Fi mrežama i Bluetooth uređajima koji se nalaze u blizini (2). Zatim, te podatke prodavala je trećoj strani – tvrtki Reveal Mobile. Čak i kada su

korisnici zabranili aplikaciji da pristupa lokaciji uređaja (prikazano na slici 7), ona je i dalje prikupljala i slala informacije o svojoj Wi-Fi i Bluetooth okolini. No, tvrtka Reveal Mobile je pomoću tih podataka i dalje uspješno određivala (i unovčila) lokacije korisnika na barem dva načina.

Kao prvo, pomoću jedne od brojnih baza podataka s lokacijama Wi-Fi mreža, bilo je moguće locirati gdje se korisnik nalazi samo na temelju informacija o Wi-Fi mrežama iz njegove okoline. Kao drugo, pomoću Bluetootha je ponekad bilo moguće precizno odrediti gdje se korisnik nalazi – tvrtka Reveal Mobile izgradila je bazu lokacija velikog broja tzv. Bluetooth „svjetionika" (eng. *beacon*). To su uređaji koji se nalaze na raznim lokacijama i emitiraju Bluetooth signal. Kada se korisnik nađe u njihovoj blizini, pomoću aplikacije kao što je AccuWeather koja prisluškuje i šalje podatke o Bluetooth okolini, moguće je saznati njegovu lokaciju.



Slika 7 – Čak i kada su korisnici odbili pristup lokaciji (odabrali prikazani *Don't Allow*), podaci pomoću kojih je bilo moguće odrediti njihovu lokaciju su se ipak prikupljali i slali (2)

2.4 Narušavanje privatnosti mrežnog prometa

Korisnici rijetko razmišljaju o tome kojim putem prolazi njihov mrežni promet i tko ga sve vidi. Prirodno je očekivati da mrežne pakete koje korisnici šalju (koji prenose Web promet, promet elektroničke pošte i slično) može pročitati samo korisnik i krajnji primatelj, no to u velikom broju slučajeva nije istina.

U prvom redu, sav mrežni promet odvija se kroz infrastrukturu koju postavlja i kontrolira pružatelj mrežnih usluga. Kako bi mogao obavljati svoju glavnu ulogu – pružanje pristupa Internetu usmjeravanjem korisnikovih odlaznih i dolaznih paketa, pružatelj mrežnih usluga mora pročitati određeni dio informacija sadržanih u tim paketima. Čak i ako korisnik koristi zaštićene protokole kao što je primjerice HTTPS, pružatelj mrežnih usluga iz dostupnih metapodataka može rekonstruirati mnoge informacije o korisnikovom korištenju Interneta i sagraditi vrlo precizan profil o njegovim navikama, Web stranicama koje posjećuje i sl.

Osim pružatelja mrežnih usluga, promet su na isti način u mogućnosti prisluškivati i svi ostali vlasnici mrežnih veza i pristupnih točaka duž cijelog puta između korisnika i njegovog sugovornika, u što svakako spadaju i vlasnici Wi-Fi pristupnih točaka.

U drugome redu, i manje poznato korisnicima, mrežni promet mogu prisluškivati i svi ostali korisnici spojeni na istu Wi-Fi mrežu. Za razliku od žične komunikacije koja zahtjeva fizički pristup mrežnom priključku, paketi u bežičnoj komunikaciji vidljivi su svakome tko se nalazi u dosegu pristupne točke. Pri tome, prisluškivač ne mora niti biti prijavljen u mrežu. Radi bolje zaštite paketi su šifrirani, ali ako se ne koristi neki od *enterprise* načina rada, svatko tko zna šifru može u pravilu njome dešifrirati sav promet. Zbog ovoga, na javnim Wi-Fi mrežama (kafići, zračne luke i sl.), potrebno je izbjegavati korištenje nezaštićenih mrežnih protokola kao što su HTTP, SMTP i DNS te pri razmjeni osjetljivih informacija obavezno koristiti dodatnu zaštitu kao što je VPN.

Osim prisluškivanja samog sadržaja mrežnih paketa, brojne osobne informacije dostupne su već i pasivnim slušanjem prometa. U nastojanju da korisniku olakšaju spajanje na Wi-Fi mreže, i laptopi i pametni telefoni neprestano oglašavaju popis zapamćenih mreža tj. kad god nisu spojeni na bežičnu mrežu, pokušavaju pronaći neku od prethodno zapamćenih mreža. Već iz samih imena ovih zapamćenih mreža moguće je saznati koja je mjesta korisnik posjetio i na kojima se često zadržava (Wi-Fi mreže kafića, restorana, knjižnica, javnog prijevoza, radnog mjesta). Uz pomoć baza podataka o lokacijama Wi-Fi pristupnih točaka moguće je i rekonstruirati kretanje korisnika po svijetu tj. znati koja je mjesta posjetio (ili barem koja je posjetio njegov uređaj).

Informacije o prethodno zapamćenim Wi-Fi mrežama ne predstavljaju samo narušavanje privatnosti nego i otvaraju vrata ozbiljnijim hakerskim napadima. Jednom kada zna koju Wi-Fi mrežu korisnikov uređaj očekuje, napadač može postaviti posebno podešen uređaj koji se lažno predstavlja upravo kao tražena mreža i automatski povezuje korisnika na sebe. U tom trenutku napadač postaje vlasnik korisnikove pristupne točke te ima puni uvid u mrežne pakete kao što je već opisano za pružatelje mrežnih usluga i vlasnike mrežne infrastrukture.

Sličnu priliku za napad pruža i Bluetooth modul ako je podešen tako da bude stalno vidljiv ostalim uređajima. Informacija o nazivu Bluetooth uređaja koji se očekuje za uparivanje otvara vrata napadaču koji simuliranjem tog uređaja može ostvariti neovlašteni pristup i omogućiti si daljnje napade.

3 Kako se zaštititi

3.1 Razumijevanje rizika

Briga o privatnosti na Internetu prije svega je odgovornost samog korisnika a razumijevanje rizika kojima je privatnost izložena uporabom Interneta prvi je korak u njenoj zaštiti. Danas prevladavajući poslovni model pružanja "besplatnih" usluga u razmjenu za osobne informacije o korisniku čini gotovo nemogućim u potpunosti sačuvati privatnost, a bez da se istovremeno drastično ne ograniči upotreba Interneta te dobrobiti najrazvijenijih i najpopularnijih platformi i usluga. Usprkos tome, poznavanje navedenih rizika te upotrebom nekih jednostavnih alata i tehnika zaštite korisnik ima mogućnost informiranog izbora usluga s kojima želi dijeliti svoje osobne podatke te može biti oprezniji i izbjeći nenamjerno i neželjeno ugrožavanje svoje privatnosti.

3.2 Ispravno podešavanje postavki postojećih alata

Svi standardni internetski alati i operativni sustavi predviđaju razne postavke kojima se upotreba Interneta može učiniti sigurnijom. Kao prvi korak zaštite privatnosti dobro je upoznati se s konkretnim mogućnostima korištenih alata i prilagoditi ih željenoj razini zaštite. Predviđene vrijednosti ovih postavki u pravilu su takve da osiguraju što veću kompatibilnost i ispravnu funkcionalnost svih postojećih tehnologija kojima se Web stranice služe, ali na štetu privatnosti korisnika.

U Web pregledniku moguće je na globalnoj razini onemogućiti upotrebu kolačića trećih strana (eng. *third party cookies*) čime se uklanja rizik od praćenja korisnika na ovaj način. Onemogućavanjem kolačića neće više ispravno raditi neke od značajki koje se na njih oslanjaju, kao što su Facebook komentari, tako da je na korisniku da izabere između privatnosti te lakoće uporabe i pune funkcionalnosti.

U alatima za elektroničku poštu moguće je isključiti automatsko učitavanje i prikazivanje slika i ostalih objekata s udaljenih lokacija. Slike uključene u samu poruku normalno će se prikazati, ali neće biti dozvoljeno spajanje na udaljeni poslužitelj u trenutku čitanja poruke i praćenje korisnika na ovaj način. Zbog vrlo čestog iskorištavanja ovih metoda u maliciozne svrhe, svi popularni alati tvornički su podešeni da onemoguće automatsko prikazivanje udaljenih sadržaja, međutim ove postavke moguće je dodatno postrožiti i prilagoditi.

Na pametnim telefonima dobra je praksa ograničiti se samo na upotrebu provjerenih i pouzdanih aplikacija. Iako sve renomirane trgovine aplikacijama redovito provjeravaju sadržaj aplikacija koje nude, brojni su primjeri zlonamjernih aplikacija koje su mjesecima uspijevale sakriti svoje prave namjere i izbjeći izbacivanje iz trgovine. Jednako tako, kriteriji za odobravanje aplikacija vrlo su labavi po pitanju sigurnosti tako da ni službeno odobrenje nije garancija prave sigurnosti aplikacije. Novije verzije operativnih sustava pametnih telefona sve više dozvoljavaju selektivno dodjeljivanje ovlasti pojedinim aplikacijama tako da je vrlo dobra praksa provjeriti točan popis ovlasti koje pojedina aplikacija zahtjeva te isključiti one ovlasti koje joj nisu nužno potrebne.

3.3 Korištenje dodatnih alata za zaštitu privatnosti

Uz prilagođavanje postavki standardnih alata, privatnost je uputno dodatno zaštititi i upotrebom posebnih alata za tu namjenu. Izbor je širok i pokriva sve aspekte upotrebe Interneta, a većina ovih alata je i besplatna za korištenje.

Kao najčešće korišteni alat u radu s Internetom, Web preglednik je najveći rizik privatnosti korisnika. Zbog toga su razvijeni brojni dodaci za Web preglednike koji uvelike povećavaju razinu zaštite.

3.3.1 uBlock Origin

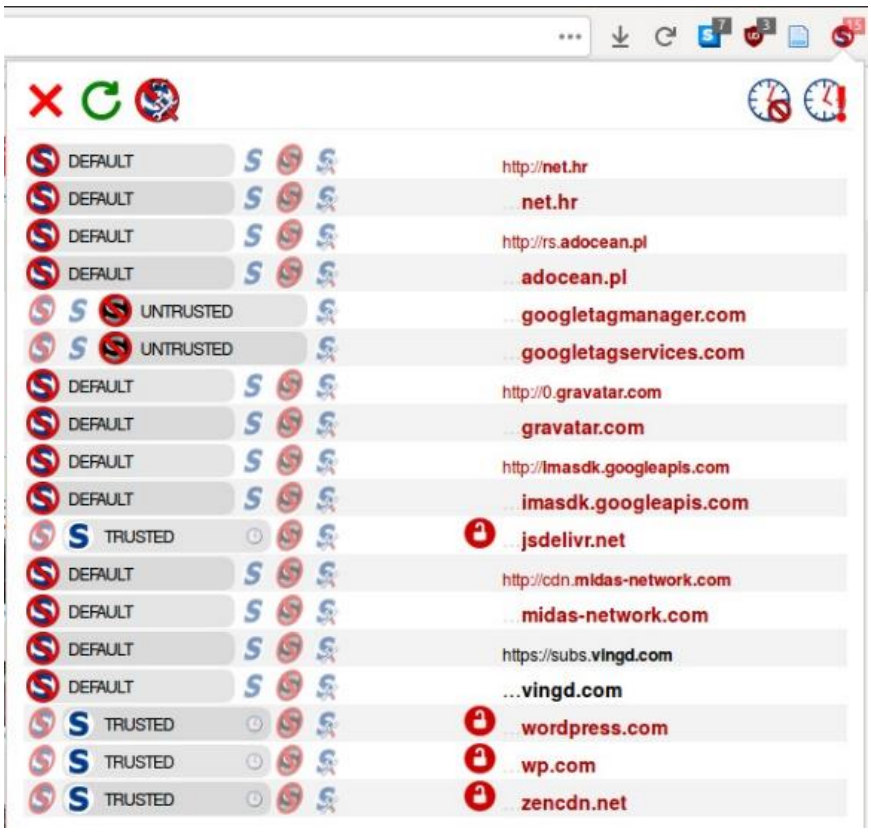
Među brojnim alatima za blokiranje sadržaja, uBlock Origin izdvaja se činjenicom da se radi o softveru otvorenog koda vrlo malenih zahtjeva za resursima. Nudi detaljne mogućnosti podešavanja razine zaštite i blokiranje raznih vrsta mrežnog prometa. Tvornički je postavljen da blokira web oglase, skripte za praćenje korisnika te web adrese koje su poznati izvori zlonamjernih programa.

Slika 8 – Skočni prozor alata uBlock Origin prikazuje broj blokiranih zahtjeva i domena povezanih s trenutnom web stranicom

3.3.2 NoScript

Ovaj dodatak namijenjen preglednicima iz Mozilla obitelji sprječava izvršavanje Web sadržaja kao što je JavaScript, Java, Flash i Silverlight osim ako je korisnik prethodno odobrio domenu na kojoj se nalaze dodavši je na popis dozvoljenih domena. Pristup "bijele liste" tj. prihvaćanje samo unaprijed odobrenih domena izvrsna je zaštita od velikog broja napada,

ali zahtjeva nešto veće znanje i angažman korisnika jer uz tvorničke postavke veliki broj Web stranica neće u potpunosti ispravno funkcionirati.

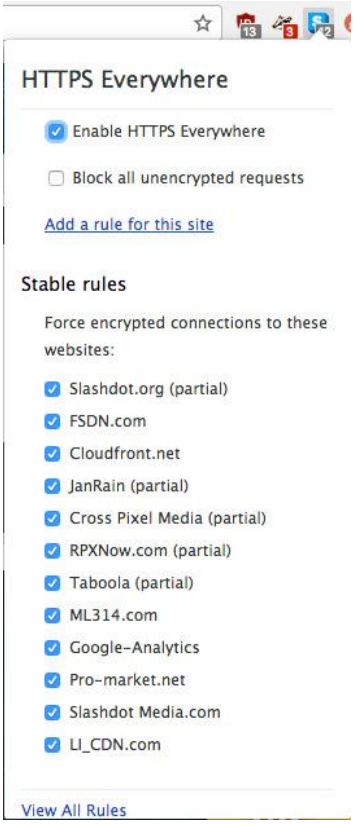


Slika 9 – Skočni prozor alata NoScript zorno prikazuje blokirane skripte za praćenje i domene trećih strana povezane s trenutnom web stranicom

3.3.3 HTTPS Everywhere

Kao što mu i sam naziv govori (prevedeno na hrv. „HTTPS svuda“), ovaj dodatak za Web preglednik pokušava postići uporabu sigurnog HTTPS protokola gdje god je to moguće. Ako

Web stranica koristi i HTTP i HTTPS protokol, ovaj dodatak će na pametan način presresti sve HTTP zahtjeve i zamijeniti ih njihovom HTTPS verzijom.



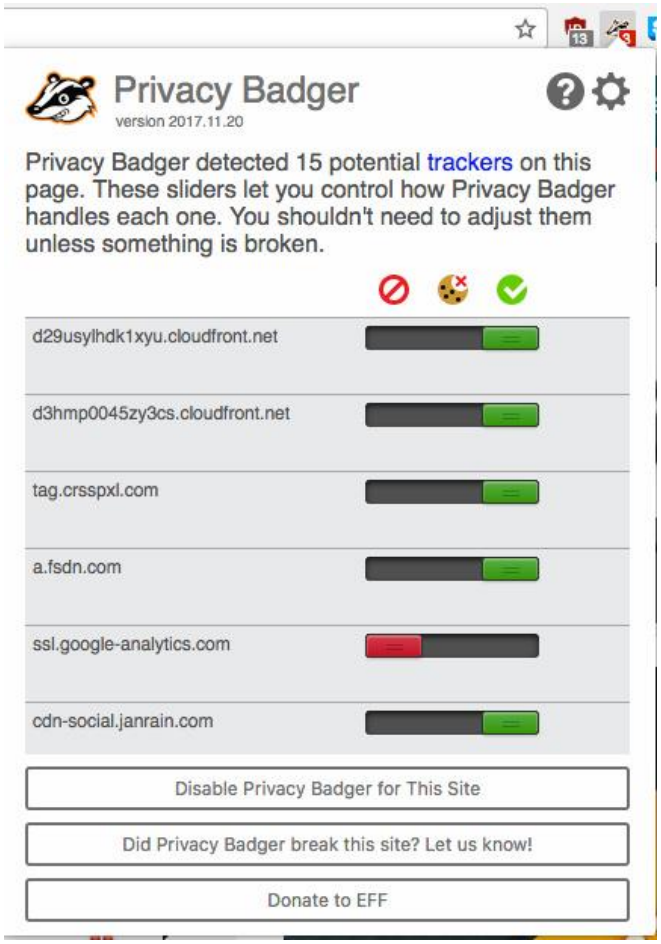
Slika 10 – Skočni prozor alata HTTPS Everywhere

3.3.4 Privacy Badger

Ovaj je alat nastao iz želje da se u jednom alatu objedine sve najbitnije metode zaštite kako bi korisnici jednim jednostavnim alatom mogli postići željenu razinu privatnosti. Druga misao vodilja bila je izbjeći potrebu za kompliciranim podešavanjem postavki i korisnikovim angažmanom, prepustivši odluku o tome što treba blokirati samom alatu. U svojoj osnovi, Privacy Badger prati s kojih sve domena dolazi sadržaj neke stranice koja se prikazuje korisniku. Kada otkrije da neki od izvora sadržaja prati korisnika i kada on posjeti druge Web

stranice, Privacy Badger u potpunosti blokira tu domenu i onemogućuje joj praćenje korisnika.

Iako nije prvenstveno zamišljen kao alat za blokiranje oglasa, zbog činjenice da većinu sadržaja za praćenja čine upravo oglasi i da ako vi vidite oglas istovremeno i oglas "vidi" vas i prati vas, većina oglasa će upotrebom Privacy Badger alata biti uklonjena.



Slika 11 – Skočni prozor alata Privacy Badger pregledno prikazuje popis trećih strana s kojima Web stranica komunicira te omogućava laku prilagodbu zaštite privatnosti za svaku od povezanih domena

3.3.5 Mailvelope

Mailvelope je dodatak za Web preglednik koji omogućuje laku integraciju PGP šifriranja u Web servise elektroničke pošte kao što su GMail, Yahoo i Outlook.com. Ako se ovim servisima pristupa preko Web preglednika, Mailvelope će uz postojeće gumbe za slanje pošte jednostavno dodati i svoje kontrole za sigurno slanje te će se pobrinuti za šifriranje i dešifriranje poruka bez potrebe za kopiranjem teksta ili dodatnim trudom korisnika.

3.3.6 Firefox Focus

Za zaštitu privatnosti pri surfanju mobilnim uređajima moguće je koristiti posebno prilagođeni preglednik Firefox Focus. Radi se o pregledniku tvornički podešenom za

blokiranje praćenja korisnika i uz pojednostavljene kontrole za zaštitu privatnosti kao što su brisanje povijesti pretraživanja i brisanje pohranjenih kolačića.

3.3.7 Signal Private Messenger

Među svim aplikacijama i platformama za slanje poruka, svojom orijentiranošću na sigurnost i privatnost posebno se ističe Signal Private Messenger. Temeljen je na sigurnom komunikacijskom protokolu koji omogućuje šifriranje s kraja na kraj (eng. *end to end encryption*), čime se onemogućuje čitanje sadržaja paketa trećim stranama. Isti ovaj protokol preuzela je i aplikacija WhatsApp, ali ona, za razliku od Signal Private Messengera, nije softver otvorenog koda te nije moguće neovisnom analizom dokazati potpunu zaštitu privatnosti i isključiti mogućnost prisluškivanja.

3.3.8 Tor Browser

Tor Browser je moćan alat za anonimno i privatno pregledavanje Weba i Tor sakrivenih servisa. Mrežni promet Tor Browsera prolazi kroz Tor mrežu anonimnosti, gdje je tehnikom slojevitog usmjeravanja sadržaj mrežnog prometa zaštićen, a njegov mrežni put prikriven.

Tor Browser ima velik broj raznolikih korisnika i dostupan je svima. Za njegovo korištenje potrebno je samo računalo, veza na Internet i slobodno dostupni alati. Građani zemalja u kojima država regulira sadržaj mrežnog prometa mogu koristiti Tor Browser kako bi anonimno i privatno pregledavali Web i zaobišli cenzure.

3.4 Virtual Private Network (VPN)

VPN je tehnologija kojom se rad privatnih mreža, kao što su interne poslovne mreže neke kompanije, omogućava i kada se promet djelomično prenosi i javnim mrežama ili Internetom. Između dvije točke u VPN vezi stvara se virtualni tunel u kojem je sva komunikacija šifrirana i nerazumljiva trećim stranama koje bi je mogle presresti na javnim mrežama.

Budući da na javnim, a pogotovo na javnim bežičnim mrežama nije moguće spriječiti prisluškivanje mrežnih paketa, potrebno je uporabom VPN-a pakete učiniti nerazumljivima trećim stranama. Na ovaj način moguće je koristiti povjerljive usluge poput Internet bankarstva čak i na Wi-Fi mreži na ulici, kafiću ili u zračnoj luci.

Svi mrežni paketi pri korištenju VPN veze usmjereni su prema VPN poslužitelju tako da osim što ne mogu pročitati sadržaj paketa, treće strane ne mogu saznati niti krajnjeg primatelja paketa. Korištenjem VPN-a moguće je vrlo dobro zaštititi privatnost od pružatelja mrežnih usluga, a korištenjem nekog od široko popularnih VPN usluga postiže se i određena doza anonimnosti jer se promet stapa s prometom velikog broja ostalih korisnika. Međutim, treba imati na umu da se prava zaštita privatnosti ne može osigurati ako VPN poslužitelj nije pod našom kontrolom jer se zaobilaženjem pružatelja mrežnih usluga problem samo prebacuje na pružatelja usluga VPN pristupa, koji sada dolazi u mogućnost potpunog nadzora korisnika jer postaje *de-facto* vlasnik korisnikove mrežne infrastrukture.

3.5 Privremene adrese elektroničke pošte

Sve je više Web stranica i usluga koje pristup sadržaju uvjetuju davanjem adrese elektroničke pošte korisnika. Kako bi se spriječilo narušavanje privatnosti i mogućnost prodaje adrese pošiljateljima neželjene pošte, moguće je koristiti se jednom od brojnih usluga privremene elektroničke pošte.

Servisi kao što su „10 minute mail" (prevedeno na hrv. „pošta od 10 minuta") dopuštaju kreiranje privremene adrese elektroničke pošte koja traje samo 10 minuta, nakon čega se briše – dovoljno za potvrdu registracije i pristup željenoj Web stranici.

Za one kojima je potrebna trajnija adresa pošte, ali koja će u potpunosti štititi njihovu anonimnost, postoje i usluge anonimne pošte kao što su GuerrillaMail, Secure Mail, The Anonymous Email i slični.

4 Zaključak

Privatnost na Internetu ozbiljna je tema koja zaslužuje pažnju svakog korisnika. Usprkos trendovima neprestane online prisutnosti i dobrovoljnog dijeljenja intimnih informacija sa širokom publikom društvenih mreža, pravo na privatnost ostaje temeljno i nepovredivo pravo svake osobe. Svaki korisnik ima pravo odlučiti koje informacije želi, a koje ne želi podijeliti te ima pravo odabrati s kime ih želi dijeliti.

Nažalost, ovo se pravo osobnog izbora često u praksi zanemaruje i zaobilazi navodeći korisnika da pristane na poopćene i loše definirane korisničke uvjete ili jednostavno prisiljavajući korisnike na izbor između odricanja od privatnosti ili odricanja od smislene uporabe Interneta. Veliki pozitivni pomaci čine se na europskoj razini donošenjem regulative koje jasno definira obaveze svih organizacija koje prikupljaju ili pohranjuju osobne podatke korisnika jednako kao i prava korisnika kao što su pravo na pristup podacima koje organizacija posjeduje o korisniku i pravo na brisanje osobnih podataka. Usprkos tome, odgovornost za zaštitu osobne privatnosti prije svega je na samom korisniku.

Budući da je preduvjet zaštite privatnosti poznavanje metoda i načina na koji se ona ugrožava, ovaj je dokument ukratko predstavio najvažnije ugroze privatnosti kojima su izloženi tipični korisnici Interneta. Poznajući ove opasnosti, korisnik može mijenjati svoje ponašanje na Internetu i prilagoditi ga željenoj razini zaštite privatnosti.

Da bi se zaštitila privatnost, a omogućilo normalno korištenje Interneta, osim povećane pažnje korisnika potrebne su i aktivne mjere zaštite. Dokument predstavlja odabir učinkovitih i pristupačnih alata kojima se uvelike podiže razina zaštite, a ne narušava se lakoća korištenja.

Bez potrebe za velikim predznanjem, prosječni korisnik uz stalnu pažnju i trud da podesi svoje uređaje i primijeni sredstava zaštite može postići vrlo visok stupanj privatnosti.

5 Literatura

1. **Englehardt, Steven.** No boundaries: Exfiltration of personal data by session-replay scripts. *Freedom to Tinker.* [Mrežno] 15. studeni 2017. [Citirano: 24. studeni 2017.] https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
2. **Strafach, Will.** Advisory: AccuWeather iOS app sends location information to data monetization firm. *Hacker Noon.* [Mrežno] 21. kolovoz 2017. [Citirano: 24. studeni 2017.] https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870.
3. **Matsakis, Louise.** Nearly Half of the Most Popular Websites Use the Same Software to Track You Around the Internet. *Motherboard.* [Mrežno] 10. srpanj 2017. [Citirano: 24. studeni 2017.] https://motherboard.vice.com/en_us/article/padge9/nearly-half-of-the-most-popular-websites-use-the-same-software-to-track-you-around-the-internet.
4. **Netsafe.** How to improve your online privacy and security. [Mrežno] 8. ožujak 2016. [Citirano: 24. studeni 2017.] How to improve your online privacy and security.
5. **Lifehacker.** Fact and Fiction: The Truth About Browser Cookies. [Mrežno] 1. veljača 2010. [Citirano: 24. studeni 2017.] https://lifehacker.com/5461114/fact-and-fiction-the-truth-about-browser-cookies.
6. **Greger, Sebastian.** Privacy-Aware Design: Replacing Google Analytics with a decentralized alternative. *sebastiangreger.net.* [Mrežno] 28. veljača 2014. [Citirano: 24. studeni 2017.] https://sebastiangreger.net/2014/02/privacy-aware-design-replacing-google-analytics/.