Praćenje korisnika na webu

Petra, Tetec

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Petra Tetec

PRAĆENJE KORISNIKA NA WEBU

ZAVRŠNI RAD

Varaždin, 2018.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Petra Tetec

Matični broj: 44286/15–R

Studij: Primjena informacijske tehnologije u poslovanju

PRAĆENJE KORISNIKA NA WEBU

ZAVRŠNI RAD

Mentorica:

Doc. dr. sc. Iva Gregurec

Varaždin, rujan 2018.

Petra Tetec

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristila drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autorica potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

U radu se istražuje i analizira proces praćenja korisnika na webu u svrhu unaprjeđenja poslovanja i poboljšanja korisničkog iskustva, uz mnogobrojne sigurnosne prijetnje koje ono sa sobom nosi. Izlaže se motivacija za praćenje korisnika, predstavlja se uvid u mehanizme za skupljanje podataka, navodi se legalni okvir unutar kojeg se praćenje korisnika mora zadržati kako se ne bi povrijedila korisnička privatnost, te se izlažu sigurnosne mjere koje svaki običan korisnik može poduzeti u svrhu povećanja vlastite sigurnosti. Generalno se kroz rad pokušava osvijestiti čitatelja o tragu koji ostavlja za sobom na webu te mu predložiti načine za zaštitu vlastite privatnosti.

Ključne riječi: web, CRM, praćenje korisnika, marketing, privatnost, sigurnost, društvene mreže

Sadržaj

Uvod

Kad se smišljao i dizajnirao koncept Interneta, bilo je teško zamislivo da će se koristiti za sve za što se koristi danas. U svojim je počecima on korisnicima služio za pronalaženje osnovnih informacija o pojedinoj temi, no s vremenom je globalno povezana mreža počela postajati čvrsta baza za puno više od toga. Vrijeme potrebno za prijenos podataka počelo je padati obrnuto proporcionalno od količine podataka koja se prenosila, mogućnosti pristupa mreži konstantno su se širile, te je broj korisnika svakim danom sve više rastao. Komunikacijski potencijal Interneta počeo se ostvarivati pružanjem usluga elektroničke pošte, chatova, prijenosom zvuka, prijenosom videa i dr., te uskoro više nije bio ograničen samo na komunikaciju između pojedinih korisnika, već su se s njima počela povezivati i razna poduzeća.

Stvarajući time stratešku prednost pred konkurencijom, danas gotovo više ne postoji poduzeće koje nema web-stranicu i ne koristi mogućnosti weba za vlastitu promociju, komunikaciju s korisnicima, pružanje kanala prodaje, dodatnih mogućnosti prodaje ili kao isključivi kanal pružanja svojih usluga tržištu. Kako bi, pak, pružatelji usluga znali kako funkcionira tržište, za kojim proizvodima/uslugama raste i pada potražnja, što u njihovom poslovanju ili poslovanju konkurencije privlači kupce, što je zajedničko njihovim klijentima, a po čemu se oni razlikuju te mnogo drugih odgovora na pitanja ključnih za njihov razvoj, web ne koriste samo za jednosmjeran odnos prema korisnicima. Razne organizacije skupljaju podatke o korisnicima te ih koriste za analiziranje korisničkih stavova, ponašanja i navika prema kojima donose prognoze za poslovanje, mijenjaju pojedine aspekte u svom radu, stvaraju nove proizvode/usluge i strategije za njihovu prodaju i sl. Ovakav se odnos može shvatiti kao prodaja osobnih podataka u razmjenu za dobra koja tržište nudi, a podaci o korisnicima sve češće predstavljaju najvrjedniju imovinu društvenih mreža i raznih web-servisa.

U radu se daje konceptualni i tehnološki uvid u praćenje korisnikovog digitalnog traga. U prvom se poglavlju predstavlja motivacija za skupljanje i obradu korisničkih podataka u kontekstu novih marketinških strategija i CRM-a. U drugom poglavlju opisuju se glavne skupine mehanizama za implementaciju praćenja. U trećem poglavlju izloženo je korisnikovo pravo na vlastitu privatnost te primjeri njegovog kršenja u slučaju najveće društvene mreže te najmoćnije sigurnosne agencije na svijetu. U četvrtom poglavlju autorica predlaže pouzdane metode i generalne savjete za očuvanje osobne privatnosti i sigurnosti, a na kraju je izveden zaključak iz napisanog rada.

1. Suvremeni marketing i CRM

Danas je teško zamisliti uspješnu kompaniju koja posluje bilo na globalnoj, bilo na maloj lokalnoj skali, a koja posluje bez provođenja marketinških aktivnosti. Teško je zamisliti koliko daleko u povijest oglašavanje seže – od glasnih prodavača na tržnici koji su ljudima željeli ponuditi svoje proizvode sve otkad tržnice postoje, preko ručno pisanih i dijeljenih letaka, preko prvih novina s oglasima, izuma radija i televizije pa sve do pojave Interneta, koji je pružio novi potencijal za oglašavanje, odnosno postao novi marketinški kanal. Međutim, postoji ogromna razlika između oglašavanja preko internetskog/mobilnog oglašavanja i svih drugih kanala – plakati na javnim površinama, oglasi u novinama, reklame na televiziji i radiju za sve su ljude jednaki, a web je sofisticiran, interaktivan medij koji dopušta, pa čak i nameće korisniku prilagođenu ponudu proizvoda i usluga.

Prvi je korak prilagođavanju tržišne ponude istraživanje tržišta. Konvencionalni načini tako su uključivali prikupljanje statističkih podataka o prodanim proizvodima, trendovima na tržištu i drugim bitnim faktorima uspješnosti prodaje, te s druge strane podatke o kupcima koje su oni sami bili voljni dati (provođenjem anketa, upitnika i drugih metoda ispitivanja). Uz konstantan i nagao razvoj tehnologije, više nije potrebno računati na iskrenost i strpljenje pojedinaca koji čine tržište, već se razni podaci o njima prikupljaju i pohranjuju u baze podataka na automatizirane načine. Tako danas velik dio poslovnih subjekata prikuplja podatke o tržištu ili dijelu tržišta na kojem posluje, no ne raspolaže uvijek s njima na pravilan, konstruktivan način. Problem može ležati u raznim aspektima, no najčešće je u tome što se podaci visoke vrijednosti ne iskorištavaju na pravilan način ili se iskorištavaju samo djelomično. Osim toga, često se događa da poslovni subjekti troše previše resursa na podatke od kojih nemaju nikakve koristi, a da toga nisu uvijek ni svjesni. [1, str. 1-4]

1.1. CRM kao strategija za restrukturiranje marketinških aktivnosti

Često se kaže kako je polovica novca uložena u promidžbu uzalud bačena. Ovo se događa kod provođenja masovnog marketinga koji se na jednak način odnosi prema čitavom tržištu. Pojedinci koji čine tržište vrlo su različiti i logično je da ne zanimaju svakog jednake stvari, niti sve zanima svakog u jednakoj mjeri. Kako bi se otkrilo koja je „polovica novca“ neučinkovito iskorištena te kako bi se drukčije rasporedili resursi, potrebno je upravljati

odnosima s klijentima, što se provodi kroz koncept poznat kao CRM. CRM (*Customer Relationship Management*) je poslovna strategija za optimizaciju ulaganja i prihoda poslovnog subjekta te poboljšavanje zadovoljstva klijenata, fokusirajući se pritom na prilagođavanje odnosa prema pojedinim tržišnim segmentima, a sve uz korištenje informacijske tehnologije. [1, str. 1-4] Ovaj koncept uključuje operativni dio koji se bavi automatizacijom i optimiziranjem prodajnih aktivnosti te integriranjem poslovnih aktivnosti iz različitih sektora, zatim kolaborativni dio koji se fokusira na kontakt prodavača i kupca te prikupljanje podataka o tržištu, te na kraju analitički dio koji je zadužen za obradu podataka prikupljenih iz različitih izvora radi utvrđivanja vrijednost klijenata i pružanja podrške poslovnim procesima. [1, str. 87-89]

CRM zahtijeva skupljanje pouzdanih i relevantnih podataka o pojedincima, da bi se oni mogli iskoristiti u korist poslovanja. No osim prikupljanja, podatke je potrebno i organizirati na smislen način jer, osim što se može dogoditi da nisu svi pohranjeni na jednom mjestu, da su nepotpuni ili međusobno nekompatibilni, da nisu ažurni ili da ih ima toliko da se na rezultat SQL upita treba čekati satima, u svom sirovom obliku oni nemaju nikakvu konkretnu vrijednost za poslovanje. Tehnološki dio rješenja ove problematike nalazi se u strukturiranju akumuliranih podataka iz baza u skladišta, čime se podaci pretvaraju u informacije koje se mogu analizirati te iskoristiti u poslovanju bez nepotrebnog trošenja vremena i materijalnih resursa. [1, str. 21-23]

1.2. Rudarenje podataka

Konceptualna struktura CRM-a obuhvaća tri glavne komponente: rudarenje podataka, marketing baza podataka i izravni marketing. Rudarenje podataka (*data mining*) podrazumijeva akumuliranje podataka o pojedincima koji djeluju na tržištu na različite načine, bilo to vlastitim izravnim dolaženjem do njih kroz obavljanje poslovnih aktivnosti, bilo njihovom kupnjom, posuđivanjem, unajmljivanjem ili nekim drugim oblikom razmjene. Ove aktivnosti predstavljaju temelj na kojem se dalje grade reformirane marketinške aktivnosti upravljanja odnosa s kupcima, te prema tome uglavnom predstavljaju operativni dio djelatnosti CRM-a. [1, str. 2-3]

1.3. Marketing baze podataka

Druga komponenta, marketing baze podataka (*database marketing*), obuhvaća aktivnosti usmjerene izgrađivanju kvalitetnog odnosa s kupcima, što podrazumijeva poboljšavanje obostrane komunikacije i optimiziranje transakcija na korist obje strane – poslovni subjekt minimizira troškove i vraća uložena sredstva, dok kupac/klijent dobiva prilagođenu ponudu. Ovaj se koncept fokusira na personalizaciju marketinškog programa pojedincima ili skupinama pojedinaca, što se ostvaruje pravilnim iskorištavanjem prikupljenih strukturiranih podataka o tržištu, što čini ove djelatnosti analitičkim dijelom implementacije CRM koncepta. [1, str. 2-3]

Kao i kod klasičnih starijih strategija, za provođenje aktivnosti promocije kod mobilnog i Internet-marketinga potrebno je napraviti segmentaciju tržišta. Marketinška je segmentacija svrstavanje pojedinaca na tržištu unutar definiranih skupina, ovisno o tome koje uvjete zadovoljavaju. Kriteriji za kategorizaciju kupaca mogu biti geografski, demografski, psihološki, bihevioralni i razni drugi, ovisno o potrebama onog koji provodi segmentaciju. Idealan segment trebao bi zadovoljavati određene uvjete – jasno određene granice, obujam koji opravdava odvajanje dotične skupine ljudi, značajan prodajni potencijal, mogućnost modificiranja navika pojedinaca unutar segmenta u nekoj mjeri te mogućnost kvantitativnog određivanja učinkovitosti primijenjene strategije. [1, str. 143] Ovaj postupak nikad nije jednostavan jer zahtijeva razmatranje mnogih čimbenika, konstantno praćenje učinkovitosti, ažuriranje i modificiranje, a može biti i rizičan za poslovanje ako se brzopleto izvede.

Segmentacija se u pravilu radi ručno, na temelju očitih obilježja pojedinaca (poput onih demografskih) ili nakon dubljeg istraživanja tržišta. No kod novih marketinških kanala, ovi su procesi toliko automatizirani i prilagođeni da se segmentacija vrši automatski za svakog pojedinog korisnika koji to dopusti – poslovni subjekt kupuje prostor na webu na kojem će se prikazivati njegovi oglasi, ovisno o ponašanju i navikama korisnika weba. Jedan je od najpoznatijih pružatelja usluga online oglašavanja Google Ads (prethodno Google Adwords), kojem poslovni subjekt plaća za prikazivanje kratkih oglasa korisnicima, a koji naplaćuje poslovnom subjektu prikazivanje oglasa po modelu PPC (*pay-per-click*) – cijena se određuje po svakom kliku na oglas koji korisnika preusmjerava na web stranicu oglašavača. Osim ovog, postoje još dva vrlo raširena modela naplate internetskih oglasa: CPM (*cost per mille*) – cijena prikazivanja tisuću oglasa, koji vole pružatelji prostora na webu jer cijena ne ovisi o reakciji potrošača, te CPA (*cost per action*) – cijena koju poslovni subjekt plaća za kupnju ili drugu

dogovorenu akciju koju je izvršio nakon klika na oglas, što odgovara poslovnim subjektima jer je obično najniža i najpreciznije se može odrediti. [1, str. 313-314] Sve što obuhvaća marketing baza podataka predstavlja čvrst temelj za idući sloj CRM-a u kojem aktivno sudjeluje i sam kupac.

1.4. Izravni marketing

Treća, posljednja komponenta CRM-a je izravni marketing (*direct marketing*). Izravni marketing podrazumijeva skraćivanje čitavog puta oglašavanja proizvoda ili usluge od prodavača (proizvođača) direktno do potencijalnog kupca, što predstavlja kolaborativni dio djelatnosti CRM-a. Komuniciranje s kupcima razvojem se tehnologije i implementacijom novih modela oglašavanja promijenilo od starijih metoda. Naime, razvojem mreže prodavaču se omogućio pristup bilo kome tko ima uređaj kojim može pristupiti mreži, bez obzira na fizičku udaljenost od njega. Osim olakšane razmjene samih dobara i usluga, zbog ovakvih novih infrastrukturnih mogućnosti razvija se i interaktivan odnos (jedan na jedan) između prodavača i potencijalnog kupca, nasuprot mnogo slabije učinkovitom masovnom marketingu. Ovakav je pristup usporediv s najstarijim metodama oglašavanja kakve su provodili putujući trgovci i prodavači na tržnicama, čime se na neki način zatvara krug razvoja metoda oglašavanja. Prodavač već, zbog provođenja rudarenja podataka i marketinga baza podataka, zna kome i kako pristupiti na temelju podataka koje je skupio o pojedincima, te istovremeno zna kako predstaviti kupcu novi proizvod, podsjetiti ga na već postojeći proizvod, potaknuti ga na ponovnu kupnju, informirati ga o posebnim prodajnim akcijama, riješiti potencijalni kupčev problem ili nedoumicu, educirati ga i pružiti mu razne druge informacije koje će produbiti njegov međusobni odnos s kupcem. Tako je olakšana međusobna interakcija, razmjena informacija i dobara te je poboljšano sveukupno zadovoljstvo poslovanjem s obje strane.

1.5. Profiliranje – nova segmentacija

Prema podacima koje korisnici weba objavljuju o sebi samima te podacima i metapodacima koji proizlaze iz njihovog kretanja webom, oni bivaju smješteni u određene okvire, odnosno prepoznati kao „ličnosti“ ili „tipovi korisnika“, koji se mogu konkretno iskoristiti u svrhe segmentacije i oglašavanja, kao i za prilagođavanje strukture i dizajna pojedinih dijelova weba. [1, str. 274-275] Kako se, osim podataka o konkretnim transakcijama, o korisnicima skupljaju osobni podaci poput imena, prezimena, starosti i kontakt podataka,

geografski podaci poput grada i adrese, podaci o komunikacijama s drugim korisnicima weba te mnoštvo drugih, osim vlastitog izravnog prikupljanja podataka te potencijalne kupnje od trećih strana, oni se mogu pratiti i po društvenim mrežama. Svaki će perspektivni poslovni subjekt tako imati svoje stranice na društvenim mrežama, kako bi dodatno izgradio vlastiti imidž, kako bi se još više približio pojedincima na tržištu, no i kako bi došao do informacija do kojih ima pristup samo putem ove, nove vrste kanala.

Kako društvene mreže ne generiraju podatke, već samo služe kao medij za njihov prijenos, danas one služe kao Petrijeva zdjelica za proučavanje korisnika pod mikroskopom – svi su podaci koje korisnik javno objavi praktički besplatni, a i praktični za prikupljanje. Jedini značajniji problem može biti u tome što nema garancije da korisnici objavljuju istinite osobne podatke, ili barem ne na jednom mjestu. [1, str. 309-315] Tako jedan prosječan korisnik može imati profil na Facebooku koji koristi za komunikaciju s prijateljima, profil na Instagramu koji koristi za objavljivanje fotografija s mjesta koja posjećuje, profil na Youtubeu na kojem ništa ne objavljuje, ali gleda na desetke videa različite tematike svaki dan, profil na Twitteru na kojem se uključuje u pojedine političke rasprave, profil na LinkedIn-u koji koristi isključivo za poslovne komunikacije te još velik broj drugih, odvojenih profila. Na svakom od njih on može djelovati kao zasebna osoba, što dodatno otežava marketinšku segmentaciju.

Tako se danas sve intenzivnije razvijaju strategije i mehanizmi praćenja i profiliranja korisnika na webu koji spajaju sve pojedinčeve informacije, do kojih mogu doći s različitih izvora, u jednu zvjezdastu strukturu koja svaki komadić informacija spaja na jezgru, u koju je upisano korisnikovo ime.

2. Metodologija praćenja korisnika

U forenzici postoji koncept pod nazivom „Locardovo načelo razmjene“, koji govori da će svaki počinitelj kriminalnog djela donijeti nešto na mjesto zločina i nešto s njega odnijeti, te obje te stvari mogu biti korištene kao dokazi. Primijenivši ovaj koncept na mrežne komunikacije, analogno se dolazi do zaključka da svaki kontakt, odnosno interakcija s mrežom, ostavlja trag. Takav se trag u ovom kontekstu naziva digitalni trag. Digitalni trag može biti pasivan, kakav se u sustavu ostavlja nesvjesno i automatizirano (podaci u kolačićima poput korisnikovih lozinki), ili aktivan, kakav korisnik ostavlja svjesno i s namjerom, komunicirajući s drugim korisnicima preko društvenih mreža, izmjenjujući elektroničku poštu, objavljujući fotografije i slično. Tragovi korisnika najčešće se pohranjuju u memoriji uređaja, na prostoru diska ili unutar evidencije uhvaćenog mrežnog prometa, ovisno o mogućnostima i namjerama subjekta koji implementira praćenje. U nastavku se objašnjavaju konvencionalni i manje konvencionalni mehanizmi praćenja korisnika na webu, od kojih se neki koriste već dugi niz godina, a neki su tek u svojim povojima. [2, str. 30-31]

2.1. Praćenje na temelju sesije

Objašnjavanje tehnika praćenja korisnika kreće s praćenjem na temelju sesije, kako je ovo i kronološki prva korištena metoda praćenja. Ova metoda generalno se ne smatra invazivnom jer joj inicijalna, a ni današnja svrha nije samo gomilanje podataka o korisnicima. Sesija je skup korisničkih interakcija s nekim web mjestom, koji se odvija unutar definiranog vremenskog okvira. To znači da će sesija, ako joj je određen životni vijek 60 minuta, trajati i ako korisnik ode s web mjesta unutar definiranog vremena te se ponovno vrati. Ako korisnik ostane na web mjestu dulje od vremena trajanja sesije bez ikakve interakcije s web mjestom, sesija će isteći. Ako pak komunicira s web mjestom dulje od zadanog vremena, sesija će ostati otvorena. [3]

Najprije je potrebno objasniti kako sesije zapravo funkcioniraju. HTTP protokol je nestalan, odnosno ne pamti stanje sesije, što znači da bi nakon svake nove TCP veze, koju pokreće korisnikov GET ili POST zahtjev, preglednik iznova morao tražiti korisnikovo korisničko ime i lozinku. Ovo se sprečava upravljanjem sesijama, koje omogućava HTTP protokolu da pamti stanje sesije. Kad se korisnik prijavi u svoj korisnički račun, spremanje stanja sesije omogućava mu pretraživanje web mjesta ili vanjskog weba bez prekidanja sesije i nametanja ponovnog prijavljivanja u račun, sve dok sesija ne isteče. Nadalje, ako korisnik pretražuje web preko

preglednika, postoji mogućnost da će se sustav ili sama aplikacija srušiti (eng. *crash*), no korisnik može vratiti prethodno otvorene i naglo prekinute sesije koje je preglednik zapamtio spremanjem podataka u kolačiće (eng. *cookies*). [4]

Tablica 1. Tehnologije koje koriste mehanizmi za praćenje na temelju sesije te podaci koje ono prikuplja [5]

Mehanizam	Tehnologije	Prikupljani podaci
Skrivena polja u HTML-u	Sesija web poslužitelja	Identifikator sesije
Autentikacija web obrascem	Sesija web poslužitelja	Identifikator korisnika
windows.name DOM svojstvo	HTML5, JavaScript (JS)	Identifikator sesije

2.1.1. Identifikatori sesije pohranjeni u skrivenim poljima

Prije 1994. godine prošlog stoljeća, kad su se za pohranjivanje korisnikovog identifikatora (podatak tipa string koji može jednoznačno identificirati korisnika unutar sesije pretraživanja weba; može biti sastavljen od vremenske oznake i nasumične brojčane oznake) počeli koristiti kolačići, morao se pronaći specifičan način za praćenje korisnika. Ovo se postiglo tako što se korisnikov identifikator prenosio između web stranica unutar URL-a (kod GET metode koja u jasnom, čitljivom obliku ispisuje imena i vrijednosti varijabli) ili kao vrijednost unutar skrivenog polja HTML obrasca (kod POST metode, koja se koristi za prijenos osjetljivijih podataka poput lozinki ili, u ovom slučaju, identifikatora). Na ovaj se način korisnikov identifikator nije pohranjivao na memoriju diska, kao ni u povijest pretraživanja. Nakon što su se u upotrebu uveli kolačići, ovaj je način postao relativno redundantan. [5]

2.1.2. Eksplicitna autentikacija korisnika preko web obrasca

„Eksplicitna autentikacija korisnika preko web obrasca“ zapravo je objašnjenje za implementaciju sustava za prijavu na neko web mjesto. To podrazumijeva da će to web mjesto imati javno dostupnu samo naslovnu stranicu ili neki manji dio sadržaja, dok će za potpun pristup korisnika tražiti da se registrira uz jedinstveno korisničko ime i lozinku, koji se tad pohranjuju u bazu podataka web mjesta. Svaka iduća prijava automatski će jednoznačno prepoznati korisnika, neovisno o pregledniku, operacijskom sustavu i ostalim tehničkim aspektima prijave. No ako se koristi bez upotrebe kolačića, ova metoda učinkovita je samo za vremena trajanja sesije. Također, iz perspektive onog koji prati korisnika, ova metoda može biti

netransparentna jer je korisnik svjestan da je neanonimno prijavljen u sustav te da je moguće njegove akcije na web mjestu povezati s njegovim imenom. Kao kad su ljudi svjesni da ih snima nadzorna kamera, i ovakav pristup može utjecati na ponašanje korisnika.

2.1.3. window.name svojstvo DOM sučelja

DOM, odnosno Document Object Model, sučelje je za programiranje aplikacija (API) koje je neovisno o jeziku i platformi na kojoj se izvodi. Namjena je DOM-a izrada HTML i XML dokumenata, čiju strukturu promatra hijerarhijski. Tako se neki dokument sastoji od objekata, od koji svaki može imati više različitih svojstava. [6]

Jedno je od tih svojstava i ime prozora, koje može sadržavati do 2 MB podataka, u koje može biti pohranjeno više varijabli. Ovo svojstvo neće se mijenjati kod ponovnog učitavanja stranice, a može se i proslijediti trećim stranama. Primjena mu se svodi na spremanje vrijednosti varijabli preko više stranica na web mjestu bez potrebe za upotrebom kolačića, a razlika je u tome što se sadržaj svojstva imena prozora ne šalje serveru unutar zahtjeva u zaglavlju, dok se sadržaj kolačića definiranog JavaScriptom šalje serveru. [5]

2.2. Praćenje na temelju skladištenja

Praćenje na temelju skladištenja podrazumijeva skladištenje podataka na korisničkoj strani. Ove su metode naprednije od praćenja temeljenog samo na sesijama, a kako mogu identificirati operacijski sustav i/ili preglednik koji korisnik koristi, u svojim su počecima predstavljale novu prijetnju korisnicima. Danas je ovo generalno najčešće korištena metodologija praćenja.

Tablica 2. Tehnologije koje koriste mehanizmi za praćenje na temelju skladištenja te podaci koje ono prikuplja [5]

Mehanizam	Tehnologije	Prikupljani podaci
HTTP kolačići	HTTP zaglavlja, JS	Identifikator instance preglednika
Flash kolačići	Flash, Java	Identifikator instance preglednika
Silverlight spremište	Silverlight	Identifikator instance operacijskog sustava
HTML5 spremišta	HTML5, JS	Identifikator instance preglednika
Web SQL i HTML5 baza podataka	HTML5, JS	Identifikator instance preglednika

2.2.1. HTTP kolačići

HTTP kolačić malen je podatak (kapaciteta 4 KB) koji server šalje korisnikovom web pregledniku, koji ga može pohraniti i proslijediti natrag istom serveru kad mu korisnik šalje idući zahtjev. Koristi se da bi se utvrdilo dolaze li dva zahtjeva od istog korisnika, što radi pohranjivanjem informacija o stanju unutar HTTP protokola, koji to sam po sebi ne pamti. Uglavnom se kolačići upotrebljavaju za prethodno spomenuto upravljanje sesijama (prijavljivanje u korisnički račun, kartično plaćanje, košarice za kupovanje), personalizaciju (korisnikove preferirane postavke dizajna sučelja preglednika i slično) te praćenje i dokumentiranje korisnikovog ponašanja. Ako nije drugačije eksplicitno određeno, kolačić se šalje poslužitelju trenutne lokacije web mjesta na kojoj se korisnik nalazi.

Treba napomenuti da kolačić nikad ne bi trebao sadržavati osjetljive informacije jer ne postoji sasvim pouzdana sigurnosna zaštita koja bi zaštitila njegov sadržaj. Tako postoji opasnost od otimanja sesije (eng. *session hijacking*) kroz iskorištavanje XSS (Cross-site scripting) i CSRF (Cross-site request forgery) ranjivosti web mjesta. Ove se ranjivosti mogu

pokrpati kod samog postavljanja kolačića tako što mu se dodijeli atribut „httponly“, filtriraju se korisnikovi unosi, prije izvršavanja osjetljive akcije traži se dupla korisnikova potvrda, a kolačići koji se koriste za osjetljive akcije imaju kratak životni vijek. Međutim, danas se mnogo ljudi da prevariti socijalnim inženjeringom – iskorištavanjem ljudske naivnosti i/ili neinformiranosti o određenoj stvari, a takva se vrsta napada gotovo nikad ne može spriječiti implementacijom samo tehničkih mjera sigurnosti.

Svaki kolačić ima svoju domenu. Ako je ta domena jednaka kao domena stranice na kojoj se korisnik trenutno nalazi, tad je kolačić po vrsti kolačić prve strane (eng. *first-party cookie*), a ako je domena s drugog mjesta, tada se govori o kolačiću treće strane (eng. *third-party cookie*). Kolačići prve strane šalju se poslužitelju stranice koju korisnik pregledava, dok se kolačići trećih strana uglavnom koriste u svrhe oglašavanja i praćenja korisnika kroz web. Preglednici prema zadanim postavkama dozvoljavaju upotrebu kolačića trećih strana, no postoje dodaci koje korisnik može instalirati u preglednik, a koji ih blokiraju. Primjer ovakvog dodatka je Privacy Badger. [7]

Uvijek je dobro obavijestiti korisnika o kolačićima (pogotovo onima trećih strana) koje koristi web mjesto na kojem se nalaze, kako se ne bi narušilo njegovo povjerenje ukoliko ih otkrije sam. Zato velik broj web stranica danas ima „cookie-bannere“, trake s obavijestima o upotrebi kolačića koje se prikazuju čim korisnik otvori web stranicu, a na kojima se nalazi gumb za eksplicitno korisnikovo odobrenje korištenja kolačića na stranici. Korisnik mora prihvatiti navedene uvjete da bi mogao nastaviti normalno pregledavati stranicu.

Ako pak korisnik namjerno želi smanjiti učinkovitost kolačića, u kojima ne vidi korist za sebe ili prepoznaje neku vrstu prijetnje, najosnovniji su načini za to ograničavanje upotrebe kolačića preko postavki preglednika, brisanje predmemorije (eng. *cache*) te korištenje različitih preglednika za pristupanje nekom web mjestu (kako su kolačići vezani i uz preglednik).

Prema trajanju, kolačići se dijele na sesijske, koji ističu zatvaranjem preglednika, te uporne, koji ističu nakon vremena koje je njihov tvorac odredio za njihov životni vijek. Osim ovakve podjele, mogu se razdvojiti i prema svojoj svrsi, te tako postoje oni koji služe za praćenje (eng. *tracking* cookies) i oni kojima to nije primarna svrha (eng. *non-tracking cookies*). Velika većina onih koji spadaju u prvu grupu ima životni vijek dulji od jednog dana (čak 90%), dok samo oko petine druge grupe ulazi u takvu statistiku. [5]

Kao mehanizam za praćenje, HTTP kolačići mogu se koristiti sami ili u kombinaciji s drugim tehnikama:

1. Kombinacija kolačića i autentikacije preko web obrasca, koja podrazumijeva spremanje korisnikovih identifikacijskih podataka u kolačić, kako se on ne bi morao prijavljivati u servis svaki put kad mu pristupi, što opet funkcionira tako dugo dok korisnik dopušta korištenje kolačića, ne briše predmemoriju te svaki put koristi isti preglednik.
2. Prosljeđivanje i sinkroniziranje kolačića, kod kojeg se kolačić s jednog web mjesta šalje na drugo, odnosno razmjenjuje se između dvije domene kao parametar zahtjeva. Ovakav sistem koriste Microsoft i Google za akumuliranje informacija o korisniku koji se kreće po njihovim domenama.
3. Oglašavačke mreže koje nastaju ugrađivanjem određenog broja unajmljenih tragača (eng. *trackers*) na web mjesto, s namjerom da skupljaju kolačiće s nekog web mjesta i prosljeđuju ih trećim stranama. [5]

2.2.2. Flash kolačići i Silverlight spremište

Nakon HTTP kolačića, na red dolazi nešto tehnički izdržljivije. Adobe Flash multimedijska je softverska platforma za reproduciranje animacija, video sadržaja, desktop aplikacija, mobilnih aplikacija i igara i sl. Međutim, zbog mnogih sigurnosnih prijetnji i skupog održavanja, Adobe planira izbaciti Flash iz upotrebe 2020. godine, te će se njihovi partneri, koji koriste Flash, morati prebaciti na nešto drugo. [9]

Flash koristi vlastito spremište pod nazivom Local Shared Objects, koje pohranjuje podatke na korisnikovom računalu. Kapacitet ovih objekata je 100 KB, čak 25 puta više nego onaj HTTP kolačića, teže ih je izbrisati, ne ističu sami od sebe, već ostaju pohranjeni u memoriji trajno, te spremaju i koriste podatke neovisno o pregledniku, prateći tako korisnika jednako učinkovito preko svih preglednika koje koristi. Osim lokalnog spremišta, Flash koristi i Remote Shared Objects, odnosno spremište podataka iz iste domene, za koje Flash nudi mogućnost brisanja. Nadogradnjama platforme došlo se do toga da se podaci brišu automatski kad preglednik briše obične HTTP kolačiće, a može se i blokirati pohrana bilo kakvih Flash objekata na korisnikovo računalo. [10]

Microsoftova alternativa Flasha, Silverlight, također može spremiti po 100 KB podataka po stranici korisničkog profila, no za razliku od Flasha, spremište nema pristup podacima kad

korisnik koristi privatni način pretraživanja. Jednako kao i Flash, omogućava isključivo ručno brisanje podataka iz spremišta, te se također uskoro planira povući s tržišta (2021. godine). [5]

2.2.3. Lokalno i sesijsko HTML5 spremište

Lokalno HTML5 spremište pohranjuje podatke o korisniku u obliku parova ključeva i vrijednosti, te ne zahtijeva instalaciju ikakvog plugin-a. Objekti u spremištu nemaju definiran životni vijek te se mogu brisati samo ručno, odnosno briše ih korisnik ili administrator web mjesta. Ogromna prednost ovakvog načina pohrane podataka nad prethodno navedenima je mnogostruko veći kapacitet – jedan objekt može biti velik čak 5 MB.

Sesijsko HTML spremište radi na jednakom principu, s razlikom u tome što se podaci automatski brišu sa svakim zatvaranjem prozora web preglednika. [5]

2.2.4.Web SQL Database i HTML5 IndexedDB

Web SQL baza podataka koristi sustav za upravljanje bazama podataka SQLite, koji je ugrađen u krajnji program, umjesto lokalnog sustava za upravljanje podacima za pohranu podataka o korisniku. Ovaj sustav bio je implementiran u svakom poznatijem pregledniku, no zamijenjen je HTML5 Indexed DB-om, koji pohranjuje podatke u korisnikov preglednik, s tim da ima jednak utjecaj na privatnost podataka kao i lokalno spremište podataka. [5]

2.3. Praćenje na temelju predmemorije

Kao i prethodna, ova grupa mehanizama za praćenje također pohranjuje podatke na klijentovoj strani. No za razliku od prijašnjih mehanizama koji su koristili spremišta isključivo za spremanje podataka o korisniku, ovi mehanizmi iskorištavaju i mogućnosti identifikacije preglednika, specifične sesije pretraživanja u pregledniku te prethodno posjećenih mjesta na webu, a sve korištenjem različitih vrsta predmemorije.

Tablica 3. Tehnologije koje koriste mehanizmi za praćenje na temelju predmemorije te podaci koje ono prikuplja [5]

Mehanizam	Tehnologije	Prikupljani podaci
Web predmemorija	HTML5, JS, HTTP zaglavlja, testovi na strani poslužitelja	Identifikator instance preglednika, povijest pregledavanja
DNS predmemorija	JS	Povijest pregledavanja
Operativna predmemorija	HTTP zaglavlja, JS	Identifikator instance preglednika

2.3.1. Web cache

Web cache je mehanizam koji može značajno poboljšati korisničko iskustvo kod pretraživanja weba, te u isto vrijeme optimizirati propusnost koja je na raspolaganju pružatelja usluge. Radi na način da u privremeno spremište (predmemoriju) sprema podatke koje je korisnik zatražio na webu. Tako korisnik nekad može primijetiti da se stranica koju je zatražio po prvi put učitava neko vrijeme, dok se kod drugog posjećivanja ona učita primjetno brže jer su određeni podaci (HTML stranice, slike i dr.) ostali pohranjeni u predmemoriji. No kako se sadržaj mnogih stranica na webu konstantno mijenja i ažurira, ne pohranjuju se uvijek svi dijelovi web stranica. Tako korisnik, na primjer, može pregledavati neki portal s vijestima ujutro. On će se najprije učitati, dijelovi poput zaglavlja, podnožja, logotipa i raznih elemenata dizajna stranice spremit će se u predmemoriju, korisnik će se vratiti na portal nekoliko sati kasnije, a dijelovi koji će se učitati ispočetka bit će samo nove vijesti, odnosno oni dijelovi koji su se od posljednje pohrane u predmemoriju promijenili. Životni vijek određenih informacija u predmemoriji, kao i dijelovi koji se automatski pohranjuju bit će određeni različito na svakoj web stranici, ovisno o razvojnom programeru, kao i o korisnikovim preferencijama. [11]

Praćenje korisnika, kao na primjer kad oglašivač ima oglase na više web stranica te želi utvrditi koje je od njih korisnik posjetio, ovdje se može provesti iskorištavanjem sljedećih svojstava predmemorije:

1. Ugradnja identifikatora u dokumente pohranjene u predmemoriju omogućena je ako je korisnikov zahtjev poslan u obliku HTML datoteke. HTML omogućuje uključivanje *div* elementa (za odvajanje sekcije dokumenta) koji može biti nevidljiv korisniku, te se u njega može ugraditi spomenuti identifikator, spreman za korištenje kroz više mjesta na webu.
2. Testiranje performansi učitavanja mogu provoditi web stranice korištenjem JavaScripta za uočavanje duljine vremena potrebnog za učitavanje nekog elementa web stranice, nakon kojeg se procjenjuje je li neki objekt bio pohranjen u predmemoriji preglednika ili nije.
3. HTTP zaglavlja osobne oznake i posljednje izmjene također se mogu upotrijebiti kao sredstvo identifikacije korisnika. ETags zaglavlje (eng. *entity tags* – osobna oznaka) ima kapacitet malo manji od 10 KB te je takav dovoljan za pohranu korisnikovog identifikatora, a zaglavlje koje prikazuje posljednju izmjenu podataka ne prima samo datum, već i bilo kakav nasumični string kao tip podataka, što se također može iskoristiti u svrhe praćenja. Nakon provjere ovog zaglavlja kad korisnik po drugi put otvori web stranicu, web poslužitelj utvrđuje jesu li spremljeni podaci u predmemoriji još ažurni, te ako jesu, vraća statusni kod *304 Not Modified*, a ako nisu, učitavaju se novi. Ako korisnik želi spriječiti vlastito praćenje preko zaglavlja, mora očistiti predmemoriju prije svakog novog posjeta na web stranicu, odnosno samo zatvoriti sve kartice pretraživača prije ponovnog posjećivanja web stranice ako koristi privatnu pretraživačku sesiju. [5]

2.3.2. DNS cache

Domenski sustav imena ili DNS (eng. *Domain Name System*) distribuirana je baza podataka koja funkcionira kao prevoditelj između korisnika i računala, odnosno prevodi smislena imena web adresa koje korisnik unosi u adresnu traku preglednika u IP adrese koje razumiju računala i obrnuto. [12]

DNS ima vlastito privremeno predmemorijsko spremište na svakom računalu, kojim upravlja operacijski sustav, a koje sadrži zapise o nedavno zatraženim i posjećenim web stranicama, odnosno o njihovim adresama i imenima domena. Ovo spremište služi za smanjenje

vremena čekanja na učitavanje određene stranice, koju je korisnik prethodno već posjetio, za vrijeme koje bi se inače potrošilo na traženje odgovarajuće IP adrese kod prvog korisnikovog pristupanja nekoj stranici. Automatska metoda, koja korištenjem JavaScripta može neizravno prouzročiti DNS zahtjev za pretraživanje i izmjeriti vrijeme odgovora na njega, može poslužiti za potvrđivanje korisnikovog pristupa web stranici u nekom trenutku u prošlosti. [13]

2.3.3. Operativna predmemorija

Operativna predmemorija podrazumijeva pohranjivanje informacija o operacijama provedenim u pregledniku, umjesto spremanja kopija preuzetih elemenata. To obuhvaća informacije kao što su preusmjeravanja, korisnička imena i odgovarajuće lozinke za prijavu u neki korisnički račun, popis domena koje je dopušteno otvoriti samo uz korištenje SSL-a (HTTPS umjesto običnog HTTP-a) i slično. Ova grupa podrazumijeva nekoliko mehanizama:

1. HTTP 301 predmemorija za preusmjeravanje (eng. *redirect cache*) služi za obavještavanje preglednika da je specifični zatraženi resurs trajno dostupan na nekoj drugoj adresi. Preglednik pamti novu adresu i koristi je umjesto one nevažeće koju je korisnik unio kod svakog idućeg pretraživanja. Ovo je korisno kad je stranica koju korisnik traži premještena na novi ili skraćeni URL, no s druge strane mogu ga iskoristiti treće strane za praćenje korisnika – kod prvog posjeta nekoj web stranici, generira se statusni kod 301, čija je svrha preusmjeravanje, no kao novi URL definira se onaj koji je korisnik već unio, no uz njega se pohranjuje i poseban identifikator korisnika. Tako će se taj URL koristiti kod svakog sljedećeg korisnikovog posjećivanja web stranice, bez njegovog znanja. [5]
2. HTTP autentikacijska predmemorija privremeno pohranjuje korisničko ime i lozinku prilikom prijavljivanja u sustav, kako bi se sesija pretraživanja mogla jednoznačno odrediti te korisnik ne mora ponovno unositi identifikacijske podatke kod svakog novog zahtjeva unutar sesije. No preglednik se može prisiliti da se poveže s poslužiteljem web stranice i pohrani korisnikove identifikacijske podatke u predmemoriju bez njegovog znanja, te ih koristi za njegovo praćenje bez potrebe za kolačićima. [14]
3. HSTS (*HTTP Strict Transport Security*) predmemorija može se iskoristiti za izgradnju spremišta s korisničkim podacima. HSTS način pretraživanja osigurava korisniku da će ostvariti HTTPS umjesto HTTP veze s poslužiteljem web stranice koju traži. Web stranica sprema njegove identifikacijske podatke, kodira ih posebno za svaku svoju pod-domenu, a treća ih strana kod idućeg posjeta web stranici može identificirati brute-force

tehnikom, isprobavajući svaku mogućnost kombinacije pod-domena; URL će se automatski prevesti u HTTPS kad se isprobana pod-domena poklopi s postojećim zapisom u bazi. Kako je svaki znak korisnikovog identifikatora kodiran u zasebnu pod-domenu, na ovaj način moguće je doći do cijelog identifikatora.

4. TLS predmemorija za nastavljanje sesije pohranjuje TLS identifikatore sesija, koje poslužitelj šalje klijentu kod postupka uspostavljanja veze, te koje klijent koristi kod idućeg spajanja s poslužiteljem. Ovime se ubrzava vrijeme uspostavljanja kontakta koje bi se inače potrošilo na postupak rukovanja, no olakšava se mogućnost praćenja korisnika od trećih strana. Ovaj se sigurnosni propust može zaobići korištenjem Tor preglednika. [5]

2.4. Praćenje „otiska prsta“

Praćenje korisnikovog otiska prsta (eng. *fingerprinting*) grupa je najkreativnijih mehanizama, naprednijih od prethodno navedenih grupa, koji mogu otkriti najširi raspon podataka o korisniku, dok su u isto vrijeme najteži za otkrivanje i onemogućavanje. Otisak prsta u ovom je kontekstu jedinstveni identifikator uređaja, operacijskog sustava, verzije preglednika ili instance pregledavanja, a može uključivati skup vrijednosti koje su čitljive web servisu kojeg korisnik pretražuje. Praćenjem takvog identifikatora korisnika se može pratiti preko više odvojenih web stranica različitih poslužitelja, što se ne može uvijek postići ni uz upotrebu kolačića. Ovdje kolačići nisu potrebni, no osim toga nije potrebna ni autentikacija – praćenje je gotovo neprimjetno korisniku, te ga se takvog teže sprečava. U manjoj se mjeri ono može ukloniti ako korisnik onemogući JavaScript i Flash u pregledniku, no ni ovo ne iskorjenjuje mogućnost praćenja jer postoje i drugi kanali za (pasivno) praćenje otiska prsta.

U glavne kategorije web stranica na kojima se ova vrsta praćenja iznimno često prakticira spadaju pornografske stranice te stranice za upoznavanje (eng. *dating sites*).

Tablica 4. Tehnologije koje koriste mehanizmi za praćenje otiska prsta te podaci koje ono prikuplja [5]

Mehanizam	Tehnologije	Prikupljani podaci
Mreža i lokacija	IP adresa, tehnologije za otkrivanje geolokacije, HTTP zaglavlja, HTML5, Java, JS, Flash	IP adresa, podaci o geolokaciji (zemlja, grad, vremenska zona)
Prepoznavanje uređaja	IP adresa, TCP zaglavlja, HTTP zaglavlja, JS, Flash	Identifikator uređaja, IP adresa, OS, rezolucija ekrana i druge hardverske specifikacije, vremenska zona, TCP oznake vremena
Prepoznavanje operacijskog sustava	Java, JS, Flash	Identifikator instance OS-a, verzija i arhitektura OS-a, jezik sustava, vremenska zona, datum i vrijeme, hardverske specifikacije, TCP/IP parametri, pristup kameri i mikrofonu, instalirani driveri
Prepoznavanje verzije preglednika	HTML5, JS, CSS	Detaljni podaci o verziji preglednika
Otkrivanje instance preglednika	HTTP zaglavlja, JS, testovi na strani poslužitelja	Identifikator instance preglednika, povijest pregledavanja, dopuštenja i ograničenja za kolačiće

2.4.1. Otkrivanje i praćenje korisnikove mreže i lokacije

Globalna mrežna adresa i geografska lokacija korisnika temeljena na IP adresi lako se mogu otkriti iz zaglavlja primljenih HTTP zahtjeva. Također, uz pomoć odgovarajućih mrežnih alata, pružatelj web servisa može saznati i domenu, odnosno ime korisnikovog internetskog poslužitelja (eng. *Internet Service Provider*). Ako korisnik koristi proxy poslužitelja, i njegova se prisutnost može otkriti putem HTTP zahtjeva, te ga se može zaobići uz pomoć specifičnih funkcionalnosti Flasha kako bi se otkrila stvarna klijentova IP adresa. Nadalje, JavaScript pomaže u otkrivanju korisnikovih podataka poput interne IP adrese (unutar podmreže) te GPS koordinata, dok Java pruža mogućnost otkrivanja prisutnosti vatrozida (eng. *firewall*). [5]

Generalno, web preglednik do korisnikove lokacije može doći na tri načina: traženjem ručnog unosa lokacije od korisnika, pribavljanjem podataka izravno od GPS senzora te putem mehanizama koji izvode informacije o geolokaciji iz IP adrese, za što postoje mnoge baze na webu. Jedna je od tih ip2location – baza koja iz IP adrese izvodi informacije o državi, gradu i regiji u kojoj se adresa nalazi, geografskim koordinatama uređaja s navedenom adresom, vremenskoj zoni, poštanskom broju regije, ISP-u korisnika, brzini prijenosa podataka, pozivnom broju, teleoperateru, proxy poslužitelju te nekoliko drugih. [15]

2.4.2. Prepoznavanje uređaja

Ova vrsta praćenja podrazumijeva pasivno skupljanje različitih informacija, čak i preko više različitih preglednika. Identifikator korisnika izvodi se iz raznih tehničkih informacija o sustavu, poput nekog dijela IP adrese, verzije operacijskog sustava, razlučivosti zaslona, vremenske zone, no i informacije o ulazno-izlaznim uređajima poput miša, tipkovnice, zvučnika i kamere. Takav identifikator tad ne ovisi o pregledniku, o instaliranim pluginovima ni o domeni koju korisnik koristi, a može se pratiti korištenjem JavaScripta.

S druge strane, postoji metoda praćenja koja se temelji na TCP-ovom bilježenju satnog skoka (eng. *clock skew*) – razlike u bilježenju među zapisima istog signala takta na dvije različite komponente računalnog sustava. Na ovaj se način može otkriti uređaj bez obzira na geografsku lokaciju, udaljenost uređaja, vrstu podmreže i prisutnost NAT-a (Network Address Translation) – metode za skrivanje i prevođenje IP adresa unutar neke podmreže, te zbog toga ovaj mehanizam ima prednost nad onima koji se temelje na praćenju IP i MAC adresa. Jedini

je nedostatak ovakve metode to što satni skokovi dvaju uređaja mogu biti previše slični da bi se precizno odredilo koji je uređaj bio u mreži u određeno vrijeme. [5]

2.4.3. Prepoznavanje operacijskog sustava

JavaScript može poslužiti kod otkrivanja arhitekture (32/64 bit-ne verzije) operacijskog sustava, jezika sustava, vremenske zone i preciznog vremena. Nadalje, Java appleti omogućavaju otvaranje, čitanje i spremanje datoteka kod klijenta te mogu biti iskorišteni za praćenje informacija. Rade tako što se skinu na klijenta kad korisnik pristupi web stranici koja ih sadrži te mogu biti ograničeni sandboxom (sigurnosni mehanizam za izolirano izvođenje programa kojima korisnik ne vjeruje) ili privilegirani, što znači da će moći raditi i izvan sandboxa, s opsežnim ovlastima pristupa korisnikovim informacijama. [16]

2.4.4. Prepoznavanje verzije preglednika

HTTP zaglavlje sadrži polje koje prikazuje ime preglednika, no ono nije uvijek posve pouzdano jer razne aplikacije mogu obfuscirati ovaj podatak, odnosno netočno ga predstaviti. No postoje novije metode za otkrivanje ovog podatka – prepoznavanje uz pomoć CSS-a i HTML5 standarda. Obje metode funkcioniraju na sličnom principu – prepoznaju vrstu i verziju preglednika ovisno o razlikama implementacije pojedinih aspekata. Tako za svaki preglednik postoji posebna skupina CSS svojstava koja on podržava, a čije se postojanje može provjeriti JavaScriptom, te skupina HTML oznaka i atributa koji se unutar tog preglednika koriste.

Još jedna metoda koja se koristi za ovakvo prepoznavanje temelji se na testiranju načina implementacije ECMA-262 standarda za JavaScript jezik (uz pomoć JavaScript interpretera), opet zbog toga što ovakvo testiranje za svaki pojedini preglednik daje drugačije rezultate. Osim verzije preglednika, ovakvo testiranje može identificirati i operacijski sustav te arhitekturu računala.

2.4.5. Otkrivanje instance preglednika uz pomoć povijesti pretraživanja

Jedan pristup ovakvom mehanizmu praćenja korisnika pokazao je da se nešto manje od polovice korisnika weba može identificirati provjeravanjem imaju li neku od 50 predefiniranih web stranica u svojoj povijesti pretraživanja. Poveća li se broj testiranih stranica na 500, moguće je identificirati gotovo tri četvrtine korisnika weba na temelju njihovih posjeta tim stranicama.

Drugi pristup ulazi u tehničke karakteristike društvenih mreža ili konkretnije, mogućnost ulaženja u grupe, javne ili privatne, koju pružaju svojim korisnicima. Svaka takva grupa ima svoj identifikator, vidljiv u URL-u, koji upućuje na korisnikovu aktivnost u grupi, makar to bilo samo pregledavanje. Ovaj se URL sprema u povijest pretraživanja te se prema njemu može pratiti korisnik, no može se saznati i njegovo stvarno ime. Kako u grupama postoje ugrađeni filtri, odnosno pretraživači, omogućeno je pisanje malicioznih skripti koje provjeravaju aktivnost velikog broja korisnika u velikom broju grupa, te smještaju korisnike u bazu podataka prema popisu članova grupe, nakon čeg je omogućena ili olakšana njihova identifikacija.

2.5. Ostali mehanizmi praćenja

2.5.1. HTTP zaglavlja

HTTP zaglavlja prenose tehničke informacije o zahtjevu, među kojima je i URL trenutne stranice s koje dolazi zahtjev. Američki teleoperater Verizon Wireless tako je poznat po tome što u HTTP zahtjeve uključuje posebno zaglavlje koje sadrži korisnikov identifikator, koji ostaje nepromijenjen danima nakon slanja zahtjeva. Tako web stranice mogu pratiti korisnike čak i ako imaju vrlo napredne postavke privatnosti, te se podaci mogu kupiti u svrhu prikupljanja statističkih podataka o demografskim i drugim geografskim segmentima korisnika.

2.5.2. Metapodaci s telefona

Nakon Snowdenovog izlaska u javnost 2013. godine [17], tadašnji američki predsjednik Barack Obama pokušao je, između ostalog, umiriti javnost naglašavanjem činjenice da Američka Nacionalna Sigurnosna Agencija (NSA) ne gleda sadržaj podataka koje prikupe preko mobilnih uređaja, već samo metapodatke. Čak i zanemarivši netočnost izjave, zbog značaja koji metapodaci nose, ova je činjenica daleko od utješne. Sami po sebi oni mogu izgledati kao dug niz beznačajnih, nesuvislih podataka, no kad se oni analiziraju, iz njih se može saznati daleko više informacija o korisniku nego bi se moglo praćenjem samih komunikacija koje ima s nekim – informacije o pojedinčevoj obitelji, religiji, karijeri, političkim opredjeljenjima, seksualnim preferencijama, ilegalnim aktivnostima i mnoštvo drugih privatnih informacija. [18]

U dokumentarcu *Nothing to Hide* iz 2017., provodi se testiranje na subjektu koji je u njemu dobrovoljno sudjelovao. Radi se o Maxu Thommesu, njemačkom glumcu i glazbeniku, o kojem njegovi „pratitelji“ nisu znali ništa kad su pokrenuli pokus, pa čak ni njegovo ime. Pet su tjedana pomoću špijunskog softvera skupljali metapodatke s njegovog mobitela, koji su uključivali detalje o kretanju subjekta (detaljne koordinate s vremenskim oznakama), a čijom su obradom dobili kartu s prikazom najčešćih kretanja i najduljih prebivanja na pojedinim lokacijama te između ostalog zaključili na kojoj je lokaciji njegov stan. Nadalje, otkrili su njegovo ime i osobne podatke nakon otkrivanja njegovog Facebook profila iz URL-a, svrstali povijest pretraživanja weba u određene kategorije, iz trenda količine komunikacije preko društvenih mreža prepoznali bitne događaje u njegovu životu (poput rođendana) te saznali razne druge stvari iz njegovog privatnog života, skupljajući samo metapodatke. Nakon eksperimenta objasnili su da su ga izvodili ručno, samo za jednu osobu, no jednom kad su razvili alat koji

omogućava automatizaciju analiza kakve su oni provodili, zaključili su da je svejedno radi li se o prikupljanju podataka o jednoj osobi ili o milijunima njih, kako to radi NSA. [19]

2.5.3. Vremenski napadi

Vremenski napadi oslanjaju se na mjerenje i analiziranje vremena potrebnog za dekriptiranje podataka, učitavanje stranice i razne druge softverske operacije. Napadač mjeri vrijeme koje odabere, shvati što utječe na razlike u izmjerenim vremenima te dolazi do tajnih podataka koje traži. Tako se, na primjer, može shvatiti je li korisnik prethodno posjetio neku stranicu prema vremenu potrebnom za iscrtavanje poveznica na tu stranicu pomoću JavaScripta – kako posjećene poveznice imaju drukčije oblikovanje od neposjećenih, mjerenjem vremena potrebnog za njihovo iscrtavanje u milisekundama utvrđuje se jesu li posjećeni ili ne. [20]

2.5.4. Nesvjesna suradnja korisnika

Nadovezivanjem na vremenske napade, vrijedi spomenuti da svi glavni preglednici imaju implementirane preventivne mjere koje sprečavaju takve napade. No uz sve mjere koje su osmišljene za obranu korisnika od neovlaštenog pristupa trećih strana njegovim podacima, on nije siguran ako ga se prevarom može navesti na otkrivanje informacija. Tako mnoga web mjesta ilegalno prikupljaju povijest pregledavanja svojih korisnika, uključujući u to stranice koje nemaju veze s njihovim serverima, kršeći pritom *same-origin policy* – sigurnosnu politiku koja se odnosi na cijeli web. Ovo se može iskoristiti kod osjetljivijih stranica, poput web stranica banaka, koje provjeravaju je li neki klijent bio na poznatom *phishing* web mjestu, no s druge strane, iskoristivo je i za povezivanje korisnikovih računa na različitim web mjestima, koje je on namjerno odvojio radi kontekstualnog predstavljanja svoje osobnosti. Jedan način na koji se ovo može provesti uključuje autentikacijski mehanizam CAPTCHA, čiji su elementi estetski uvjetovani poviješću korisnika koja se provjerava. CAPTCHA se sastavi od poveznica koje se žele ispitati, a od kojih je svako slovo/riječ jedna poveznica – različita ako je prethodno posjećena i ako nije. Improvizirani se mehanizam prekrije prozirnim slojem da korisnik ne shvati njegov sastav, u polje za unos ispiše sadržaj slike i tako nesvjesno kaže web stranici ono što onaj koji ga provjerava želi čuti.

Osim nekoliko načina na koje se CAPTCHA može iskoristiti u ovu svrhu, postoji i jedan neobičniji. Ponovno vezano uz CSS oblikovanje, pozadinska boja stranice ili nekog elementa stranice može biti određena ovisno o tome je li korisnik prethodno posjetio poveznicu na koju se element odnosi ili ne. Način na koji korisnik odaje ovu informaciju je bizaran – dopuštanjem

stranici korištenje vlastite web kamere. Pozadinska boja reflektira se na korisnikovom licu te poslužitelj web stranice zna je li korisnik prethodno posjetio poveznicu ili nije. [21]

2.5.5. Clickjacking

Clickjacking (eng. *click* + *hijacking*; otimanje klika) je napad koji podrazumijeva preusmjeravanje korisnika na nelegitimno mjesto ili aktivnost, skrivajući pritom poveznicu na spomenuto mjesto ili aktivnost unutar objekta koji korisniku djeluje legitimno (manipuliranjem svojstava unutar CSS-a), a sve u pravilu s malicioznim namjerama. Ovaj se napad može iskoristiti u svrhu skupljanja „lajkova“ na Facebooku, pogleda na Youtubeu, pratitelja na Twitteru i slične radnje koje ne oštećuju korisnika, no može se iskoristiti i za neovlašteno objavljivanje u nečije ime uz potencijalno širenje neke vrste malwarea, javno objavljivanje korisnikovih osobnih informacija, neovlašteno pristupanje korisnikovoj kameri ili mikrofonu te mnoge druge radnje koje ugrožavaju korisničku privatnost i/ili čak sigurnost. [22]

2.5.6. Evercookies

Evercookies ili Supercookies je naziv za mehanizam koji pohranjuje kolačiće te ih ponovno postavlja nakon što se oni ručno obrišu, što ih čini praktički neizbrisivima. Vrijednost kolačića tako se pomoću JavaScripta može pohraniti unutar Flash kolačića (iako se ovi sve manje koriste), Silverlight spremišta, povijesti pregledavanja, ETags HTTP zaglavlja, web predmemorije, raznih HTML5 spremišta i drugih spremnika korisničkih podataka. Kao što se u kontekstu zlonamjernog softvera (*malwarea*) razmnožavaju crvi, tako se u kontekstu tehnologije za praćenje korisnika implementacijom evercookiesa osigurava nemogućnost brisanja podataka koji su se jednom zapisali o korisniku u neki kolačić, čak i ako korisnik redovito briše kolačiće. [23]

3. Privatnost i sigurnost

Prethodno opisani mehanizmi, kao i mnogi drugi koji su tek u različitim fazama razvoja ili uvođenja u upotrebu, kao i oni za koje se javno ni ne zna, kao svoju svrhu najčešće imaju prilagodbu korisniku – prilagodbu oglasa, prilagodbu ponude, prilagodbu predloženog sadržaja, prilagodbu pretraživanja i slično, što poboljšava korisničko iskustvo te, s druge strane, pomaže prodavačima u dubokom razumijevanju tržišta te, posljedično, većem povratu uloženih sredstava.

No ne ispada sve uvijek samo pozitivno za kupca. Prikupljanje njegovih osobnih podataka s weba pruža mogućnost procjene financijskog kredibiliteta, što može ispasti subjektivno i oštetiti ga na razne načine. Jednako tako prikupljeni podaci mogu pripomoći u predviđanju nesreća koje pokriva osiguranje, pružajući osiguravateljima modifikacije police i bez znanja osiguranika. Stoga ovdje navedeni i mnogi drugi prikupljeni podaci o pojedinim korisnicima omogućavaju provođenje cjenovne (i drugih vrsta) diskriminacije koja se može definirati na temelju geografskih i demogeografskih podataka, mjesta s kojeg je korisnik došao na neku stranicu za naručivanje preko weba (ako je to oglas, možda je uključen neki znatan popust), no i na temelju korisnikovih navika zabilježenih kroz vrijeme. [10]

Nadalje, postoje još opasnije stvari koje mogu oštetiti korisnika, poput krađe identiteta koja se može provesti zlouporabom nečije neosviještenosti o opasnostima neopreznog objavljivanja prevelike količine osobnih podataka poput datuma rođenja, vlastite trenutne ili bivše obrazovne institucije, broja telefona, imena ljubimaca (koje može biti odgovor na pojedina sigurnosna pitanja) i drugog.

Na kraju, globalno praćenje populacije od strane divova poput sigurnosnih agencija, nacionalnih agencija i korporativnih institucija nešto je čega se svakodnevno boji sve više ljudi. Ne nužno zato što rade nešto pogrešno, nego zbog toga što postaju svjesniji da postoji mogućnost da im se prati svaki korak, bili oni toga svjesni ili ne. Kao u Orwellovoj 1984., ljudi su okruženi ekranima preko kojih ih „Veliki brat“ može vidjeti u bilo kojem trenutku, a s razvojem tehnologije smanjuje se vjerojatnost da će globalni nadzor ikad biti onemogućen. [24]

3.1. Pravo na privatnost

Zbog prethodno navedenih i mnogih drugih razloga, među korisnicima Interneta javlja se zabrinutost o privatnosti podataka, koja uključuje pitanja o tome tko sve skuplja njihove podatke, skuplja li se o njima veća količina podataka od one za koju su svjesni te za koju su dali dopuštenje te na kraju – za što se zapravo svi prikupljeni podaci koriste.

Privatnost se općenito odnosi na pravo pojedinca da sam upravlja vlastitim osobnim, tajnim podacima te da se nitko neovlašteno ne upliće u njegov privatni život. Općenito, dimenzije koje obuhvaća pojam privatnosti obuhvaćaju fizičku privatnost pojedinca koja se odnosi na njegovu tjelesnost, privatnost ponašanja koja dopušta pojedincu odlučivanje vlastitog ponašanja, mišljenja, opredjeljenja i slično, zatim privatnost komuniciranja s okolinom bez neželjenih interferencija, te privatnost osobnih podataka, koja određuje ovlasti pojedinih subjekata o prikupljanoj količini informacija o nekom pojedincu.

U kontekstu mrežnih komunikacija, privatnost se odnosi na pojedinčevu mogućnost kontrole prikupljenih podataka, kao i onih koje sam ostavlja za sobom u obliku digitalnog traga. Uobičajeno je da korisnik dobrovoljno razmjenjuje neki dio svojih podataka za odabranu prednost, na čemu se temelje korisnički računi na društvenim mrežama, web trgovine koje traže podatke o korisnikovim karticama, pretplate na multimedijske servise, dozvole korištenja kolačića trećih strana radi prikazivanja relevantnijih oglasa i slično. No s porastom mogućnosti ovakve vrste razmjene, ujedno rastu i rizici od povrede privatnosti, kao i mnogi drugi sigurnosni rizici. [1, str. 61-70]

3.2. Politika privatnosti i praćenje na primjeru Facebooka

S više od dvije milijarde mjesečno aktivnih korisnika, Facebook je danas generalno najpopularnija društvena mreža na svijetu. 2004. godine razvio ga je Mark Zuckerberg u spavaonici kampusa sveučilišta Harvard, zajedno sa svojim kolegama kao neku vrstu društvenog eksperimenta te mu je svrha bila da bude interna društvena mreža za studente sveučilišta, no ubrzo se počeo širiti izvan predviđenih granica. [25, str. 27]

U počecima Facebooka, bilo je ljudi koji su bili mišljenja da bi svaki korisnik trebao imati dva odvojena profila – radni i društveni, no Zuckerberg se nikad nije slagao s tim. Namjerno ga je osmislio tako da bi korisnici na njemu spajali sve svoje djelomične internetske profile u jedan cjeloviti. Po njegovim riječima, svaki pojedinac ima jedan identitet te tako treba i predstaviti

radi očuvanja vlastitog integriteta. Preko Facebooka želi stvoriti otvoreniji svijet na kojem se ljudi neće bojati podijeliti veliku količinu osobnih informacija, no s druge strane konstantno ponosno ističe činjenicu kako je Facebook od svojih početaka svojim korisnicima pružao mogućnost da sami precizno odrede s kim će dijeliti sadržaj. [25, str. 219-221]

Ovaj mu je paradoks više puta u prošlosti prouzročio probleme, od kojih je najrecentniji značajan onaj koji je počeo 2014., u kojem je velika količina podataka o korisnicima iz SAD-a bila prikupljena neovlašteno, bez njihove svijesti i dopuštenja, te su prikupljeni podaci bili iskorišteni za invazivno utjecanje na američke glasače pred izbore. Nakon skandala koji je ovo prouzročilo, 10. travnja 2018. Zuckerberg je sjeo na „vruću stolicu“ pred američki senat i odgovarao na brojna pitanja koja su mu senatori postavljali o mnogim temama vezanim uz Facebook i njegovu manjkavu politiku privatnosti. Ovo je dugi dokument na čije se uvjete korisnik pri registraciji na Facebook mora složiti. Postoji, međutim, visoka vjerojatnost da velika većina budućih korisnika ne pročita uvjete na koje pristaje, ni u trenutku registracije, a ni kasnije. Nadalje, nekoliko senatora istaknulo je da je Facebookova politika privatnosti poprilično opširan dokument, te da je uz to poprilično nejasan čak i pravnicima, a kamoli prosječnom korisniku.

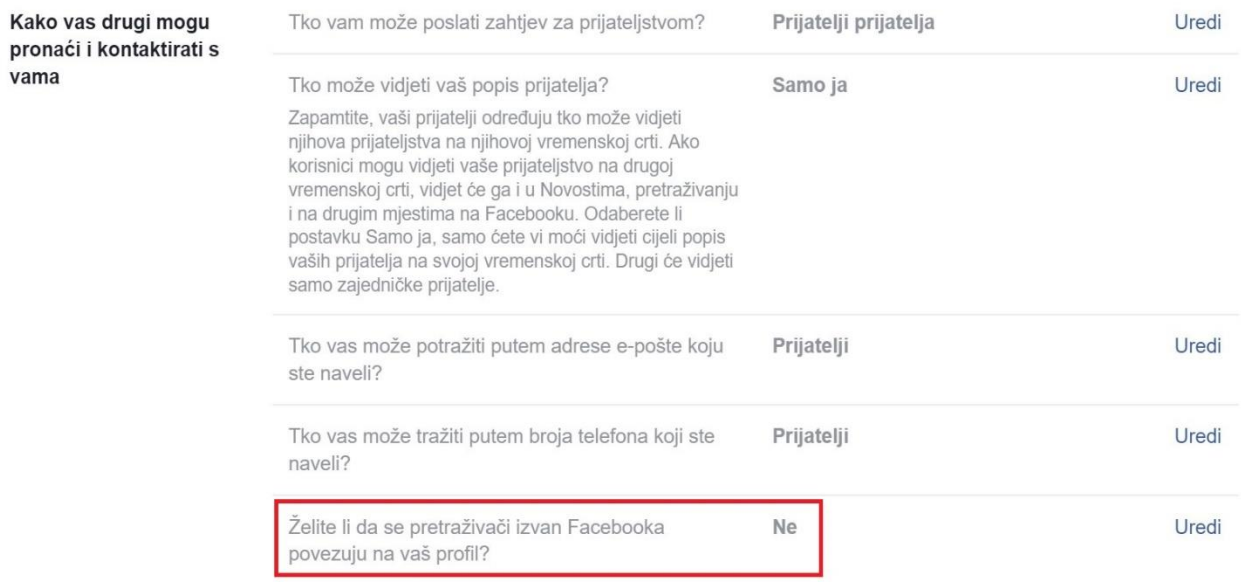
Zbog problema koje je njegovoj tvrtki donijela interna regulacija, po pitanju regulacije izvana Zuckerberg je više puta istaknuo da nije protiv regulacije općenito, već za primjerenu, racionalnu regulaciju, te se slaže da su Europljani „napravili dobar posao implementacijom GDPR-a“. [26]

Od drugih važnih pitanja može se istaknuti kako je Zuckerberg, na pitanje prati li Facebook korisničku aktivnost čak i kad je korisnik odjavljen s Facebook računa, odgovorio da ljudi koriste kolačiće na Internetu, te da se tako može povezati i korisnička aktivnost među sesijama. Kao primarnu svrhu takvog sistema navodi sigurnost (kod sustava prijavljivanja i upravljanja računima) te, naravno, poboljšanje korisničkog iskustva s oglašavanjem. Kad je upitan povezuju li se pojedini korisnički računi među različitim uređajima, objasnio je da Facebook radi upravo tako – povezuje korisnikov račun kroz više uređaja na koje se on prijavio da mu se ne bi prikazivali identični oglasi na svakom pojedinom uređaju, te da bi se sinkronizirali njihovi podaci koji se razmjenjuju između Facebooka i njegovih partnera, poput Instagrama. Na pitanje skuplja li Facebook pasivno podatke poput audio zapisa s mobilnih uređaja, odgovorio je negativno, no na pitanje prikuplja li Facebook metapodatke o drugim korištenim aplikacijama na mobilnom uređaju nekog korisnika, metapodatke o geografskoj lokaciji, komunikacijama i

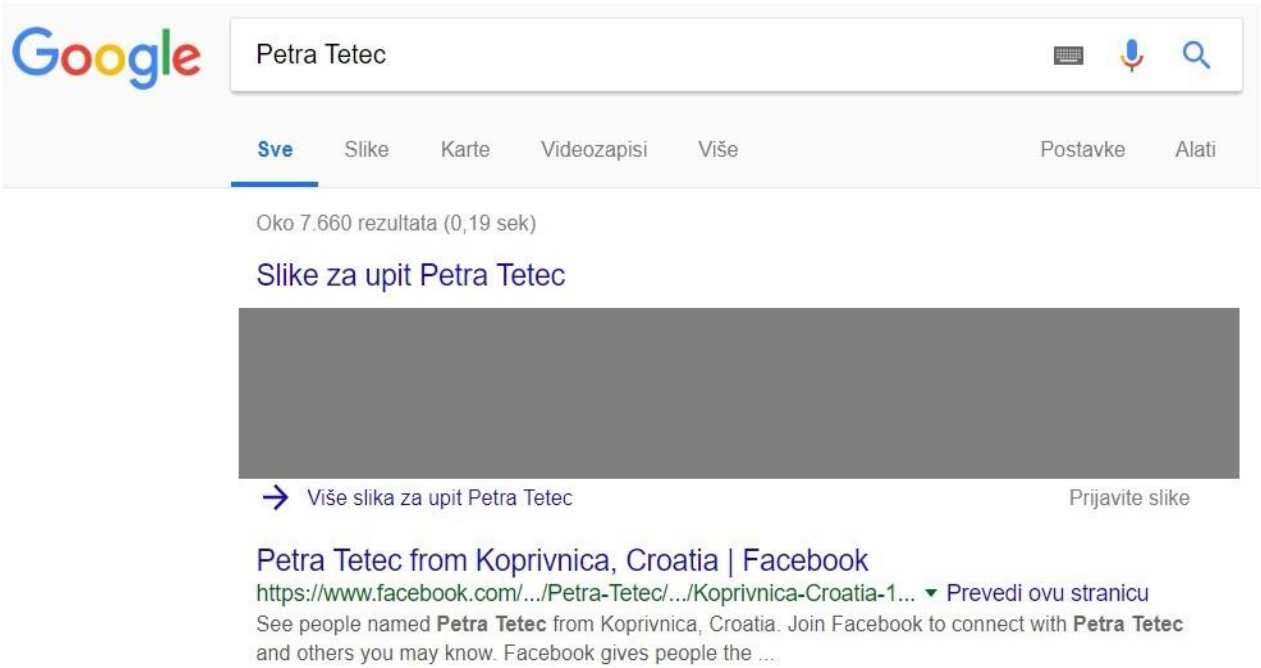
slično nije znao dati konkretan odgovor. I mnoga su druga važna pitanja ostala neodgovorena: koliko dugo treba Facebooku da u potpunosti obriše nečije podatke nakon brisanja korisničkog računa, obavještavaju li se korisnici kad dođe do nekog sigurnosnog napada ili druge vrste aktivnosti koje ugrožavaju privatnost korisničkih podataka, može li se sadržaj komunikacija preko Facebooka pročitati interno (unutar same tvrtke) u jasnom, nekriptiranom obliku te mnoštvo drugih. [26]

Nadalje, u politici privatnosti navedeno je da Facebook detaljno skuplja metapodatke o uređajima na kojima je korišten, poput jakosti signala, dostupne memorije, razine napunjenosti baterije, specifikacija operacijskog sustava, pokreta miša, identifikatora raznih vrsta, jezika, vremenske zone, informacija o uređajima koji se nalaze blizu trenutno korištenog, informacije pohranjene u kolačiće te još mnoge druge. Ne pojašnjava se kojim se mehanizmima dolazi do svih ovih informacija, no iz priloženog se vidi da i nema tolik značaj kad korisnik onemogući aplikaciji pristup mikrofonu, kameri, SMS porukama i slično, jer se svi prikupljani metapodaci ionako pohranjuju automatski. [27]

Na kraju, Zuckerberg oduvijek ističe kako svaki pojedini korisnik sam određuje koje informacije objavljuje kome te da ima apsolutnu kontrolu nad njima. Međutim, i ovdje se očituje ozbiljan sigurnosni propust. Korisnik zaista može određivati vide li njegove objave i fotografije samo prijatelji, prijatelji njegovih prijatelja ili javnost. No problem se javlja kod postavke vezane uz privatnost korisnika izvan Facebooka. Postoji postavka koja pita korisnika „Želite li da se pretraživači izvan Facebooka povezuju na vaš profil?“, na što korisnik može dati binaran odgovor. Čak i ako je na pitanje korisnik odgovorio negativno, kad se pokuša naći preko Googlea, među prvim će poveznicama biti ona na Facebook profil s traženim imenom. Ali ne samo da Google pronalazi specifičan korisnikov profil, već ispisuje i podatke poput mjesta stanovanja, koje je korisnik na Facebooku zaključao od pogleda javnosti. Ako se korisnik želi obratiti korisničkoj službi Facebooka radi prijave ovakvog problema, ne može to učiniti, već može naći samo ponuđene gotove odgovore na „često postavljena pitanja“. [podaci iz osobnog iskustva autorice]



Slika 1. Postavka privatnosti pretraživača izvan Facebooka (izvor: izrada autorice)



Slika 2. Kršenje eksplicitno konfigurirane gore prikazane sigurnosne postavke (izvor: izrada autorice)

3.3. Kršenje prava na privatnost – NSA i globalni nadzor

Nakon što se stekne uvid u Facebookovu zaštitu korisničke privatnosti, može se zaključiti da svaki korisnik ima razloga za zabrinutost, no očigledni su Facebookovi problemi i propusti tek vrh ledenjaka neovlaštenog prikupljanja i korištenja korisničkih podataka.

Velik je broj ljudi koji danas znaju priču o Edwardu Snowdenu, bivšem CIA-inom i NSA-inom zaposleniku koji je, radeći tamo, ostao zapanjen dubinom pristupa koji NSA ima pojedincima, ne samo onima u Sjedinjenim Američkim Državama, već po cijelom svijetu, uz izgovore otkrivanja terorizma i drugih prijetnji nacionalnoj sigurnosti. Nije se sve ljude pratilo jednakim intenzitetom, no logika je bila sljedeća: pod sumnjom u terorističku aktivnost nekog pojedinca, pratile su se sve komunikacije koje je imao sa svim svojim kontaktima. Nadalje, pratile su se komunikacije koje su njegovi kontakti imali sa svojim kontaktima, a u trećem takvom skoku broj praćenih pojedinaca koji su na neki način povezani sa sumnjivcem narastao je do nekoliko milijuna običnih ljudi, koji su vodili obične živote, nesvjesni da se svaka njihova mrežna interakcija nadzire i da je u svakom trenutku dostupna za pregled u jasnom obliku. [28]

Ovo se provodilo uz pomoć specijaliziranih sustava poput Prism-a, XKeyscore-a i mnogih drugih, koji su funkcionirali putem senzorskih mreža distribuiranih diljem cijelog svijeta, od kojih je svaka pretraživala vlastitu bazu podataka da nađe rezultate za upit koji postavlja zaposlenik NSA-e. Ovo nije uključivalo samo metapodatke, već i nekriptirani sadržaj svih komunikacija zabilježenih u prošlih nekoliko dana (čiji vremenski raspon se konstantno povećava s povećanjem kapaciteta baza podataka). [29]

Snowden je shvatio kako se kod globalnog nadzora ne radi o sprečavanju terorizma koji se čitavo vrijeme navodi kao izgovor, već o nadmoći onih na vlasti te o ekonomskoj i društvenoj kontroli masa. Oko polovice 2013. godine, neautorizirano je iz NSA-e iznio na tisuće povjerljivih dokumenata koje je predao novinarima iz The Guardiana i The Washington Posta, te koji su bili analizirani i pretvoreni u članke koji javnosti vrlo specifično i tehnološki objašnjeno opravdavaju prethodne sumnje o mogućnostima globalnog nadzora. U intervjuu, kojeg je dao novinarima Glennu Greenwaldu i Ewenu MacAskillu iz Guardiana kad se potajno našao s njima u Hong Kongu i predao im ukradene povjerljive dokumente, Snowden objašnjava kako svojim postupcima nije namjeravao oštetiti Sjedinjene Američke Države na bilo koji način, već je postupio tako kako jest da bi upozorio javnost diljem cijelog svijeta koliko im je zapravo privatnost ugrožena. Želio je da javnost, u duhu demokracije, sama bude omogućena

da izrazi svoje mišljenje o opravdanosti i etičnosti ovakvog invazivnog prodiranja u privatnost svakog pojedinca s pristupom mreži. [30]

Kako se sam izrazio, Snowdenov je najveći strah u trenutku pred objavljivanje bio da se ništa neće promijeniti – da će svijet vidjeti kakve su mjere američka vlada i razna internacionalna upravna tijela spremni poduzeti za postizanje jače kontrole masa, da će prihvatiti situaciju i ostati pasivni, umjesto da riskiraju i izbore se za radikalne promjene u pristupu vlasti prema čitavom društvu.

Globalna se svijest o čuvanju privatnosti podataka od 2013. u nekoj mjeri pojačala, iako se ništa značajnije nije promijenilo u sustavu. Ne postoji garancija da se itko na kog se NSA namjeri može sakriti od nje, no postoje mjere koje običan, prosječan korisnik weba može primijeniti u svom svakodnevnom životu te tako istovremeno zaštititi vlastitu privatnost i sigurnost.

4. Vodič za privatnije pretraživanje weba

Među svim postojećim mehanizmima i tehnologijama za praćenje te novima koji će se nastaviti pojavljivati u budućnosti, teško je držati korak ukoliko se korisnik želi zaštititi od invazivnih akcija usmjerenih prema njegovim podacima. No postoje određene metode i alati koje olakšavaju vlastitu anonimizaciju na webu. U nastavku su predstavljene neke od najpoznatijih i najučinkovitijih, ne samo unutar preglednika, već i u drugim oblicima korisnikovih interakcija s webom.

4.1. Infrastrukturne i konceptualne razlike između Interneta, weba, dubokog weba i tamnog weba

Mnogi ljudi još i danas koriste pojmove Interneta i weba kao sinonime. U stvarnosti Internet obuhvaća mnogo više od samog weba, no ne i obrnuto. U nastavku se izlažu detaljnija objašnjenja pojmova i bitne razlike među njima.

4.1.1. Internet

Internet je fizička mrežna infrastruktura koja kablovima i bežičnim signalima povezuje računala, mobitele i razne druge elektroničke uređaje diljem svijeta. U svojim se počecima koristio u akademske svrhe, za povezivanje raznih institucija koje su se bavile istraživanjem, a u 90-im godinama prošlog stoljeća svakim ga je danom koristilo sve više običnih ljudi. Ne postoji jedna osoba ili vlada koja posjeduje Internet, no postoje pravila i standardi koji određuju kako se ljudi spajaju na Internet u pojedinim dijelovima svijeta te do kojeg sadržaja mogu ili ne mogu doći. [31]

4.1.2. Web

Web je dio mreže sa sadržajem koji je dostupan navigiranjem po preglednicima (poput Chromea, Edgea, Firefoxa i dr.). Web stranice moraju biti posebnog formata te se međusobno povezuju poveznicama, oslanjajući se tako na HTTP (Hyper Text Transfer Protocol). One mogu sadržavati tekst s raznim informacijama, grafiku, slike, video i sličan sadržaj koji u određenoj mjeri može biti interaktivan, razlikujući tako statične i dinamične stranice.

Ako se odnos Interneta i weba opiše metaforički kao slika željezničkog prometa, Internet se može prikazati kao tračnice, odnosno infrastruktura za transport, kroz koje prolaze

novi brzi vlakovi, spori putnički vlakovi, teretni vlakovi, vozila za održavanje i popravke pruge i slično. Web je u kontekstu ove slike samo jedna vrsta vlakova. [32, str. 35-36]

Tako osim web stranica, Internet sadrži razne servise za elektroničku poštu, istovremene poruke, telefonske razgovore (VoIP), ažuriranje softvera, razmjenu datoteka i slično, koji se oslanjaju na druge specifične protokole (FTP, SMTP). [31]

4.1.3. Deep web, Dark web

Deep web, odnosno duboki web, često se u medijima opisuje kao mjesto na Internetu na kojem se događaju mračne stvari poput trgovanja na crnom tržištu, no to je samo manjim dijelom točno. Pojam dubokog weba podrazumijeva neindeksirani dio weba, odnosno onaj dio koji tražilice neće pronaći. Pod time se podrazumijeva velika većina sadržaja weba, koji nije indeksiran jednostavno radi lakšeg snalaženja korisnika u nezamislivo velikom moru sadržaja koji postoji na webu, a koji nije relevantan širokom spektru korisnika. Dijelovima dubokog weba može se pristupiti putem unutarnjih pretraživača ili filtera nekog web mjesta (kao kod traženja autobusnih linija ili cijena noćenja u hotelu na određeni datum), preko izravnih poveznica ako korisnik dođe do njih ili preko korisničkog imena i lozinke. Kako u to ulaze profili na društvenim mrežama, računi elektroničke pošte, bankovni računi korisnika i slično, lako je shvatiti kako duboki web čini veći dio weba (preko 90%), koji nije dostupan bilo kome. [33]

Dark web (ili mračni web) nije nužno toliko mračan koliko ljudi pretpostavljaju i koliko mu ime govori, već je zapravo jedan od puteva postizanja korisničke privatnosti. Dark web je podskup dubokog weba koji se obično nalazi na specijaliziranim podmrežama, od kojih je najpoznatija Tor mreža. Inicijalna svrha dark weba bila je omogućavanje anonimnog pristupa webu, kako bi se njegovi korisnici zaštitili od ikakve vrste špijuniranja, kako bi zaštitili tajnost svoje lokacije ili pristupali web mjestima kojima je u pojedinim (diktatorskim) zemljama zabranjen pristup. Ovakav pristup sam po sebi nije osmišljen da bi služio ikakvoj zloj svrsi, no nezaobilazno je rezultirao takvim posljedicama. Tako je dark web danas bogat korisnicima koji ga koriste s namjerom izvođenja kriminalnih radnji uz skrivanje vlastitog identiteta. [34]

4.2. Poboljšanje privatnosti unutar preglednika

Logično je početi s metodama koje će pomoći korisniku postići potpunu ili djelomičnu anonimnost na izravnoj točki dodira s mrežom – unutar preglednika koji koristi.

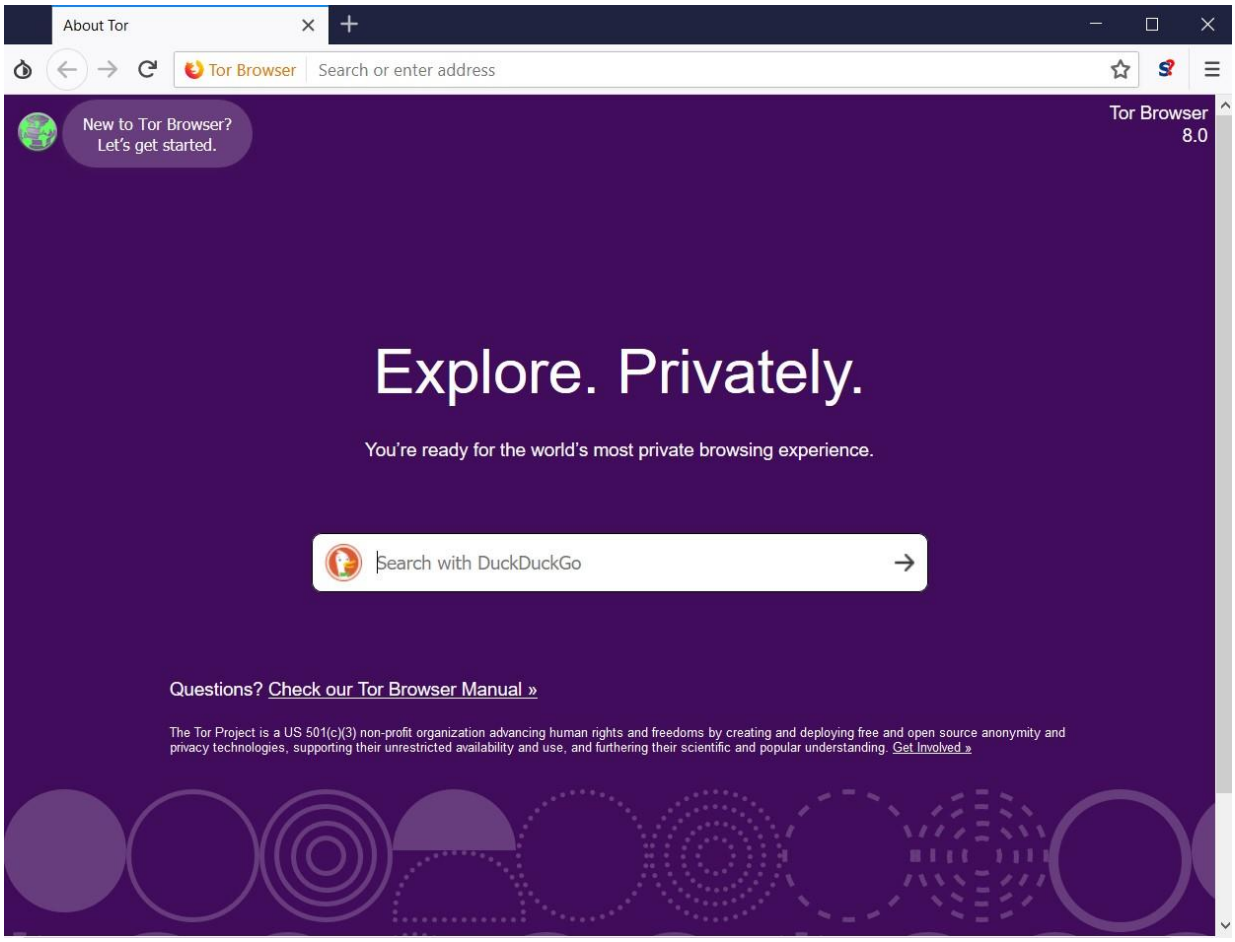
4.2.1. Tor

Tor (akronim od *The Onion Router*) je besplatna, otvorena mreža koja korisniku pomaže osigurati anonimnost kod pretraživanja. Koristi se u obliku preglednika s postavljenom DuckDuckGo tražilicom, kojeg korisnik skida na vlastito računalo te pokreće u novom prozoru. Tor radi tako što kriptira korisnikov promet te ga preusmjerava do zatraženog odredišta preko čvorova preklapajuće mreže na globalnoj razini, do te razine na kojoj je gotovo nemoguće provoditi nadzor mreže ili analizirati mrežni promet, čime je osigurana anonimnost, ojačana korisnikova sigurnost te skinuta cenzura pojedinih dijelova weba.

Odmah po pokretanju Tor preglednika, on sam preporuča korisniku da ne maksimizira prozor do veličine punog ekrana, jer i dimenzije ekrana predstavljaju parametar prema kojem se može identificirati korisnika. Reagira nešto sporije od konvencionalnih preglednika, što ne iznenađuje kad je poznato kako on radi. Izolira kolačiće koje web mjesta nameću korisniku, a nakon svake korisnikove pretraživačke sesije automatski briše povijest pretraživanja.

Osim zadanih sigurnosnih postavki (poput automatskog onemogućavanja Flasha), Tor nudi korisniku dodatnu prilagodbu koja uključuje onemogućavanje JavaScripta na svim stranicama koje nemaju pouzdan certifikat (ili na svim stranicama koje korisnik posjećuje), onemogućavanje pojedinih znakova i fontova te isključivanje automatske reprodukcije audio i video sadržaja. Još je jedna značajna Torova prednost to što u svojoj infrastrukturi nema jednu točku kvara (*single point of failure*).

Sve su bitne postavke automatski konfigurirane te se u Tor preglednik ne moraju dodavati nikakva nova proširenja. Jedina mu je primjetna mana smanjena brzina, no korisnik će sam odrediti vrijedi li malo dulje pričekati na prikaz rezultata u zamjenu za značajno jačanje vlastite privatnosti i sigurnosti. [35]



Slika 3. Izgled početne stranice Tor preglednika (izvor: izrada autorice)

4.2.2. VPN

Virtualna privatna mreža ili VPN (*Virtual Private Network*) pojam je koji opisuje povezivanje dva uređaja preko Interneta, bez obzira na to koliko su međusobno fizički udaljeni, na takav način da mogu komunicirati kao da se nalaze u istoj lokalnoj mreži. To znači da će interakcija sa svakim web mjestom izgledati kao da dolazi iz lokalne mreže tog istog mjesta. Analogno, korisnikova IP adresa neće biti njegova stvarna IP adresa, već će izgledati kao IP adresa korištenog VPN-a. Adresa koju će vidjeti korisnikov ISP (*Internet Service Provider*) bit će ona koja je postavljena između korisnika i VPN servisa, no u kriptiranom obliku.

VPN-ovi se koriste kad korisnik želi sakriti svoju IP adresu i svoju aktivnost na webu, bez da ga blokira firewall ili bilo koja vrsta cenzure, kad želi pristup web mjestu koje ne dopušta pristup pojedinim zemljama te kad koristi javnu, nesigurnu mrežu te ne želi ugroziti privatnost podataka koje šalje ili prima. [36]

Neki od pružatelja VPN usluge su NordVPN, Private Internet Access, ExpressVPN, Anonymizer, TorGuard, IPredator te mnogi drugi, a kriteriji po kojima ih korisnik može birati su cijena, način naplačivanja, način implementacije, podrška pojedinih protokola za dijeljenje podataka, količina bilježenih podataka o korisnicima i drugo.

4.2.3. Blokiranje servisa za oglašavanje; ad-blockeri i druga proširenja

Kolačići trećih strana prisutni su na velikom broju web stranica te invazivno djeluju na korisnikovu privatnost. Na svakoj web stranici koja sadrži Facebookov „sviđa mi se“ gumb, Facebook se ponaša kao treća strana koja prikuplja korisnikove podatke bez ikakve direktne veze sa samom društvenom mrežom te korisnik od njega nema nikakvu značajnu korist. Za usporedbu, Google ima ulogu treće strane na još većem broju web stranica, s jednakim učinkom. Zbog takvih stvari postoje razni servisi i proširenja, koji često dobivaju i nove funkcionalnosti.

Jedno od trenutno najpopularnijih proširenja za preglednike je Privacy Badger, kompatibilan s Firefoxom (uključujući verziju za Android) te, od nedavno, s Chromeom i Operom. Privacy Badger je besplatno proširenje koje korisnik skida i dodaje u preglednik, a koje ga štiti od kolačića trećih strana koji dolaze s ugrađenim dodacima za praćenje (*trackers*). Funkcionira na principu samoučenja, što znači da će na početku korištenja biti prazan, a s vremenom i količinom generiranog mrežnog prometa, naučit će blokirati određene stavke na određenim web mjestima. Ima tri glavne postavke za svaki tracker – dozvoljavanje pojedine domene na trenutnoj stranici, blokiranje kolačića pojedine domene te kompletno blokiranje pojedine domene. [37]

Slično proširenje prethodnome je Ghostery. Ghostery je također besplatan, kompatibilan s još većim brojem preglednika te ima malo proširene mogućnosti, koje uključuju još i provjeravanje JavaScript koda kako bi se blokirali trackeri koji su drugačije nevidljivi korisniku, a koji mogu skupljati podatke o korisniku u HTTP kolačiće, kao i pratiti njegov digitalni otisak prsta. Također, slično principu ažuriranja antivirusnog softvera, Ghostery se konstantno ažurira i pamti novonastale skripte za praćenje da bi ih kod idućeg posjeta web mjestu mogao automatski onemogućiti. [38]

Ova proširenja dobro je koristiti u kombinaciji s ad-blockerom po izboru: AdBlock, Adblock Plus, AdGuard, Fair AdBlocker, uBlock, Social Network Adblocker, Adaware Ad Block, Facebook Adblock te mnogi drugi koji funkcioniraju na sličnom principu.

4.2.4. Privatni način pretraživanja

Privatni način pretraživanja (*Incognito mode*) posebna je modifikacija pojedinih preglednika, koja isključuje pohranjivanje povijesti pretraživanja, onemogućava spremanje u web predmemoriju, pohranu podataka u kolačiće (što uključuje popunjavanje obrazaca, lozinke itd.) te u Flash kolačiće. Anonimnost je u ovom načinu pretraživanja samo lokalna – ne skriva aktivnost korisnika od ISP-a, poslodavca ili obrazovne ustanove, kao ni od web stranica koje korisnik posjeti. Oznake favorita te datoteke koje korisnik skine tijekom sesije privatnog pretraživanja ne mijenjaju se nakon zatvaranja prozora. [39]

Ovaj način pretraživanja može se koristiti kad korisnik želi obaviti pretraživanje na koje neće utjecati nikakvi prethodno spremljeni podaci, uključujući povijest pretraživanja, kad ne želi da mu preglednik pamti korisničko ime i lozinku putem Smart Locka, kad se istovremeno želi prijaviti u više računa odjednom, kad želi testirati neku web stranicu ili kad gleda sadržaj za koji jednostavno ne želi da ostane pohranjen u povijesti pretraživanja.

Privatni način pretraživanja otežava ili onemogućava identifikaciju korisnika kod jednostavnijih mehanizama praćenja (mehanizmi temeljeni na skladištenju i predmemoriji) te kod nekih naprednijih (poput evercookiesa i vremenskih napada), a generalno je mnogo učinkovitiji kod Chromea, Firefoxa i Internet Explorera nego kod Safarija.

4.2.5. Konfiguriranje postavki unutar preglednika

Postoji posebna stranica s postavkama za svaki preglednik (chrome://settings/ za Google Chrome), na kojoj korisnik može personalizirati izgled preglednika, jezik i ostale generalne postavke, no također ima pristup popisu spremljenih kolačića te predmemoriji, što oboje valja što češće čistiti.

Za svaku je stranicu pojedinačno moguća prilagodba postavki unutar nekog preglednika. Između ostalog, postavke omogućuju blokiranje pojedinih aspekata poput pristupa lokaciji uređaja, kamere, mikrofona, JS-a i Flasha, oglasa, pop-up prozora, zvuka i slično. Korisnik ovdje može sam odrediti vjeruje li nekom web mjestu dovoljno da mu dopusti izvođenje JS skripti ili pristup kameri. No za neke se stvari, poput Flasha i skočnih prozora, uglavnom preporuča blokiranje.

Relativno nova postavka privatnosti unutar preglednika zove se Do Not Track – posebno HTTP zaglavlje koje zahtijeva od web mjesta da ne prati korisnika. Ovu su opciju uveli svi glavni preglednici, no da bi ona funkcionirala na zamišljen način, potreban je pristanak strane

koja prati, za čije provođenje ne postoji velika vjerojatnost. Također postoji i postavka za blokiranje kolačića trećih strana, no analogno prethodnoj, upitno je koliko je ona zapravo učinkovita – korisnik bi umjesto vjerovanja ovim postavkama trebao instalirati specijalizirana proširenja.

4.2.6. Generalni savjeti za ponašanje unutar preglednika

Osim gore navedenih, pouzdanih i provjerenih metoda, korisnik bi sam trebao istraživati mogućnosti poboljšanja vlastite privatnosti i sigurnosti kod pretraživanja weba te ponekad razmišljati izvan okvira.

Ne bi se trebalo vjerovati stranicama čiji URL počne s „http“ umjesto „https“. HTTPS protokol uključuje enkripciju komunikacijskog protokola korištenjem TLS-a (*Transport Layer Security* - kriptografski protokol za sigurnost transportnog sloja), koji provjerava autentičnost web stranice kojoj korisnik pristupa te štiti privatnost i integritet razmijenjenih podataka, štiteći korisnika od napada posrednika koji pokušava presresti komunikaciju. Nikad nije dobra ideja unositi povjerljive podatke poput brojeva kreditnih kartica ili lozinki korisničkih računa u obrasce na stranicama koje ne koriste TLS.

Svugdje gdje je to moguće, korisnik bi trebao izbjegavati povezivanje više računa na jedan mail, korištenje jednakog korisničkog imena (i lozinke), pa čak i slike na više različitih mjesta na webu. Korištenje stvarnog imena i slike također valja izbjeći gdje je to moguće. Povezivanje na razne servise preko Facebooka ne treba posebno ni isticati. Za različite korisničke račune dobro je napraviti više email računa, a za manje bitne račune ili one koje će korisnik koristiti samo jednom ili nekoliko puta, postoji mogućnost izrade privremenog emaila.

Bitno je paziti i na postavke automatskog povezivanja na javno dostupnu WiFi mrežu, u kojoj mogu ležati ozbiljne sigurnosne prijetnje poput malicioznog špijunskog softvera.

Na kraju, najbolja je zaštita oprezno rukovanje osobnim podacima, prilagođavanje postavki korisničkih računa, konstantno vlastito informiranje o politikama privatnosti korištenih servisa na webu, o starim i novim oblicima prijetnji privatnosti te obrazovanje o potencijalnim metodama vlastite obrane.

4.3. Briga za osobnu privatnost i sigurnost u ostalim komunikacijama

Kao na osobnim računalima, i na mobitelima treba pomno birati aplikacije kojima korisnik može vjerovati. Važno je ne davati pristup nekom aspektu aplikacijama koje taj pristup ne trebaju. GPS uređaja logično je isključiti kad ga korisnik izravno ne koristi. Za zaključavanje zaslona dobro je imati nevidljiv uzorak da ga se izvana teže zapamti, a potencijalno osjetljive podatke na uređaju također je dobro zaštititi lozinkama. Kao i na računalima, važno je često čistiti predmemoriju i kolačiće.

Kao sigurniji oblik komunikacije s osobnim kontaktima, korisnik može instalirati aplikacije s jačom implementacijom sigurnosnih mjera, poput enkripcije od kraja do kraja, što osigurava da potencijalni posrednik koji presretne komunikaciju između dvije strane istu ne može dekriptirati, a takva mu ne vrijedi mnogo. Danas postoje kvalitetni messengeri za sigurniju komunikaciju, poput Wirea i Signala, koji ne skupljaju više osobnih podataka nego bi trebali i nisu povezani ni s kojim većim servisom, društvenom mrežom ili institucijom, već su sami sebi svrha. Analogno, korisnik može koristiti PGP enkripcijski program koji osigurava privatnost i integritet kod prijenosa podataka poput mailova i drugih vrsta poruka.

Na kraju, ako je korisnik paranoičan u vezi neovlaštenog pristupa trećih strana njegovoj kameri na raznim uređajima, uvijek može takve probleme riješiti mehanički (prekrivanjem kamera).

5. Zaključak

S konstantnim razvojem tehnologije, čitavom se svijetu svakodnevno otvaraju nove mogućnosti – smanjuju se fizičke udaljenosti, olakšava se pristup informacijama i pruža se mogućnost gubljenja samog sebe u satima besciljnog lutanja webom ili u satima provedenim u nekoj aktivnosti osmišljenoj za zabavu. Sve ove i mnoge druge mogućnosti služe kao mamac masama koje se svaki dan priključuju na veliku mrežu i postaju sve ovisniji o njoj. Struktura društva se mijenja, a ponašanje svakog se pojedinca na neki način programira, čeg korisnici nisu svjesni jer se promjena događa vrlo postepeno i na vrlo velikoj skali. No istina je da čitav ljudski rod postaje sve predvidljiviji, do točke gdje se ponašanje masa može izračunati algoritmima. Ovakav sustav pogoduje razmjeni – razmjeni informacija i znanja, razmjeni dobara, usluga, novca i vremena – te pretvara čitav svijet u masivnu globalnu tržnicu. Onima koji prodaju ovakvo stanje stvari pogotovo odgovara; govori se o prilagodbi čitave ponude kupcu, o prilagodbi oglasa, prilagodbi cijena, o poboljšanju čitavog korisničkog iskustva. Korisnik tako postaje naivan i, zaveden ponudama koje su krojene posebno za njega, zaboravlja razmišljati o tome zašto mu toliko pružatelja usluga daje svoje usluge na pladnju, besplatno. Zaboravlja razmišljati o tome da je on sam imovina, najvrjednija imovina koju mnogi web servisi, a pogotovo društvene mreže posjeduju i čiju privatnost kupuju u zamjenu za neznatan popust zbog kojeg će se sam korisnik osjećati posebno. Nije ni svjestan kome će prikupljeno znanje o njemu biti dostupno, te što oni koji posjeduju to znanje s njime rade.

Kad pojedinac shvati kako taj dio sustava funkcionira i kako utječe na njega, kad je prikupio dovoljno informacija da sam može prosuđivati isplati li se njemu prihvaćati ovakav sustav, tek tad može učiniti nešto da se zaštiti.

Postoje mnoga rješenja za obranu vlastite privatnosti i sigurnosti. Mnoga su od njih jednostavna i nadohvat ruke svakom prosječnom korisniku weba. No najbolji je način za očuvanje privatnosti konstantna edukacija samog sebe i drugih oko sebe, krenuvši od razuvjeravanja pojedinaca u istinitost toliko ponavljane tvrdnje o samima sebi kako „nemaju što sakriti.“ Edward Snowden najjednostavnije je to objasnio rekavši da je „govorenje kako vas nije briga za privatnost jer nemate što sakriti kao da kažete da vas nije briga za slobodu govora jer nemate što reći.“ Svatko bi trebao uzeti stvari u svoje ruke i poticati onog do sebe da čini isto. U tom se slučaju svijet idućih generacija ne bi pretvorio u paradoksalnu kombinaciju Orwellovog svijeta u kojem ljude uništava kontrola potpomognuta strahom, te onog Huxleyjevog, u kojem ljude uništava kontrola pomoću onog u čemu uživaju.

Literatura

[1] D. Dobrinić et al., *Marketing i baze podataka.* Varaždin: Fakultet organizacije i informatike, 2011.

[2] S. Datt, *Mrežna forenzika*. Zagreb: Dobar plan, 2016.

[3] Google support, *How a web session is defined in Analytics*, Dostupno: https://support.google.com/analytics/answer/2731565?hl=en [posljednje pristupano 21.08.2018.]

[4] Java papers, *Session Tracking Methods*, [blog post] Dostupno: https://javapapers.com/servlet/explain-the-methods-used-for-session-tracking/ [posljednje pristupano 21.08.2018.]

[5] T. Bujlow, V. Carela-Español, J. Solé-Pareta, P. Barlet-Ros, „Web Tracking: Mechanisms, Implications, and Defenses“ [na Internetu], 2014., Dostupno: https://arxiv.org/pdf/1507.07872v1.pdf [posljednje pristupano 03.09.2018.]

[6] W3, „What is the Document Object Model?“ [na Internetu], Dostupno: https://www.w3.org/TR/WD-DOM/introduction.html [posljednje pristupano 21.08.2018.]

[7] MDN web docs, *HTTP Cookies*, Dostupno: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies [posljednje pristupano 22.08.2018.]

[8] Google policies, *Koje vrste kolačića upotrebljava Google*, Dostupno: https://policies.google.com/technologies/types?hl=hr [posljednje pristupano 22.08.2018.]

[9] Adobe Blog, *Flash & The Future of Interactive Content* [blog post], Dostupno: https://theblog.adobe.com/adobe-flash-update/ [posljednje pristupano 22.08.2018.]

[10] G. Fleischer, „Implementing Web Tracking“ [na internetu], 2012., Dostupno: https://media.blackhat.com/bh-us-12/Briefings/Fleischer/BH_US_12_Fleischer_Implementing_Web_Tracking_gfleischer_WP.pdf [posljednje pristupano 27.08.2018.]

[11] Visolve, „Optimized Bandwidth + Secured Access = Accelerated Dana Delivery; Web Caching“ [na Internetu], 2009., Dostupno: http://www.visolve.com/uploads/resources/ViSolve_Web_Caching.pdf [posljednje pristupano 29.08.2018.]

[12] WhatIsMyIPAdress, *What is the Domain Name System (DNS)?* [blog post], Dostupno: https://whatismyipaddress.com/dns[posljednje pristupano 03.09.2018.]

[13] B. Mitchell, *DNS Caching and How It Makes Your Internet Better* [blog post], 05.09.2018., Dostupno: https://www.lifewire.com/what-is-a-dns-cache-817514 [posljednje pristupano 02.09.2018.]

[14] J. Grossman, *Tracking users with Basic Auth* [blog post], 20.04.2007., Dostupno: https://blog.jeremiahgrossman.com/2007/04/tracking-users-without-cookies.html [posljednje pristupano 03.09.2018.]

[15] J. Jia, (29.08.2016.) „I Know Where You've Been: Geo-Inference Attacks Via The Browser Cache“ *Youtube* [video datoteka], Dostupno: https://www.youtube.com/watch?v=lGb0AACAk1A [posljednje pristupano 04.09.2018.]

[16] Oracle Java Documentation, *What Applets Can and Cannot Do*, Dostupno: https://docs.oracle.com/javase/tutorial/deployment/applet/security.html [posljednje pristupano 05.09.2018.]

[17] B. Gellman, A. Blake, G. Miller, „Edward Snowden comes forward as source of NSA leaks“ [na internetu], 09.06.2013., Dostupno: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.dcd210e1571c [posljednje pristupano 07.09.2018.]

[18] J. Mayer, „MetaPhone: The Sensitivity of Telephone Metadata“ [na Internetu], 12.03.2014., Dostupno: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ [posljednje pristupano 07.09.2018.]
[19] M. Meillassoux, „Nothing to Hide“ [dokumentarni film], 2017., Dostupno: https://www.youtube.com/watch?v=M3mQu9YQesk [posljednje pristupano 09.09.2018.]
[20] P. Schwabe, „Timing Attacks and Countermeasures“ [na Internetu], 10.06.2016., Dostupno: https://cryptojedi.org/peter/data/croatia-20160610.pdf [posljednje pristupano 05.09.2018.]
[21] E. Chen, C. Jackson, P. R. Jayaraman, Z. Weinberg, „I Still Know What You Visited Last Summer“ [na Internetu], 2011., Dostupno: https://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper010.pdf [posljednje pristupano 06.09.2018.]
[22] OWASP, *Clickjacking*, Dostupno: https://www.owasp.org/index.php/Clickjacking[posljednje pristupano 06.09.2018.]
[23] D. Albright, „What Are Supercookies, and Why Are They Dangerous?“ [blog post], 25.03.2016., Dostupno: https://www.makeuseof.com/tag/what-are-supercookies-and-why-are-they-dangerous/ [posljednje pristupano 06.09.2018.]
[24] M. Hypponen, (07.11.2013.) „How the NSA betrayed the world's trust – time to act“ *Youtube* [video datoteka], Dostupno: https://www.youtube.com/watch?v=9CqVYUOjHLw [posljednje pristupano 07.09.2018.]
[25] D. Kirkpatrick, *Facebook efekt*. Zagreb: Lumen izdavaštvo d.o.o., 2012.
[26] The Washington Post, *Transcript of Mark Zuckerberg's Senate Hearing*, 10.04.2018., Dostupno: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing [posljednje pristupano 07.09.2018.]
[27] Facebookova pravila o upotrebi podataka, Dostupno: https://www.facebook.com/policy.php [posljednje pristupano 07.09.2018.]
[28] G. Dance, E. MacAskill, „NSA Files decrypted: Edward Snowden's surveillance revelations explained“, 01.11.2013., Dostupno: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [posljednje pristupano 08.09.2018.]
[29] E. Snowden, (16.09.2014.) „Snowden – XKEYSCORE“ *Youtube* [video datoteka], Dostupno: https://www.youtube.com/watch?v=K9yHAQtVNME [posljednje pristupano 08.09.2018.]
[30] E. Snowden, (09.07.2013.) „NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'“ *Youtube* [video datoteka], Dostupno: https://www.youtube.com/watch?v=0hLjuVyIIrs [posljednje pristupano 08.09.2018.]
[31] P. Gil, „The Difference Between the Internet and the Web“, 05.09.2018. Dostupno: https://www.lifewire.com/difference-between-the-internet-and-the-web-2483335 [posljednje pristupano 20.08.2018.]
[32] J. Naughton, *Od Gutenberga do Zuckerberga*. Zagreb: Edicije Božičević, 2014.
[33] M. Wilson, (22.06.2016.) „Secrets of the Deep Dark Web (Deep Dark Web Pt2) - Computerphile“, *Youtube* [video datoteka] Dostupno: https://www.youtube.com/watch?v=joxQ_XbsPVw [posljednje pristupano 08.09.2018.]
[34] B.P., „Deep i dark web“ [blog post], 05.09.2016., Dostupno: https://pcchip.hr/internet/deep-i-dark-web/ [posljednje pristupano 20.08.2018.]
[35] Tor Project, Dostupno: https://www.torproject.org/ [posljednje pristupano 09.09.2018.]
[36] S.M., „Što je VPN? Za što se koristi?“ [blog post], 20.12.2016., Dostupno: https://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/ [posljednje pristupano 09.09.2018.]
[37] EFF: Privacy Badger, Dostupno: https://www.eff.org/privacybadger [posljednje pristupano 09.09.2018.]

[38] Ghostery proširenje, Dostupno: https://www.ghostery.com/ [posljednje pristupano 09.09.2018.]
[39] Chromebook Help, *Browse in private*, Dostupno: https://support.google.com/chromebook/answer/95464 [posljednje pristupano 09.09.2018.]
[40] ip2location softver, Dostupno: https://www.ip2location.com/ [posljednje pristupano 03.09.2018.]

Popis slika

Popis tablica