SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2017./ 2018.

Matej Ljubić

Borba za privatnost podataka na internetu

Završni rad

Mentor: dr.sc. Kristina Kocijan

Zagreb 2018.

Sadržaj

Sažetak

Privatnost podataka sve je češća tema otkako je niz incidenata unazad pet godina pokazao da privatnosti na internetu imamo zapravo vrlo malo. Ovaj rad promotrit će neke od tih slučajeva ukazujući na problematiku privatnosti na internetu, kako GDPR pokušava utjecati na to stanje, te što kao korisnici možemo sami poduzeti kako bi se zaštitili ulazeći u doba semantičkog weba.

Ključne riječi: *privatnost, podaci, facebook, wikileaks, nadzor, GDPR, sigurnost, alati za zaštitu podataka*

The ongoing battle for online privacy

Abstract

Nowadays data privacy is being more and more discussed, since a series of incidents in the last five years showed us that there is actually very little privacy on the internet. This paper will look at some of these cases showing the issues of privacy online, how the GDPR tries to affect the current state of things, and what we as users can do to protect ourselves going into the age of the semantic web.

Key words: *privacy, data, facebook, wikileaks, surveillance, GDPR, safety, tools for data protection*

1. Uvod

Kada govorimo o privatnosti na internetu, referiramo se, ustvari, na sigurnost naših osobnih podataka poput kreditnih kartica, adrese i privatnih poruka od različitih vrsta napada hakera. Unazad pet godina pogled na privatnost se drastično promijenio počevši od Edwarda Snowdena, zvždača (engl. *whistleblower*) koji je razotkrio program prisluškivanja američke vlade u suradnji s najvećim tehnološkim tvrtkama, PRISM 2013. godine (Ball & Borger, 2013).

To je pokrenulo mnoge debate i niz drugih kontroverznih događaja koji su nam postepeno otkrivali kako je internet ulaskom u semantičko doba postao mjesto gdje smo svi izloženi nekoj vrsti špijunaže, bilo to od strane privatnih tvrtki, državnih institucija ili hakera. Metode su se isto promijenile. Prije su bile vezane uz računala s Windows operativnim sustavima (Skillings, 2006), sada su vezane uz bilo koji uređaj koji ima pristup internetu, a uz dovoljno truda može biti i lokalno hakiran puno lakše nego što je bivalo, objašnjava Schneier u svojoj knjizi (2015).

Smatram da je ova tema važna zbog same količine tehnologije koja trenutno postoji oko nas. Svaki dan koristimo računala i mobitele da nam olakšaju komunikaciju i automatiziraju stvari koje ručno zahtijevaju puno vremena. Korištenjem aplikacija, društvenih medija, stranica za kupovinu preko interneta i sličnog ostavljamo za sobom trag podataka iz kojega se puno može saznati o nama što ne bi nikako trebalo spadati u javno znanje. Kada izgubimo osobnu privatnost, gubimo pravo da budemo onakvi kakvi jesmo (Allen, 2015). Ovim radom pokušavam približiti ideju privatnosti pojedincu prikazujući kako je lako preko interneta utjecati na njih putem sadržaja, te da napadi na privatnost nisu briga samo ljudi u visokim rangovima već svih nas.

U prvom poglavlju baviti ću se temom uljeza: na koje načine se narušava naša privatnost preko društvenog medija Facebook, koja računalna oružja koristi američka organizacija CIA (*Central Intelligence Agency*), te kako je Facebook utjecao na važne demokratske odluke u 2016. godini. U drugom poglavlju analizirati ću nedavno doneseni

GDPR, što donosi sa sobom te kako se provodi u Hrvatskoj. U zadnjem ću poglavlju navesti mjere zaštite koje sami možemo poduzeti kako bi osigurali vlastitu privatnost i smanjili razinu prodora trećih strana u naše živote.

2. Uljezi

U ovom ću poglavlju navesti tri studije slučaja. Prva će proučavati Max Schremsa kao osobu koja je potaknula diskusiju u Europi oko nekompatibilnosti pravnih sustava američke i europske vlade na internetu. Druga će se baviti dokumentima iz 2017. godine zvanim „*Vault 7*" koji pokazuju koje probleme može prouzročiti velika koncentracija računalnog oružja na jednom mjestu. Naposljetku ću obraditi slučaj „*Cambridge Analytica*", tvrtke koja se bavila utjecajem na razne grupe ljudi preko društvenih medija kroz sadržaj.

2.1. Slučaj: Max Schrems protiv DPC-a

Studija iz 2010. (Hoofnage et al., 2010) pokazuje da samo 3% od skoro 1000 ispitanika zna da podaci koje ostavljaju za sobom na internetu mogu biti podijeljeni bez njihovog pristanka, da se podaci kao kupovine i poštanski brojevi mogu podijeliti s drugim opskrbljivačima, da se podaci ne mogu obrisati na želju korisnika, da nemaju mogućnost tužiti pružatelja usluge ako krši vlastite smjernice, te da ih se ne mora pitati ako se želi pratiti njihova aktivnost na drugim web-stranicama.

U 2011. godini Maximilian Schrems, tadašnji student fakulteta Santa Clara, odlučio je napisati seminarski rad o manjku znanja europskog zakona o privatnosti tvrtke Facebook, uočivši opasnost koju takve tvrtke predstavljaju. Zatražio je svoje podatke od Facebooka i zauzvrat je dobio CD s preko 1200 stranica podataka o sebi, uključujući točno sve što je ikada *lajkao,* svaku njegovu objavu i slične detalje. Time je pokrenuo val od preko 40 tisuća korisnika koji su tražili istu proceduru (EPIC, 2013).

Snowdenove tvrdnje u 2013. bile su glavni pokretač Schremsovog slučaja protiv povjerenika za zaštitu podataka. Schrems cilja zaustaviti Facebook od slanja podataka u SAD preko Irske[1] zbog sudjelovanja Facebooka u programu PRISM. Bazirao je svoju

1 Sjedište *Facebook* tvrtke u Europi

tužbu na tadašnjem europskom zakonu o zaštiti podataka, koji nije dozvoljavao prijenos podataka u zemlje koje nisu članice EU, osim ako osiguravaju propisanu zaštitu. No, slučaj je odbijen ("Data Protection Commissioner says no action", 2013).

U 2014. godini slučaj je prebačen pred Sud Europske Unije pošto su europski zakoni vezani uz privatnost smijenili irske zakone. U 2015. godini održalo se prvo saslušanje Suda Europske Unije, gjde Schrems tvrdi da principi Safe Harbor direktive nisu održani od strane američke vlade zbog sudjelovanja Facebooka u PRISM programu za nadzor (Peers, 2015). Iako mu je sud isprva predložio da samo onemogući svoj Facebook profil, Schrems je i dalje stajao iza svoje tvrdnje da komisija nije mogla osigurati adekvatne mjere sigurnosti podataka. 23. rujna 2015. godine donesena je odluka da Safe harbor stvarno nije adekvatna mjera zaštite (Titcomb, 2015). 6. listopada 2015. Sud Europske Unije stavlja američki *Safe Harbor* van snage na temelju toga što se prelako zaobilazi, ne osigurava adekvatne mjere sigurnosti, te daje premalo kontrole korisniku nad vlastitim podacima (Gibbs, 2015).

Krajem 2015. odlučio je ponovno pokrenuti svoj slučaj protiv *Facebooka*, ovaj put s osvrtom Suda Europske Unije o *Facebooku*, pod tvrdnjom da Facebook ne poštuje *Safe Harbor* za svoje prijenose podataka (Schrems). Irski Visoki Sud donio je odluku da ne može prosuditi takvo što, pošto nema autoritet nad proglašavanjem Facebookovih klauzula nevažećima.

Schremsova stranica[2] zahvalila se svima koji su sudjelovali u slučaju protiv Safe Harbora. U intervjuu za *Financial Times* Schrems govori kako je prosječni korisnik "glup", u smislu da nema vremena za doći doma i čitati o tome kako određeni algoritmi funkcioniraju, ili što zapravo znače različiti uvjeti korištenja (Kuchler, 2018). Schrems smatra da privatnost na internetu treba biti nešto što se očekuje, jer se jednostavnost korištenja očekuje u svim drugim područjima. Kaže da bi čovjek trebao zaključati vlastitu kuću, ali da bi trebali postojati i zakoni protiv provalnika (Council of Europe, 2016). Na području Europe osniva novu organizaciju NOYB – *European Center for Digital Rights* u 2017. NOYB pokušava objediniti aktivnost svih organizacija za privatnost na području

2 https://www.crowd4privacy.org/

Europe. Bavi se pravnim zastupanjem onih pojedinaca koji uočavaju nepoštivanje zakona vezanog uz privatnost, a nemaju financije za pokrenuti sudski proces sami.

Schrems je svojim djelovanjem smanjio iskorištavanje manjka privatnosti puno prije nego što se GDPR bavio tom temom. Za svoj trud dobio je podršku od mnogih grupa vezanih uz privatnost (EFF, EPIC, Privacy International), te mnoge nagrade ("Big Brother Awards", 2011; EFF, 2016; EPIC, 2013). Trenutno pod novom regulativom radi ono što zna najbolje. S više moći no ikada, tuži Facebook i Google za nepoštivanje nove regulative, tjerajući korisnika da prihvati njihove politike sakupljanja podataka (Scally, 2018).

2.2. Slučaj: Vault 7

Prošle godine WikiLeaks, međunarodna medijska organizacija, objavila je *Vault 7* (WikiLeaks, 2017k) najveću količinu dokumenata o aktivnosti tajne agencije CIA. Količina dokumenata veća je od bilo koje kolekcije koja je procurila na internetu do sada. Kroz ostatak 2017. godine objavljuje sveukupno 24 dijela. Dokumenti pokrivaju period od 2013. do 2016. godine. Neki od žrtava su Apple, Microsoft, Google i Samsung, koji pokrivaju većinu uređaja i softvera koji se aktivno koriste. Ovi su dokumenti važniji od projekta PRISM.

CIA je veća organizacija od NSA-a (*National Security Agency*). Od 2001. godine CIA dobiva političku i financijsku nadmoć nad NSA-om (WikiLeaks, 2017k). Dok se NSA bavi nacionalnom sigurnošću, CIA djeluje globalno od svojeg osnutka. Snowden, kao bivši zaposlenik CIA-a, kaže kako su ovi dokumenti kredibilni, jer prepoznaje neke od njih po njihovim nazivima (2017). No, kako doznajemo od Morsea (2017), CIA nije željela komentirati autentičnost tih dokumenata.

Year Zero (WikiLeaks, 2017k) prvi je dio tih dokumenata. Fokusira se na takozvane „napade na ne zakrpane rupe“ (engl. *zero-day exploits*). Dobile su naziv po tome što je prošlo nula dana od kada se radi na zakrpavanju grešaka u kodu (engl. *patching*). WikiLeaks je ovim putem ponudio proizvođačima pomoć u zakrpavanju tih rupa. Uz metode napada na nezakrpane rupe, dolaze i upute kako CIA izvodi svoje

napade. Obuhvaćaju: način na koji bi zloćudan softver (engl. *malware*) trebalo pisati da bi izbjegli ostavljanje tragova (WikiLeaks 2017c), korištenje metoda zakrivanja za skrivanje komunikacija i identiteta hakera CIA-e (WikiLeaks, 2017g), smjernice za opisivanje žrtava i izvučenih podataka (WikiLeaks, 2017f), kako izvršavati nosive komponente (WikiLeaks, 2017h), kako da virusi ostanu na uređajima praćenih meta kroz duže vrijeme (WikiLeaks, 2017i).

Dark Matter (WikiLeaks, 2017b) se bavi alatima i metodama koje je CIA razvila kako bi mogli hakirati Apple proizvode napadajući ugrađeni softver. CIA inficira ugrađeni softver tako da ostane na uređaju čak ako je operativni sustav bio ponovo instaliran, unatoč tome je li bila šifra na ugrađenom softveru ili ne. Dokumenti otkrivaju da se na tome radi već od 2008. godine.

Marble (WikiLeaks, 2017e) dokumenti govore o softverskom okviru koji služi za obmanu antivirusnih softvera i mrežnih forenzičara. Može natjerati mrežne forenzičare da misle da su napade proveli Rusija, Kina, Sjeverna Korea i Iran.

Weeping Angel (WikiLeaks, 2017l) dokumenti objašnjavaju kako CIA, kroz pametne televizore (engl. *smart tv*), promatra privatne domove. CIA je taj alat razvila u suradnji s britanskim MI5 (*Military Intelligence, Section 5*). Instalacijom preko USB-a alat omogućava da se uključi mikrofon ugrađen u televizor bez da se aktivira lampica koja signalizira da je uključen, a u televizorima s kamerom može i kameru uključiti. Snimke se spremaju na televizoru lokalno ili se mogu proslijediti putem interneta nazad CIA-i.

Scribbles (WikiLeaks, 2017j) sadrži dokumentaciju za alat koji služi za praćenje stranih špijuna, novinara i zviždača. Alat infestira Microsoft Office dokumente stvaranjem web-pratilice (engl. w*eb beacon*). Svaki put kada se otvori dokument, šalje se pristup u CIA-in server za praćenje. Prosljeđuje se ime korisnika koji je koristio dokument, vrijeme kada mu je pristupio i njegovu IP adresu. Alat funkcionira samo u Microsoft Office-u pod uvjetom da je korisnik spojen na Internet.

Cherry Blossom (WikiLeaks, 2017a) dokumenti opisuju softverski okvir za hakiranje uređaja na bežično spajanje. Uključuje stotine modela kućnih usmjerivača. Iskorištavanjem slabih točaka u usmjerivačima i bežičnim pristupnim točkama, instalira

svoj softverski okvir. Sastoji se od više dijelova koji zajedno omogućavaju praćenje aktivnosti na internetu, te instaliranje drugih softverskih alata ako je potrebno. Jedan od tih dijelova, FlyTrap, omogućava sakupljanje podataka poput elektroničkih adresa, MAC adresa uređaja, VoIP brojeva i korisničkih imena u brbljaonicama (engl. *chat rooms*), dozvoljava usmjerenje korisnika na zlonamjerne web-stranice.

Elsa (WikiLeaks, 2017d) dokumenti opisuju geolokacijski orijentiran zloćudan softver namijenjen za uređaje s bežičnim spajanjem koji imaju Windows operativni sustav. Jednom kada je instaliran na nekom uređaju, skenira vidljive bežične pristupne točke i bilježi njihov ESS identifikator, MAC adresu i jačinu signala u intervalima. Kako bi prikupio podatke, uređaj ne mora biti spojen na Internet. Dovoljno je da ima mogućnost bežičnog spajanja. Pri spajanju na internet zloćudan softver automatski se pokušava spojiti na javne geolokacijske baze podataka kako bi odredio poziciju uređaja i pohranio te podatke zajedno s vremenima pristupa. Uklapa se u okolinu prilagođavajući veličine datoteke sa zapisima podataka, interval prikupljanja, zadavanje novih ciljeva itd.

Dokumenti otkrivaju kako je CIA financirala vlastitu globalnu flotu hakera, te na taj način oslobađa agenciju od priznavanja svojih djela. Do kraja 2016. hakerska divizija CIA imala je preko pet tisuća registriranih hakera i proizvela je više od tisuću hakerskih sistema, trojanskih konja, virusa i drugih vrsta „oružanog" zlonamjernog softvera. Veličina tog pothvata toliko je velika da koristi više koda nego što se koristi za stranicu Facebook.

Računalni kriminal predstavlja prijetnju i mrežnim forenzičarima (Šeruga, 2018). Spekulira se kako je dio ovih dokumenata procurio na internet od raznih hakerskih organizacija još i prije (Mathews, 2017). To bi zasigurno objasnilo ogroman porast u računalnom kriminalu (Ismail, 2018).

2.3. Slučaj: Cambridge Analytica

Cambridge Analytica naziv je tvrtke koja je prouzročila jedan od najvećih sigurnosnih provala ikada. Ukradeno je oko 87 milijuna korisničkih računa (Meyer, 2018) sa stranice Facebook. Osniva se pod grupacijom SCL (*Strategic Communication*

Laboratiories), tj. tvrtkom koja se bavila promjenama u ponašanju naroda. Postavlja se pitanje možemo li uopće reagirati demokratski na ovakve događaje, kada ni najveće tvrtke na svijetu ne mogu reagirati kako treba.

Cilj im je bio koristiti SCL-ova istraživanja u području ponašanja i psihologije s modeliranjem podataka (engl. *data modeling*) da stvore model za nagovaranje. Zviždač Christopher Wylie raskrio je stvarno djelovanje tvrtke 2018. godine (Cadwalladr). Kaže kako je tvrtkin osnivač, Alexander Nix, surađivao s dešnjačkim administracijama korištenjem psihografskih alata kako bi utjecala na inshod predsjedničkih izbora u Sjedinjenim Američkim Državama 2016. godine i Brexit-a (Osborne, 2018).

Alexander Nix u intervjuu iz 2016. godine (Swift) govori kako je cilj tvrtke bio „osloviti vakuum u republikansom političkom tržištu“ nakon poraza kandidata Mitta Romneya na predsjedničkim izborima 2012. godine. Njegovo opravdanje za djelovanje tvrtke je da demokrati vode tehnološku revoluciju, a ovo je za tvrtku bila prilika da konkuriraju. Klijenti s kojima su surađivali bile su države, vojske i agencije za pomoć.

Cambridge Analytica ima značajne veze s nekima od Trumpovih najistaknutijih podržavatelja i savjetnika. Rebekah Mercer, republikanski donor i jedna od vlasnica američkih novina Breitbart News sudjeluje u C*ambridge Analytici*. Njen otac, Robert Mercer, investirao je 15 milijuna američkih dolara u *Cambridge Analyticu* po preporuci svojeg političkog savjetnika, Steve Bannona (Confessore & Gelles, 2018).

Wiley kaže kako je tvrtka adoptirala naziv *Cambridge Analytica* u trenutku premještanja tvrtke na Sveučilište u Cambridgu. Tamo počinju surađivati sa znanstvenikom Alexandrom Koganom. Kogan je razvio aplikaciju „*This Is Your Digital Life*“ za Facebook. Aplikacija je bila test osobnosti, kao i mnoge druge koje postoje na Facebooku. Bila je pod velikim utjecajem slične takve aplikacije koju su razvili u centru za psihometriju na sveučilištu u Cambridgeu gdje je Kogan radio. Oko 270 tisuća ljudi pristupilo je Koganovoj aplikaciji na svojem Facebook korisničkom računu. Kogan je mogao pristupiti podacima o korisniku koji ju je instalirao, a preko njih i podacima njihovih prijatelja. Kada je Koganova aplikacija tražila pristup njihovim podacima, spremala bi te informacije u privatnu bazu podataka, umjesto da ih odmah izbriše.

Kogan je dao privatnu bazu podataka računa na Facebooku Cambridge Analytici koja se bavila profiliranjem birača. Baza podataka sadržavala je informacije za oko 87 milijuna korisnika (Meyer, 2018). Koristila je podatke kako bi napravila 30 milijuna psihografskih profila o biračima. Svoje alate koristila je da napravi reklame za Brexit kampanju, predsjedničku kampanju Teda Cruza u 2016., te predsjedničku kampanju Donalda Trumpa u 2016. godine (Meyer, 2018).

Uskoro nakon što je Wiley otkrio djelovanje tvrtke, snimka skrivene kamere prikazivala je Alexandra Nixa, kako govori o nuđenju mita i ucjenjivanju javnih službenika diljem svijeta. Nix u Guardianovom intervjuu (McKee, 2018) kaže kako kandidati nikada nisu saznali što se događalo. Snimka je prouzročila istragu i zatvaranje tvrtke.

Istraga dokazuje da je Facebook znao za sakupljanje podataka još u 2015. godini. Mark Zuckerberg, osnivač Facebooka pozvan je na suđenje pred američki senat. Iz saslušanja saznajemo da Zuckerberg nije izvjestio FTC (*Federal Trade Comission*) o ilegalnom prikupljanju podataka. Zatražio je od *Cambridge Analytice* da obriše podatke još u 2015. godini smatrajući da su to napravili. Nikada nije provjereno jesu li podaci stvarno obrisani. Zuckerberg kaže da surađuju na istrazi o predsjedničkim izborima 2016. godine, te kako mu je žao da nije reagirao na vrijeme. Tvrdi kako se takvo nešto više neće ponoviti i da će opremiti svoju društvenu mrežu alatima potrebnima za prevenciju (Kharpal, 2018). Tvrtka SCL je bankrotirala u svibnju, a Facebook je dobio svoju prvu kaznu u srpnju (Hern, 2018).

3. GDPR

Već 2011. godine većina Europljana izražava želju za kontrolom nad podacima, te žele znati što se s njihovim podacima radi sumnjajući da se iskorištavaju u krive svrhe (Eurobarometer, 2011). Donesene promjene rješavaju probleme mnogih studija vezanih uz privatnost na internetu:

- smanjuju zabrinutost oko privatnosti (Krafft, Arden, & Verhoef, 2017),
- smanjuju rizik krađe osobnih podataka (Trepte, Reinecke, Ellison, Quiring, Yao, & Ziegele, 2017),
- olakšavaju vlastoručno upravljanja postavkama privatnosti (engl. *privacy fatigue)* (Choi, Park, & Jung, 2017).

Uredba o zaštiti osobnih podataka (*GDPR - General Data Protection Regulation*) je uredba koja cilja da cijela Europa bude pod jednim setom zakona za kojeg se vjeruje da će olakšati i pojeftiniti proces organizacija da posluju jednako po cijeloj Uniji (Galdies, 2017). Izglasana je u 2016. godini i odmah je stupila na snagu. No, uz regulativu je objavljen i rok prilagodbe od dvije godine koji je istekao 25.05.2018. Nakon toga je stupila na snagu u cijeloj Europskoj Uniji. Zamjenjuje *Data Protection Act* donesen 1998. godine i dalje uzimajući ga u obzir, pokušavajući ga uskladiti s trenutnim tehnologijama.

Prema izvještaju tvrtke Ovum, otprilike dvije trećine američkih tvrtki vjeruje da će ih GDPR natjerati da promjene strategiju u Europi, a oko 85% njih vide GDPR kao regulativu koja ih stavlja u lošu poziciju u odnosu na tvrtke u Europi (Nadeau, 2018).

Fokus GDPR-a stavljen je na osam principa ("The 8 Principles of the Data Protection Act", 2017). Ukratko ću objasniti svaki od njih.

1. Organizacije moraju ***poslovati fer i unutar zakona***. Korištenje usluga ne smije imati negativne posljedice na korisnika ili koristiti se suprotno od očekivanja.
2. Organizacije moraju biti ***transparentne sa svojim namjerama prikupljanja*** osobnih podataka. To znači da tvrtke više ne smiju koristiti

podatke korisnika kako bi reklamirali druge tvrtke osim ako je korisnik eksplicitno pristao na takvo što. Ne bi smjeli prosljeđivati podatke korisnika trećim stranama, ponovo, osim ako je korisnik pristao na to.

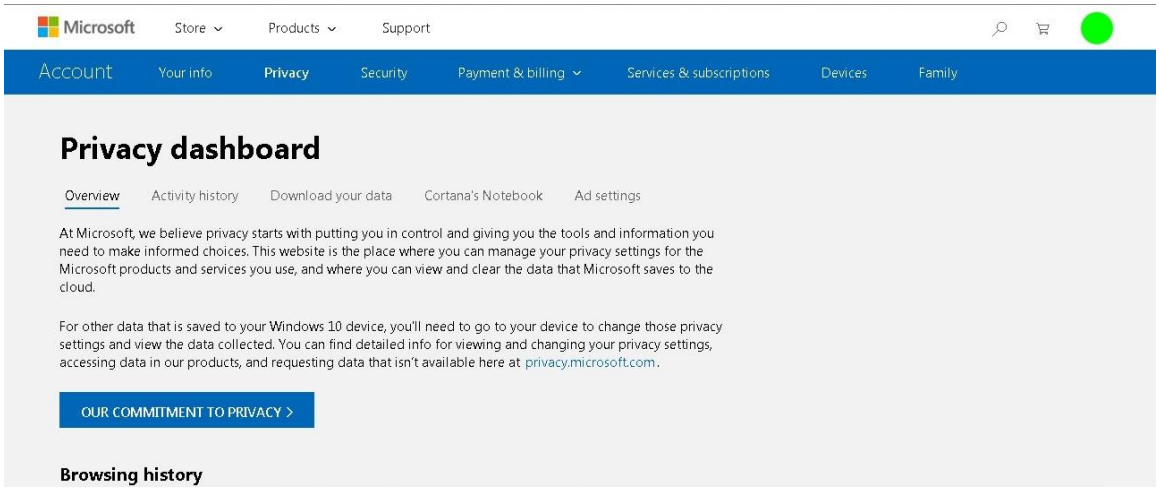
3. Zahtjevi za podatke moraju biti ***adekvatni svrsi*** iza koje tvrtka stoji. Od korisnika se moraju tražiti samo podaci koji su potrebni za funkcioniranje usluge koju tvrtka pruža. Korisnik može pristati davati više podataka, ali mora imat mogućnost korištenja uz samo potrebne podatke.
4. Informacije o korisnicima moraju biti ***točne i ažurirane***, i tvrtke moraju težiti k tome da to aktivno traže od svojih korisnika, umjesto da korisnici sami kontaktiraju tvrtke kako bi ažurirali svoje podatke. Nakon ažuriranja, tvrtka mora kontaktirati korisnika striktno pod novim podacima.
5. Podaci moraju biti zadržani samo onoliko ***vremena koliko je stvarno potrebno***. Zastarjeli podaci i podaci koji više nisu potrebni moraju biti pravilno obrisani tako da više ne postoje.
6. U svakom trenutku moraju se uzimati ***korisnikova ljudska prava*** u obzir. Korisnici imaju pravo pristupiti svojim osobnim podacima, zaustaviti njihovo korištenje ako im to uzrokuje brigu, zaustaviti korištenje podataka ako se koriste za direktan marketing, mijenjati netočne podatke i tražiti kompenzaciju ako dođe do provale u sustav koja im je naškodila. Korisnik ima pravo zatražiti pristup informacijama podnošenjem zahtjeva putem elektroničke pošte, faksa ili poštom. U određenim slučajevima korisnici moraju imati pravo da specifične podatke unište. Korisnici imaju pravo tražiti podatke koji su isključivo povezani s njima, tuđe nikako. Organizacija ima odgovornost procijeniti jesu li podaci relevantni korisniku koji ih traži. Smiju zatražiti od korisnika da im prestanu slati zahtjeve, iako to ne bi smjela biti jedina mogućnost koju pružaju.
7. Pravilan način pohranjivanja podataka koji ih čuva fizički, a sigurnosni sustav bi trebao garantirati da su ***informacije na sigurnome***. Poželjno je da se zaposlenici obrazuju o osnovama zaštite podataka i računalne

sigurnosti. Dokazano da to drastično smanjuje rizik od najpoznatijih vrsta napada poput *phishing* napada (Aronovich, 2018).

8. Podaci ***ne smiju biti prenošeni*** u druge države koje nemaju jednaku razinu zaštite podataka.

Postoji još mnogo dodatnih pravila. Neka od njih su: pravilo da korisnici moraju uvijek biti obavješteni o svojem pravu za povlačenjem suglasnosti o davanju podataka (pravo da „budemo zaboravljeni" o kojemu se godinama raspravljalo postoji li ili ne (Powels & Chaparro, 2015; Prashar, 2014)), zahtjev za prijenos osobnih podataka na drugu platformu besplatno, zapošljavanje službenika za zaštitu podataka (engl. *Data Protection Officer*) ako tvrtka procesuira preko 5 tisuća osobnih evidencija i zapošljava preko 250 radnika godišnje, itd.

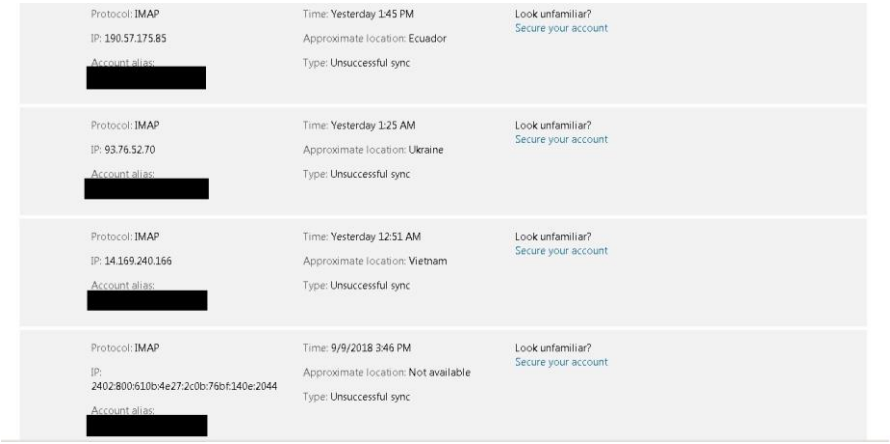
GDPR je već utjecao na svijet uveliko, stavljajući naglasak na implementiranje privatnosti u fazi dizajna. Za primjer implementacije odabrao sam Microsoftov Outlook Mail.



Slika 1: Sučelje za upravljanje postavkama privatnosti Outlook Mail-a - 11.9.2018.

Na slici 1 vidimo sučelje za upravljanje postavkama privatnosti koje je u skladu s GDPR-om. Za ulazak u sučelje potrebno je potvrditi naš identitet s druge elektronske pošte. Možemo preuzeti vlastite podatke, vidjeti što smo pitali osobnog glasovnog asistenta (engl. *personal voice assistant*) Cortanu, mijenjati postavke vezane uz reklame, obrisati našu povijest pretraživanja, lokacija, uputa glasom, urediti naš LinkedIn profil i povijest aktivnosti (možemo vidjeti točno kada i kako smo koristili koju *Microsoftovu*

aplikaciju). Postoji i pregled sigurnosnih postavki, gdje možemo mijenjati svoju lozinku (postoji mogućnost za podsjećanjem na promjenu lozinke svakih 72 dana), nadograditi svoje sigurnosne informacije (možemo promijeniti samo sigurnosno pitanje i alternativnu adresu elektroničke pošte), te pregledati kada i od kuda smo se pokušali prijaviti na svoj korisnički račun.



Slika 2: Povijest prijava na elektroničku poštu Outlook Mail - 11.9.2018.

Na slici 2 vidimo povijest prijava. Otkriva da su postojali pokušaji ulaska u moju elektroničku poštu iz mnogih različitih država uključujući Rusiju, Njemačku, Nizozemsku, Ekvador, Vijetnam, SAD, Srbiju, Ukrajinu, pa čak i neke nepoznate adrese. Mislim da ti napadi nisu bili usmjereni direktno na mene, već su vjerojatno bili dio neke skripte koja pokušava upasti u mnoge račune elektroničke pošte.

Slika 3: Obavijest o promjeni lozinke Outlook Mail-a - 11.9.2018.

Na slici 3 vidimo što se dogodi u slučaju da promijenimo lozinku. Možemo vrlo lako vratiti našu prvotnu lozinku koristeći alternativnu elektroničku poštu.

AZOP (Agencija za zaštitu osobnih podataka) hrvatska je organizacija kojoj se možemo obratiti u slučaju povrede privatnosti prema smjernicama GDPR-a. Pruža nam pomoć oko brisanja podataka iz baza podataka Google i Facebooka, te njihovih podružnica Youtube i Instagram, kontakt na službenika za informiranje o rješavanju ostvarivanja prava na pristup informacijama, te kontakt na službenika za zaštitu podataka ("Kontakt agencija za zaštitu osobnih podataka", n.d.).

Kazne ne nazivaju drakonskima bez razloga: uzima se ili iznos u milijunima (manji slučajevi do 10 milijuna eura, veći do 20 milijuna eura) ili u postotku globalne zarade godine prije prekršaja (manji slučajevi 2%, veći 4%). Iznos koji je u konačnici veći uzima se za kaznu. Razlozi za kažnjavanje dijele se na 10 kategorija koje se uzimaju u obzir pri dodjeli kazne: prirodu prekršaja, namjeru, mjere poduzete za smanjenje štete, preventivne metode, povijest prošlih kršenja GDPR-a, mjera suradnje, tip podataka pomoću kojih je šteta napravljena, obavijest o šteti, je li tvrtka kvalificirana pod odobrenim potvrdama tj. je li se pridržavala prema kodeksu ponašanja i druge ("Administrative fines", n.d.). Nedostaci GPDR-a time bi mogli biti kočenje manjih tvrtki u usponu koje još nemaju dovoljno razvijenu sigurnost, pošto su one češće žrtve računalnog kriminala u odnosu na veće tvrtke (Smith, 2016).

4. Ostale protumjere

Prva opcija je da se naučimo kako se efikasnije zaštiti pomoću takozvanih programa za „triježnjenje od korištenja interneta" (engl. *data detox*), namijenjenih da osvijeste prosječne korisnike o korištenju interneta na siguran i neovisan način. Iako priče o takvim programima za triježnjenje i razne radionice postoje već dugo vremena, Mozilla nudi jedan program koji obećava da u 8 dana ulažući pola sata vremena svaki dan možemo postati svjesniji i sretniji korisnici interneta ("Data Detox", 2017). Program se sastoji od objašnjenja kako da pretvorimo triježnjenje u životni stil.

Virtualna privatna mreža (engl. *Virtual Private Network - VPN*) je softver koji dobiva sve više na popularnosti (Wollf, 2018). VPN nam omogućava da se spojimo na privatnu mrežu. Poslužitelj VPN-a postaje naš poslužitelj interneta. VPN ima dvije glavne prednosti: možemo surfati po stranicama koje možda naša vlada blokira i daje nam veću privatnost nego što bi imali inače. Kina želi odstraniti VPN softver iz svih trgovina aplikacija (engl. *app store*), ali do sad nisu bili uspješni u tom pothvatu (Cadell, 2017). Ruski zakon brani VPN uslugama da daju korisnicima mogućnost pristupa listi blokiranih stranica, tražeći od poslužitelja interneta da blokiraju pristup VPN uslugama, ali također uz malo uspjeha u praksi (Devitt, 2017). U SAD-u VPN se većinski koristi kako tvrtke ne bi mogle prodavati podatke trećim stranama. Možemo zaključiti da se ne može baš kontaminirati korisnike VPN-a od slobode koju pružaju. Poslužitelji usluga se ponašaju s poštovanjem prema svojim korisnicima, ne otkrivajući brojeve korisnika njihovih usluga kako ne bi privukli pažnju i potencijalno morali zatvoriti vlastite usluge.

Oblak (engl. *cloud*) je velika količina podataka koji su organizirani, zakriveni i, najvažnije od svega, nalaze se na jednom mjestu gdje mogu biti lako nadgledani. Postoje tvrtke koje se već godinama bave računalnom sigurnošću i oblacima, pošto si ne mogu dozvoliti da budu provaljeni jer bi im to naškodilo reputaciju. Te tvrtke uključuju Amazon, IBM, Google, Oracle, Microsoft i mnoge druge. Pohrana na oblaku također nije skupa, čineći je dostupnom svakome. Predviđa se da će u budućnosti svu sigurnost

potrebnu za zaštitu od računalnih napada i krađe podataka izvršavati upravo poslužitelji oblaka (O'Neill, 2018).

4.1.Dark Net

Mnogi korisnici interneta znaju danas da su na površinskom netu (engl. *surface net*) izloženi eksploataciji, profiliranju i represiji. Prije postojanja interneta kakvog poznajemo danas, postojao je internet u kojemu su ljudi morali aktivno tražiti sadržaj koji ih je zanimao, visiti na forumima i zbližavati se s korisnicima na puno privatniji način, koristeći anonimna korisnička imena i zakrivene elektroničke pošte (Callaghan, 2018).

Takav internet i dalje postoji, samo što nije dio površinskog interneta. Znamo da je tzv. mračni net (engl. *Dark net*) poznat kao mjesto gdje se ilegalno posluje drogama, oružjem, ljudima i dječjom pornografijom. Tržišta na mračnom netu, poput famoznog *Silk Roada,* dala su negativnu reputaciju cijelom mjestu (McCarthy, 2018).

Mračni net zapravo je mjesto gdje čovjek može biti nesmetan dok surfa internetom. Korisnicima pruža mnoga mjesta gdje mogu ostati anonimani dok komuniciraju s drugima. Novinari mogu sigurno komunicirati sa zviždačima, humanitarci se mogu naći i diskutirati svoje planove. WikiLeaks koristi mračni net kako bi mogli prikupljati dokumente. Omogućava ljudima koji žive u tiranskim režimima da imaju mjesto gdje ih se ne može pratiti, gdje se mogu suprotstaviti svojoj državi. Od kad je Erdoğan dobio izbore, mnogi Turci su se okrenuli mračnom netu. Danas su, prema kategoriji narodi, Turci drugi na ljestvici po korištenju mračnog neta ("Users", 2018).

Princip funkcioniranja mračnog neta bazira se na delokalizaciji podataka. Za spajanje na mračni net potreban nam je preglednik Tor. Mada nije inicijalno lagan za koristiti koliko i prosječan preglednik, Tor preglednik čini nas skoro nemogućima za pratiti. Ako se držimo smjernica, kojih postoji u izobilju (Fernandez, 2017; Grimes & Gralla 2018; Phillips, 2017), nećemo biti otkriveni. U slučaju da pokušavamo nešto kupiti preko mračnog neta koriste se kriptovalute. To je delokaliziran način plačanja razvijen kako bi osigurao anonimnost transakcije.

Naravno nije sve toliko bajno. Kada se nalazimo na mračnom netu moramo uzeti u obzir da ne smijemo koristiti društvene medije i slične stranice koje zahtijevaju naše osobne podatke kako bi funkcionirale. Brzina interneta na mračnom netu sporija je od brzine površinskog neta. Ovisi o broju čvorova, zakrivanju i anonimnosti koja je ugrađena u strukturu.

4.2. Tails

Tails je operativni sustav (distribucija bazirana na *Debian Linuxu*) koji cilja zaštititi i očuvati privatnost svojih korisnika. Inspiriran je operativnim sustavom *Incognito LiveCD* ("Acknowledgements", n.d.). Pruža korištenje računala na potpuno anoniman način. Služi za krajnje ekstremne slučajeve očuvanja privatnosti. Dizajniran je da bude korišten uživo (engl. *live boot*), s USB-a ili s DVD-a, neovisno o originalnom operativnom sustavu računala. Tails možemo koristiti na bilo kojem računalu, ne ostavljajući tragove na tvrdom disku. Sva memorija koju koristi pohranjuje se na radnoj memoriji, brišući sve podatke kada ugasimo operativni sustav. Ne ostavlja tragove naše aktivnosti za sobom u pohrani računala osim ako mu to eksplicitno ne naglasimo. Besplatan je i dolazi s aplikacijama koje su imale sigurnost i privatnost na umu u fazi dizajniranja.

Koristi mnoge zakritne tehnologije uključujući: zakrivanje pokrenith medija za pohranu (USB ili vanjski tvrdi disk), automatski koristi HTTPS za zakrivanje svih komunikacija, zakriva sve elektroničke pošte i dokumente koje stvorimo, itd. ("About", n.d.). Koristio ga je Edward Snowden kada je slao elektroničku poštu urednicima *Guardiana* (Stahie, 2014), a spekulira se kako ga je koristila i osoba koja je objavila NSA-in *Xkeyscore*, kaže Schneier (2015).

5. Zaključak

Max Schrems obranio je svijet od nezakonitog prosljeđivanja podataka. Njegovim činom započela je diskusija o privatnosti podataka u Europi. Vault 7 pokazao je postajanje velike količine računalnog oružja, te kako će ovo stoljeće biti pamćeno kao stoljeće računalnih ratova ako se ništa ne promjeni u području zaštite podataka. Slučaj *Cambridge Analytica* pokazala je kako u višim slojevima poslovanja ne postoji kočnica u pokušaju stjecanja moći. Facebook se u ovom desetljeću pokazao kao platforma za kontrolu mase. Kroz pasivno nekontrolirano prikupljanje podataka dozvoljeno svim stranama, a kasnije za aktivno pokušavanje kontroliranja na mikro razini.

Utječući na svakog pojedinca zasebno stvaramo polarizirane mase. GDPR regulativa pokušava reformirati način procesuiranja i pohrane podataka kako bi se broj incidenata smanjio, a prosječni pojedinac na internetu više poštivao. GDPR, iako važi samo za područje Europe, nada se postići globalni utjecaj. Obrazovanje na temu računalne sigurnosti krucijalno je za poboljšanje privatnosti na internetu. Računalni kriminal i kontroliranje sadržaja evoluiraju alate za osiguravanje privatnosti. Vidjeli smo da ako nam je stvarno stalo do privatnosti, možemo se prilagoditi.

Ulaskom u semantički web mnoge stvari se očekuju od korištenja interneta: veće brzine, komunikacija među uređajima svih vrsta, veći fokus na zdravlje pojedinca, samovozeći auti, znanje koje nam je dostupno i skroz relevantno i druge. Vidjeli smo da unatoč svim naporima da tehnologija našeg doba ne bude iskorištavana u krive svrhe, tehnologija ipak ostaje dvosjekli mač. Javna sumnja u uređaje koji su vječno povezani veća je no ikada (Majumdar, n.d). Slučajevi kao smrt novinara Michael Hastingsa (Overly, 2017), navodno prouzrokovana hakiranjem automobila, ne pomažu skepticima da odustanu od svojih strahova. Uvijek su postojali pokušaji eksploatacije novih izuma. Zato ćemo uvijek trebati savjesne ljude kao što su bili Snowden, Schrems, Assange ili Wylie koji su spremni staviti se pred gigante i žrtvovati vlastitu slobodu kako bi istaknuli neku manu civilizacije.

Prema njihovom primjeru trebali bi se obrazovati u polju onoga što svakodnevno koristimo, a ne biti samo prolaznici u cijeloj situaciji koji za sebe misle da nemaju nikakvog utjecaja na stvari koje se događaju oko njih. Živimo u vremenu koje poziva na edukaciju o tehnologiji više no ikada.

Isto tako ne valja biti previše pesimističan u vezi trenutnog stanja i nadolazećih novina jer ipak živimo u dobu gdje postoji više inovacije no ikada prije, u svim područjima. Sve što trebamo osigurati je da radimo korak u pravom smjeru. Možda već u bliskoj budućnosti, auti će voziti sami od sebe, roboti će nam pomagati i olakšavati život, adekvatnim i sigurnim praćenjem naših aktivnosti moći ćemo postizati bolje rezultate, skeniranjem bioritama moći ćemo sasjeći problem bolesti u korijenu, edukacija će biti kohezivnija, glasat će se redovito i putem interneta, transakcije preko interneta bit će potpuno sigurne, a osobni digitalni sadržaj koji stvaramo napokon će postati ono što smo željeli da bude: reguliran od strane nas samih.

6. Popis literature

1. *Administrative fines* (n.d.). Preuzeto sa: https://www.gdpreu.org/compliance/fines-and-penalties/ Pristupljeno: 11.9.2018.
2. Aronovich, A. (2018, 14. lipnja). *Why educating your employees on cyber intelligence and security will reduce risk.* Preuzeto sa: https://www.linkedin.com/pulse/why-educating-your-employees-cyber-intelligence-reduce-aronovich/?published=t Pristupljeno: 11.9.2018.
3. AZOP (n.d.) *Kontakt agencija za zaštitu osobnih podataka*. Agencija za zaštitu osobnih podataka. Preuzeto sa: https://azop.hr/zastita-podataka-hrvatska/detaljnije/kontaktirajte-nas Pristupljeno: 11.9.2018.
4. Allen, C (2015, 21. travnja). *The Four Kinds of Privacy*. Preuzeto sa: https://medium.com/@christophera/the-four-kinds-of-privacy-bf4b0bf222ac Pristupljeno: 17.9.2018.
5. Ball, J., & Borger, J. (2013, 6. srpnja). *Revealed: how US and UK spy agencies defeat internet privacy and security*. Preuzeto sa: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. Pristupljeno 4.9.2018.
6. *Big Brother Awards: Die Gewinner stehen fest* (2011, 26. listopada). Preuzeto sa: https://futurezone.at/netzpolitik/big-brother-awards-die-gewinner-stehen-fest/24.572.297 Pristupljeno: 5.9.2018.
7. Cadell, C. (2017, 29. srpnja). *Apple says it is removing VPN services from China App Store*. Preuzeto sa: https://www.reuters.com/article/us-china-apple-vpn/apple-says-it-is-removing-vpn-services-from-china-app-store-idUSKBN1AE0BQ Pristupljeno: 15.9.2018.
8. Cadwalladr, C. (2018, 18. ožujka). *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*. Preuzeto sa:

https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump Pristupljeno: 9.9.2018.

9. Callaghan, G. (2018, 10. ožujka). *The dark web: uncovering monsters (and myths) in the Net's 'evil twin'*. Preuzeto sa: https://www.smh.com.au/technology/the-dark-web-uncovering-monsters-and-myths-in-the-net-s-evil-twin-20180307-p4z39d.html Pristupljeno: 16.9.2018.
10. Choi, H., Park, J., & Jung, Y. (2017, 1. prosinca). *The role of privacy fatigue in online privacy behavior*. Preuzeto sa: http://iranarze.ir/wp-content/uploads/2018/04/E6393-IranArze.pdf Pristupljeno: 5.9.2018.
11. Confessore, N., & Gelles, D. (2018, 10. travnja). *Facebook Fallout Deals Blow to Mercers' Political Clout.* Preuzeto sa: https://www.nytimes.com/2018/04/10/us/politics/mercer-family-cambridge-analytica.html Pristupljeno: 9.9.2018.
12. Council of Europe, (2016, svibanj, 24). *Data Protection - Max Schrems*. Preuzeto sa: https://www.youtube.com/watch?v=TN4nkVQ0ljA Pristupljeno: 5.9.2018.
13. *Data Protection Commissioner says no action will be taken against Apple and Facebook* (2013, 26. srpnja). Preuzeto sa: https://www.rte.ie/news/2013/0726/464770-data-protection/ Pristupljeno 4.9.2018.
14. Devitt, P. (2017, 30. srpnja). *Putin bans VPNs to stop Russians accessing prohibited websites*. Preuzeto sa: https://www.reuters.com/article/us-russia-internet/putin-bans-vpns-to-stop-russians-accessing-prohibited-websites-idUSKBN1AF0QI Pristupljeno: 15.9.2018
15. EFF (2016, 9. kolovoza) *EFF Announces 2016 Pioneer Award Winners: Malkia Cyril of the Center for Media Justice, Data Protection Activist Max Schrems, the Authors of 'Keys Under Doormats,' and the Lawmakers Behind CalECPA. Electronic Frontier Foundation*. Preuzeto sa: https://www.eff.org/press/releases/eff-announces-2016-pioneer-award-winners-malkia-cyril-center-media-justice-data Pristupljeno: 5.9.2018.
16. EPIC (2013, 24. siječnja) *EPIC Gives 2013 Privacy Champion Award to Austrian Privacy Advocate*. Electronic Privacy Information Center. Preuzeto sa:

https://epic.org/2013/01/epic-gives-2013-privacy-champi.html Pristupljeno: 4.9.2018.

17. Eurobarometer (2011*). Attitudes on Data Protection and Electronic Identity in the European Union.* Preuzeto sa: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf Pristupljeno: 10.9.2018.
18. Fernandez, A. (2017, 12. rujna). *The Grand Tor: How to Go Anonymous Online*. Preuzeto sa: https://www.wired.com/story/the-grand-tor/ Pristupljeno 16.9.2018.
19. Galdies, P. (2017, 12. listopada). *A Summary of the EU General Data Protection Regulation.* Preuzeto sa: https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation Pristupljeno: 10.9.2018.
20. Gibbs, S. (2015, 6. listopada). *What is 'safe harbour' and why did the EUCJ just declare it invalid?*. Preuzeto sa: https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection Pristupljeno: 4.9.2018.
21. Grimes, A.R., & Gralla, P. (2018, 1. siječnja). *17 steps to being completely anonymous online*. Preuzeto sa: https://www.csoonline.com/article/2975193/data-protection/9-steps-completely-anonymous-online.html Pristupljeno: 16.9.2018.
22. Hern, A. (2018, 11. srpnja). *Facebook fined for data breaches in Cambridge Analytica scandal.* Preuzeto sa: https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal Pristupljeno: 18.9.2018.
23. Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies*? SSRN. Preuzeto sa: http://dx.doi.org/10.2139/ssrn.1589864 Pristupljeno: 4.9.2018.
24. Ismail, N. (2018, 2. siječnja). *2017 – the year that defined cybercrime*. Preuzeto sa: https://www.information-age.com/2017-year-defined-cybercrime-123470158/ Pristupljeno 9.9.2018.

25. Kharpal, A. (2018, 11. travnja). *Mark Zuckerberg's testimony: Here are the key points you need to know*. Preuzeto sa: https://www.cnbc.com/2018/04/11/facebook-ceo-mark-zuckerberg-testimony-key-points.html Pristupljeno: 18.9.2018.
26. Krafft, M., Arden, C.M., & Verhoef, P.C. (2017, kolovoz). *Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?. Journal of Interactive Marketing*, 39, 39-54. Preuzeto sa: https://www.sciencedirect.com/science/article/pii/S1094996817300191 Pristupljeno: 10.9.2018.
27. Kuchler, H. (2018, 5. travnja). .*Max Schrems: the man who took on Facebook – and won*. Preuzeto sa: https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544 Pristupljeno: 5.9.2018.
28. Majumdar, S. (n.d.). *Why Companies and Customers Are Still Skeptical of IoT* [Blog post]. Preuzeto sa: https://www.kovair.com/blog/companies-customers-still-skeptical-iot/ Pristupljeno: 9.9.2018.
29. Mathews, L. (2017, 8. ožujka). *WikiLeaks Vault 7 CIA Dump Offers Nothing But Old News*. Preuzeto sa: https://www.forbes.com/sites/leemathews/2017/03/08/the-wikileaks-vault-7-cia-dump-shouldnt-terrify-you/#4dba72ac6b8a Pristupljeno: 8.9.2018.
30. McCarthy, N. (2018, 22. ožujka). *Where Guns Are Sold Through The Darknet* [Infographic]. Preuzeto sa: https://www.forbes.com/sites/niallmccarthy/2018/03/22/where-guns-are-sold-through-the-darknet-infographic/#176d3842647a Pristupljeno: 16.9.2018.
31. McKee, R. (2018, 20. ožujka). *Alexander Nix, Cambridge Analytica CEO, suspended after data scandal.* Preuzeto sa: https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-suspends-ceo-alexander-nix Pristupljeno: 18.9.2018.
32. Meyer, R. (2018, 10. travnja). *My Facebook Was Breached by Cambridge Analytica. Was Yours?*. Preuzeto sa:

https://www.theatlantic.com/technology/archive/2018/04/facebook-cambridge-analytica-victims/557648/ Pristupljeno: 18.9.2018.

33. Morse, J. (2017, 9. ožujka). *The CIA thinks you should be 'deeply troubled' by the WikiLeaks data dump it won't confirm is authentic*. Preuzeto sa: https://mashable.com/2017/03/08/wikileaks-cia-vault7/?europe=true#QNoWVSQLrOqK Pristupljeno:: 8.9.2018.
34. Mozilla (2017, studeni) Data Detox. Mozilla. Preuzeto sa: https://datadetox.myshadow.org/en/detox Pristupljeno: 13.9.2018.
35. Nadeau, M. (2018, 23. travnja). *General Data Protection Regulation (GDPR): What you need to know to stay compliant*. Preuzeto sa: https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html Pristupljeno: 11.9.2018.
36. O'Neill, E. (2018, 27. travnja). *Why the future of cybersecurity is in the cloud.* Preuzeto sa: https://www.cloudcomputing-news.net/news/2018/apr/27/why-future-cybersecurity-cloud/ Pristupljeno: 17.9.2018.
37. Osborne, H. (2018, 18. ožujka). *What is Cambridge Analytica? The firm at the centre of Facebook's data breach.* Preuzeto sa: https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach Pristupljeno: 18.9.2018.
38. Overly, S. (2017, 8. ožujka). *What we know about car hacking, the CIA and those WikiLeaks claims*. Preuzeto sa: https://www.washingtonpost.com/news/innovations/wp/2017/03/08/what-we-know-about-car-hacking-the-cia-and-those-wikileaks-claims/?noredirect=on&utm_term=.688387230369 Pristupljeno: 9.9.2018.
39. Peers, S. (2015, 29. ožujka). *Do Facebook and the USA violate EU data protection law? The CJEU hearing in Schrems*. Preuzeto sa: http://eulawanalysis.blogspot.com/2015/03/does-facebook-and-usa-violate-eu-data.html Pristupljeno 4.9.2018.

40. Phillips, G. (2017, 31. srpnja). *Really Private Browsing: An Unofficial User's Guide to Tor*. Preuzeto sa: https://www.makeuseof.com/tag/really-private-browsing-an-unofficial-users-guide-to-tor/ Pristupljeno: 16.9.2018.
41. Powels, J., & Chaparro, E. (2015, 18. veljače). *How Google determined our right to be forgotten.* Preuzeto sa: https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search Pristupljeno: 11.9.2018.
42. Prashar, U. (2014, 31. srpnja). *The 'right to be forgotten' simply doesn't exist*. Preuzeto sa: https://www.telegraph.co.uk/news/uknews/law-and-order/11000631/The-right-to-be-forgotten-simply-doesnt-exist.html Pristupljeno: 11.9.2018.
43. Scally, D. (2018, 25. svibnja). *Max Schrems files first cases under GDPR against Facebook and Google.* Preuzeto sa: https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177 Pristupljeno: 5.9.2018.
44. Schneier, B. (2015). Data and Goliath : the hidden battles to collect your data and control your world. New York, W.W. Norton & Company.
45. Schrems, M. (2015, 2. prosinca). *Data Protection Authorities in Ireland, Belgium and Germany requested to review and suspend Facebook's data transfers over US spy programs.* Preuzeto sa: http://www.europe-v-facebook.org/prism2_en.pdf Pristupljeno: 4.9.2018.
46. Skillings, J. (2006, 4. svibnja). *Apple's 'Get a Mac' attack*. Preuzeto sa: https://www.cnet.com/au/news/apples-get-a-mac-attack/ Pristupljeno: 4.9.2018.
47. Smith, M. (2016, 8. veljače). *Huge rise in hack attacks as cyber-criminals target small businesses.* Preuzeto sa: https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses Pristupljeno: 11.9.2018.
48. Snowden, E. [Snowden] (2017, 7. ožujka). *What makes this look real? Program & office names, such as the JQJ (IOC) crypt series, are real. Only a cleared insider could know them* [Tweet]. Preuzeto sa:

https://twitter.com/Snowden/status/839157182872576000?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E839159736977227777%7Ctwcon%5Elogo&ref_url=https%3A%2F%2Fwww.ibtimes.com%2Fedward-snowden-reacts-wikileaks-vault-7-dump-calls-cia-documents-authentic-2503814 Pristupljeno: 7.9.2018.

49. Stahie, S. (2014, 16. travnja). *Edward Snowden Used the Tails Linux Distro to Stay Hidden*. Preuzeto sa: https://news.softpedia.com/news/Edward-Snowden-Used-the-Tails-Linux-Distro-to-Stay-Hidden-438074.shtml Pristupljeno 16.9.2018.
50. Swift, James (2016, 28. rujna). *Interview / Alexander Nix*. Preuzeto sa: https://www.contagious.com/blogs/news-and-views/interview-alexander-nix Pristupljeno: 18.9.2018.
51. Šeruga, D. (2018). *Mrežna forenzika*. Zagreb, Filozofski Fakultet Sveučilišta u Zagrebu.
52. Tails (n.d.) *About*. The amnesic incognito live system. Preuzeto sa: https://tails.boum.org/about/index.en.html Pristupljeno: 16.9.2018.
53. Tails (n.d.) *Acknowledgements and similar projects*. The amnesic incognito live system. Preuzeto sa: https://tails.boum.org/doc/about/acknowledgments_and_similar_projects/index.en.html Pristupljeno 16.9.2018.
54. *The 8 Principles of the Data Protection Act 1998 and how GDPR will affect them* (2017, 21. veljače). Preuzeto sa: https://vinciworks.com/blog/8-principles-data-protection-act-gdpr-guide/ Pristupljeno: 11.9.2018.
55. Titcomb, J. (2015, 23. rujna). *US surveillance makes 'Safe Harbour' data treaty with EU invalid, European court adviser says*. Preuzeto sa: https://www.telegraph.co.uk/technology/internet/11884432/EUs-data-sharing-deal-with-US-is-invalid-European-Courts-Advocate-General-says.html Pristupljeno: 4.9.2018.

56. Tor Metrics (2018) *Users*. Tor. Preuzeto sa: https://metrics.torproject.org/userstats-censorship-events.html?start=2018-06-19&end=2018-09-15. Pristupljeno: 16.9.2018.
57. Trepte, S., Reinecke, L., Ellison, N.B., Quiring, O., Yao, M.Z., & Ziegele, M. (2017, 1. siječnja). *A Cross-Cultural Perspective on the Privacy Calculus*. SAGE journals. Preuzeto sa: https://doi.org/10.1177%2F2056305116688035 Pristupljeno 11.9.2018.
58. WikiLeaks(2017a) Cherry Blossom. WikiLeaks. Preuzeto sa: https://wikileaks.org/vault7/#Cherry%20Blossom Pristupljeno 9.9.2018.
59. WikiLeaks(2017b) Dark Matter. WikiLeaks. Preuzeto sa: https://wikileaks.org/vault7/#Dark%20Matter Pristupljeno 8.9.2018.
60. WikiLeaks(2017c) Development Tradecraft DOs and DON'Ts. WikiLeaks. Preuzeto sa: https://wikileaks.org/ciav7p1/cms/page_14587109.html Pristupljeno: 7.9.2018.
61. WikiLeaks(2017d) Elsa. WikiLeaks. Preuzeto sa: https://wikileaks.org/vault7/#Elsa Pristupljeno: 9.9.2018.
62. WikiLeaks(2017e) Marble Framework. WikiLeaks. Preuzeto sa: https://wikileaks.org/vault7/#Marble%20Framework Pristupljeno 8.9.2018.
63. WikiLeaks(2017f) Network Operations Division CNE Operational Data Exchange Format (Codex) Specification. WikiLeaks. Preuzeto sa: https://wikileaks.org/ciav7p1/cms/files/Codex-Spec-v1-SECRET.pdf Pristupljeno 7.9.2018.
64. WikiLeaks(2017g) Network Operations Division Cryptographic Requirements. WikiLeaks. Preuzeto sa: https://wikileaks.org/ciav7p1/cms/files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf Pristupljeno 7.9.2018.
65. WikiLeaks(2017h) Network Operations Division In-memory Code Execution Specification. WikiLeaks. Preuzeto sa: https://wikileaks.org/ciav7p1/cms/files/ICE-Spec-v3-final-SECRET.pdf Pristupljeno 7.9.2018.

66. WikiLeaks(2017i) Network Operations Division Persisted DLL Specification. WikiLeaks. Preuzeto sa: https://wikileaks.org/ciav7p1/cms/files/Persisted-DLL-Spec-v2-SECRET.pdf Pristupljeno 7.9.2018.
67. WikiLeaks(2017j) Scribbles. WikiLeaks. Preuzeto sa: https://wikileaks.org/vault7/#Scribbles Pristupljeno: 9.9.2018.
68. WikiLeaks(2017k) Vault 7: CIA Hacking Tools Revealed. WikiLeaks. Preuzeto sa: https://wikileaks.org/ciav7p1/ Pristupljeno 7.9.2018.
69. WikiLeaks(2017l) Weeping Angel. WikiLeaks. Preuzeto sa: https://wikileaks.org/vault7/#Weeping%20Angel Pristupljeno 8.9.2018.

7. Popis priloga