.

1 Država i privatnost(promeniti naslov)

Međutim, privatnost na internetu nije samo lični problem pojedinca, već ima daleko šire razmere koji dostižu i nivo same države. Stoga, kada se govori o privatnosti na internetu, treba pomenuti i odnos države i državnih institucija prema privatnosti pojedinca. Kroz istoriju je bio čest slučaj da su države narušavale privatnost pojedinaca kako bi ostvarile određene interese, rešile određene probleme ili u situacijama ekstremne opasnosti, kao što je na primer borba protiv terorizma. Ovome u prilog ide i činjenica da je slučajeva u kojima su američka administracija i službe kršile privatnost građana bilo mnogo, od prodaje podataka službenika tajnih službi novinarima i privatnim detektivima, do ilegalnog prisluškivanja američkih i stranih državljana od strane FBI-ja.

Neki od tih slučajeva su zloupotreba popisnih spiskova od strane američke vojske u Prvom i Drugom svetskom ratu, korišćenje policijskih dronova, kao i televizijske kamere zatvorenog kruga (eng. *closed-circuit television, CCTV*). O ovome svedoči i podatak da prosečan stanovnik Velike Britanije bude uhvaćen na kameri u proseku 300 puta dnevno [22,23]. Ne samo da pojedinac može biti uhvaćen na kameri, već se dešava i da država prisluškuje ono što određeni pojedinci u svakom trenutku govore. Iako je prisluškivanje razgovora i postavljanje bubica aktom američkog kongresa iz 1934. godine zabranjeno, osim u slučajevima kada postoji sudski nalog, to nije sprečilo FBI da nastavi da to da radi ilegalno, čak i tokom Drugog svetskog rada uz dozvolu predsednika Ruzvelta [28]. Nakon rata, nacionalna sigurnosna agencija (eng. *National Security Agency,* NSA), FBI i druge bezbednosne službe nastavile su sa kršenjem zakona o privatnosti pojedinaca, što se kasnije i proširilo na druge vidove komunikacije, i pre svega na internet.

Legalno narušavanje privatnosti na internetu

Usled pretnje po bezbednost SAD-a, donošeni su zakoni koji su bezbednosnim službama dali veća ovlašćenja, koja su automatski dozvoljavala ovim organizacijama upad u privatnost pojedinaca. U narednim odeljcima, biće navedeni neki zakoni kojima američka administracija dozvoljava narušavanje privatnosti na internetu.

Zakon o nadzoru stranih službi

Američka administracija je 1978. godine donela zakon o nadzoru stranih službi (eng. *Foreign Intelligence Surveillance Act*, FISA), kojim se dozvoljava tajni nadzor inostranih vlada i njihovih službi. Ovim zakonom američki predsednik je mogao da odobri elektronski nadzor stranih državljana na jednu godinu, pod uslovom da se time ne krši privatnost državljana Amerike. U suprotnom, administracija bi morala da dobije sudski nalog za prisluškivanje. Međutim, bez obzira na postojanje ovog zakona, postoje mnogi slučajevi kršenja njegovih odredbi. Tako je 2013. godine Edvard Snouden, bivši zaposleni u NSA i FBI, obelodanio na hiljade tajnih dokumenata američkih tajnih službi, među kojima se našao i projekat PRISM, koji je dozvoljavao NSA-i pristup mnogim serverima pojedinih internet kompanija, kao i velikoj količini privatnih informacija, među kojima su bili i video pozivi čijim je ovim odredbama dozvoljen

pristup čak i bez sudskog naloga [10]. U odeljku 3.2 detaljno će biti detaljno prikazan projekat PRISM.

Zakon o skladištenoj komunikaciji

Zakon o skladištenoj komunikaciji (eng. *Stored Communication Act*) predstavlja deo zakona o privatnosti pri elektronskoj komunikaciji (eng. *Electronic Communication Privacy Act*) iz 1986. godine i odnosi se na privatnost kolekcija elektronske pošte. Po ovom zakonu, vlastima nije potreban sudski nalog kako bi od dobavljača internet usluga (eng. *Internet provider*) dobili mejlove starije od 180 dana. Problem sa ovim zakonom se usložnjava činjenicom da od skoro provajderi pružaju klaud usluge, te korisnice više ne čuvaju na ovim serverima samo mejlove, već i veliku količinu drugih privatnih podataka, koje bi inače čuvali na svojim privatnim računarima. Prema tome, odredbe ovog zakona pružaju uvid u podatke koji prevazilaze skladištenu komunikaciju elektronske pošte i dozvoljavaju vlastima uvid i u privatne podatke koji su nekim drugim odredbama suštinski zaštićeni. Usled proširenja skladištenog prostora i funkcija provajderskih servera, skoro pedeset kompanija i organizacija koje smatraju da administracija ne bi smela da dobavlja privatne informacije korisnika sa klauda bez sudskog naloga, udružilo se u organizaciju pod nazivom Digital Due Process, kako bi zahtevali od administracije da unapredi ovaj zakon [24].

Commented [M1]: Ovde mi se čini da imate neku grešku – ne bi trebalo da internet provajderi mogu da pruže pristup mejlovima, već provajderi mejl usluga? Tipa gmail ili outlook ili šta god – u suprotvnom ova priča posle sa klaudom nema puno smisla

3.2 PRISM

Edvard Snouden je u junu 2013. godine obelodanio na hiljade tajnih dokumenata NSA i FBI, čime je otvoren jedan od većih slučajeva narušavanja privatnosti podataka. Među ovim dokumentima su se našli i dokumenti vezani za program PRISM, koji predstvlja tajni program korišćen za nadzor aktivnosti na internetu. Program je započet 2007. godine i u narednih nekoliko godina sve velike kompanije su dale saglasnost za nadzor njihovih servera: Majkro- soft 2007., Jahu 2008., Gugl, Fejsbuk i PalTalk 2009., Jutjub 2010., Skajp i AOL 2011. i Epl 2012. godine [10].

Prema FISA zakonu, NSA je imala pravo da uz sudski nalog traži podatke o pojedincu od internet kompanije. Međutim, kako su u NSA smatrali da ceo taj proces predugo traje i da su potrebni nalozi za oba učesnika internet konverzacije, program PRISM je bio idealno rešenje tog problema. Agencija je imala direktan pristup serverima gorenavedenih kompanija i mnogo veću slobodu u nadzoru i prikupljanju podataka, pa čak i praćenju poziva uživo preko interneta. NSA ovo i navodi u svojim dokumentima, gde ovaj program nazivaju "jednim od najvrednijih, jedinstvenih i najproduktivnijih pristupa koji NSA ima"[10]. Kada se uzme u obzir da je PRISM program omogućio prikupljanje mejlova, razgovora, video poziva, slika, video poziva i istorije pretraživanja korisnika, ne čudi što je za ove organizacije program PRISM bio od tolikog značaja.

Commented [M2]: Ovo je pisalo i gore, mislim da treba naglasiti kojim serverima, čijim serverima, u suprotnom je malo neozbiljno

Pored problema sudskih naloga, FISA zakon je predstavljao problem za NSA-u jer je sprečavao praćenje komunikacije između dva strana državljanina ukoliko ona ide preko servera koji se nalaze u SAD-u. Kako je većina servera velikih internet kompanija locirano u SAD-u, ovaj zakon je u velikoj meri ograničavao mogućnost praćenja komunikacije između stranih državljana. Zbog toga je 2007. godine donet zakon o zaštiti Amerike (eng. *Protect America Act*, PAA), koji je omogućio NSA-i da pokrene program PRISM i da zloupotrebi ovlašćenja data ovim zakonom kako bi prikupljali i pratili komunikaciju na internetu [13].

Iako su sve kompanije umešane u ovaj program negirale bilo kakvu povezanost, kasnije su izlazile sa izveštajima gde navode da je američka administracija zahtevala od njih nadzor i pristup podacima svojih korisnika.

Tako na primer, u izveštaju kompanije Jahu, navodi se da im je administracija pretila i kaznom od 250 hiljada dolara godišnje ukoliko ne budu saradivali [3]

2 Zaštita privatnosti

Enkripcija

Internet je otvoren sistem, što znači da se svi podaci kroz više uređaja, deljenih konekcija, ili čak bežično šalju kako bi stigli do željene destinacije. Ovaj sistem omogućava komunikaciju između uređaja koji mogu biti udaljeni više hiljada kilometara, ali zbog ključnog mehanizma koji to dozvoljava, ovaj sistem pravi i jedan od najvećih problema. Svaki uređaj koji se nalazi između početnog i krajnjeg odredišta može videti šta je poslato. Svaka elektron- ska pošta, ukucana lozinka i broj kreditne kartice mogu biti pročitani od strane nekoga u sredini te se da bi se ovo sprečilo koristi enkripcija.

Enkripcija je mehanizam kojim se bilo kakva informacija šifruje, tj. prebacuje iz čitljivog oblika u naizgled nasumične karaktere, koji se uz pomoć odgovarajućeg ključa mogu vratiti u svoj prvobitan oblik [14]. Jedan od prvih mehanizama enkripcije je Cezarova šifra (eng. *Caesar's cipher*) koja je dobila ime po Cezaru koji je slao šifrovane poruke svojoj vojsci koje su samo oni mogli da razumeju. Cezarova šifra je prilično jednostavna i zasniva se na zameni svakog karaktera za karakter koji je pomeren u abecedi za nekoliko mesta. Jedina potrebna informacija za šifrovanje je ključ koji označava broj pozicija za koji je karakter pomeren, a za dešifrovanje primalac samo treba da isko- risti negativnu vrednost ključa. Ovu enkripciju bi bilo koji čovek mogao da dešifruje vrlo brzo, tako da nije primenljiva u domenu računara, ali daje osnovu za razumevanje kompleksnijih algoritama koji se koriste pri upotrebi veb pregledača, elektronske pošte ili prilikom onlajn kupovine.

Enkripciju je moguće podeliti na simetričnu i asimetričnu enkripciju, pri čemu je Cezarova šifra primer simetrične enkripcije. Simetrična enkripcija se koristi u situacijama kada već postoji siguran kanal za komunikaciju, te je potreban samo jedan ključ. Još jedan primer ove vrste enkripcije je AES (eng. *Advanced Encryption Standard*), koji se koristi kod virtuelnih privatnih mreža (o kojima će biti reči u odeljku 5.2), za enkripciju hard diska, kompresiju (WinZip, RAR), kod alata koji se koriste za čuvanje šifara i za enkripciju poruka koje se šalju putem društvenih mreža kao što je Fejsbuk. Do sada nije zabeležen uspešan napad na AES, ali to ne znači da je u potpunosti siguran. Postoje takozvani šide-channel"napadi (tajming ili elektromagnetni napadi koji) koji su bazirani na poznava- nju informacija o fizičkom načinu implementacije algoritma, okruženju ili samom sistemu na kome se izvršava [18].

Na internetu se uglavnom koristi asimetrična enkripcija. Ona podra- zumeva da svako ko učestvuje u komunikaciji ima svoj javni i privatni ključ, tako da postoje dva različita ključa, za razliku od simetrične u kojoj postoji samo jedan. Javni ključ pojedinca je poznat svima, a privatni ključ zna i koristi samo osoba koja ga poseduje. Pri slanju poruke, pošiljalac je najpre šifruje sa javnim ključem primaoca, a zatim svojim privatnim ključem. Kada primalac do- bije poruku, on je dešifruje uz pomoć javnog ključa pošiljaoca i nakon toga sopstvenim privatnim ključem. Ovim je obezbeđena komunikacija tako da niko sa strane ne može da pročita niti promeni prosleđenu poruku, a da se to ne detektuje. Par ključeva kod asimetrične enkripcije se generiše po matematičkim principima, tako da ako se nešto šifruje uz pomoć javnog ključa, može se dešifrovati privatnim i obrnuto. Najpopularniji primer asimetrične enkripcije je RSA (eng. *Rivest–Shamir–Adleman*) [12]. Ona se obično ne koristi za enkripciju čitavih poruka ili fajlova, već se koristi u kombinaciji sa drugim šemama enkripcije

Commented [M3]: Možda je do toga što ja pojma nemam, ali je meni ovo najnerazumljiviji deo, ostalo mi je sve ok.
Ne umem ni da ga preformulišem lepo koliko je konfuzno

Commented [M4]: Ovo ovde isto kao sa Marsa palo, ali ne umem da promenim tako da se bolje uklapa jer ne razumem

ili kao digitalni potpis za dokazivanje autentičnosti i integriteta

poruke. Fajlovi se obično enkriptuju nekom simetričnom enkripcijom, a zatim se njihovi ključevi enkriptuju pomoću RSA. Pošto za razliku od AES, RSA može biti razbijena faktorizacijom celih brojeva, ključevi moraju biti duži. Nacionalni Institut za Standarde i Tehnologiju predlaže korišćenje ključa dužine 2048 bitova. RSA je prisutna kod pretraživača veba, imejlova, VPN usluga, četova i drugih komunikacionih kanala.

Virtuelne privatne mreže (VPN)

Virtuelne privatne mreže (eng. *virtual private network*) nastale su usled potrebe da se biznisi, organizacije, vlade i slični subjekti koji poseduju osetljive informacije zaštite od hakovanja i gubitka podataka u slučajevima kada je potrebno da im udaljeni korisnici ili satelitske kancelarije pristupe, kao i radi smanjenja telekomunikacionih troškova efikasnijim korišćenjem infrastrukture. VPN su privatne mreže koje rade preko deljene javne infrastrukture kao što je internet [26]. Virtuelna je zato što ne postoji odvojena fizička infrastruktura za datu mrežu, već koristi već postojeću javnu infrastrukturu. Privatna je zato što omogućava bezbednu upotrebu uz garanciju da će samo članovi mreže moći da vide poslate informacije [17]. VPN omogućavaju privatnost podataka korišćenjem sigurnosnih procedura(enkripcija) i protokola tuneliranja (IPsec, PPTP, L2TP). Pod tuneliranjem se podrazumeva da VPN pravi "tunel"između korsinika pri čemu se podaci enkriptuju na strani pošiljaoca, šalju kroz tunel i zatim dekriptuju na strani primaoca. Pored podataka mogu se kriptovati i polazna i završna adresa radi veće sigurnosti [11].
Jedan od poznatijih tipova VPN-a je VPN "od lokacije do lokacije"(eng. *site-to-site*) je tip mreže koja omogućava uspostavljanje bezbedne komunikacije između više poslovnica na različitim lokacijama preko javne infrastrukture, i time se podaci sa jedne lokacije stavljaju na korišćenje zaposlenima na drugoj. Drugi osnovni tip ovih mreža je VPN za udaljen pristup (eng. *remote access VPN*), koja omogućava pojedincima da uspostave bezbednu vezu sa udaljenom mrežom i pristupe njenim resursima kao da su direktno povezani na dati server.

Iako prvobitno nisu bile namenjene za to, usled skorašnjih otkrića o velikim projektima za nadzor i ograničenja koje određene vlade nameću svojim građanima, sve više raste upotreba VPN usluga za zaštitu privatnosti pojedinaca, zaštitu od cenzurisanja kao i za pristup sadržaju koji je geografski ograničen [21]. Još jedan od razloga za povećano korišćenje je porast upotrebe javnih mreža koje je prouzrokovano širenjem mobilne industrije. Ovo je dovelo do stvaranja uslova za napade kao što su krađa akreditiva, presretanje paketa i krađa sesija, što vodi do toga da neki korisnici koriste VPN za zaštitu svojih interakcija. Mnoge VPN usluge nude mogućnost izbora izlaznih tačaka tako da korisnici mogu da dobiju IP adrese u različitim državama.

Iako do nekog stepena VPN provajderi pružaju navedene usluge, dovodi se u pitanje njihova sposobnost da očuvaju anonimnost i privatnost. Privatnost se kod ovih mreža ne odnosi na privatnost krajnjih korisnika već na povezivanje više privatnih mreža. Zbog lakoće korišćenja, velikih performansi i jakog marketinga postoji velika privlačnost prema ovim mrežama, iako neinformisanost korisnika dovodi do problema.

Rizici za korisnike VPN

Iako veliki broj pružalaca VPN usluga tvrde da pružaju robusne i sigurne infrastrukture uz obezbeđivanje bezbedonsti korisnika tako što ne

Commented [M5]: Ovde bi bilo dobro da se doda neka praktična primena ili nešto, pošto je ovo do sada bilo baš nekako zasnovano na ne znam nekim praktičnim stvarima a ova enkropcija je onako baš suvoparna

Commented [M6]: Ovde možda dodati kako se to VPN koristi u ove svrhe

Commented [M7]: Kako??? Kog problema???

loguju podatke, ne postoje alati i istraživanja koji te tvrdnje proveravaju. Pored toga neki provajderi su poznati po tome što prodaju podatke korisnika i manipulišu saobraćajem. Takmičenje između provajdera zajedno sa nedostatkom objektivnih mera kvaliteta dovodi do manipulacije i prikrivanja informacija koje bi bile od značaja za klijenata. Usled nedostatka nezavisnih ocena VPN usluga korisnici su primorani da se o tome informišu sa blogova ili veb sajtova. Ti sajtovi su većinom podržani od strane VPN partnerskog marketinga i usluga, pa se od njihovih ocena ne može očekivati nepristrasnost. To se odnosi na neke od najbolje rankiranih sajtova za ocenjivanje VPN usluga. Pored curenja saobraćaja zbog loše bezbednosti oko 10% VPN servisa presreću i/ili ma- nipulišu saobraćajem s tim što su mogući načini za nadziranje saobraćaja koji su teški da se otkriju. Takođe, VPN servisi obično obećavaju veliki broj različitih geografskih lokacija koje korisnici mogu da izaberu kao iz- lazne čvorove, ali oko 10% njih daje netačne informacije. Između 5 i 30 procenata tih čvorova nalazi se na potpuno drugim lokacijama od onih koje su predstavljene. Čak postoje provajderi koji tvrde da imaju lokacije u preko 190 država, a u stvarnosti se serveri nalaze u ne više od 10 centara podataka [21].

Commented [M8]: Preglupo

Commented [M9]: Ovo je konfuzno + kontradiktorno jer kao nema informacija o opasnosti, a onda se govori o konkretnim procentima, što znači da zapravo ima informacija…. Glupavo mi je ovo