Përgjimet në Internet

Altin Ukshini

Janar / 2016
Prishtinë

Altin Ukshini

Përgjimet në Internet

Janar / 2016

ABSTRAKTI

Ky shkrim merret me fenomenin e përgjimit në masë dhe më saktësisht me përgjimin e përdoruesve të rrjeteve kompjuterike si Interneti. Përgjimi në masë është një ndër debatet më të nxehta në botën digjitale. Privatësia dhe siguria e të dhënave tona personale po bëhet më e vështirë çdo ditë e më shumë pasi që qeveri e agjenci të ndryshme të inteligjencës në botë po përgjojnë përdoruesit e internetit dhe shërbimeve tjera teknologjike me dhe pa dijeninë e tyre përmes programeve tashmë të njohura si p.sh PRISM – program i cili doli në pah nga ish punonjësi i NSA Edward Snowden. Korporata të ndryshme po bashkëpunojnë me këto programe përgjimi dhe po detyrohen që të ndajnë informacionet tona si përdorues. Pak nga ne kemi njohuri për këto përgjime masive të cilat edhe thyejnë rregullat themelore të të drejtave të njeriut, e madje edhe po të dinim për to, si përdorues të thjeshtë të internetit ndihemi të paaftë për të reaguar dhe nuk kemi njohuri të mjaftueshme teknologjike për të ndërmarrë hapa për mbrojtjen e privatësisë tonë duke përdorur softuerë e aplikacione me burim të hapur për të cilat flitet në këtë temë.

Përmbajtja

FJALORI I TERMAVE

CCTV	-	Closed-circuit television
CIA	-	Central Intelligence Agency
FBI	-	Federal Bureau of Investigation
NSA	-	National Security Agency
CIPAV	-	Computer and Internet Protocol Address Verifier
PC	-	Personal Computer
OKB	-	Organizata e Kombeve të Bashkuara
CALEA	-	Commission on Accreditation for Law Enforcement Agencies
DARPA	-	Defense Advanced Research Projects Agency
DHS	-	Department of Homeland Security
IP	-	Internet Protocol
GPS	-	Global Positioning System
ISP	-	Internet Service Provider
VoIP	-	Voice over IP
SHBA	-	Shtetet e Bashkuara të Amerikës
CEO	-	Chief Executive Officer
OTR	-	Off-the-Record
HTTPS	-	Hypertext Transfer Protocol Secure

1 HYRJE

Përgjimi është monitorim i sjelljes, aktiviteve, ose informacioneve tjera që ndryshojnë, zakonisht i njerëzve për qëllim që të ndikojë, menaxhojë, drejtojë, ose mbrojë ata. Kjo mund të përfshijë vëzhgimin nga distanca me anë të pajisjeve elektronike (të tilla si kamera CCTV), ose përgjimin e informacionit të transmetuar në mënyrë elektronike (të tillë si trafiku në internet apo thirrjet telefonike); dhe kjo mund të përfshijë metoda të thjeshta, relativisht teknologji të ulëta ose jo, si agjentë të inteligjencës njerëzore dhe përgjimit postar.

Përgjimi për shumë vite është përdorur nga qeveritë për mbledhjen e informatave, parandalimin e krimit, mbrojtjen e një procesi, personi, grupi apo objekti, apo për hetimin e krimeve, gjë që mendohet t'i ketë pasur fillet në vitet 1791. Përgjimet janë përdorur edhe nga organizatat kriminale të planifikojnë dhe të kryejnë krime të tilla si vjedhje dhe rrëmbime, nga bizneset për të mbledhur inteligjencë dhe të dhëna të vlefshme për to, dhe nga hetuesit privatë.

Përmes këtij dokumenti tentohet të jepet një pasqyrë e shkurtër mbi ndodhitë e fundit dhe diskutimin global mbi epokën e përgjimeve masive, jepen informata rreth llojeve dhe programeve të përgjimit në masë, arsyeve që qeveritë kanë për të ndërmarrë aktivitete të tilla, ligjeve të shumta në shtete të ndryshme që lejojnë përgjimin e qytetarëve, pse qytetarëve duhet të ju interesoj privatësia e tyre si dhe në fund përfshihen edhe detaje bazike / rekomandime mbi veglat dhe softuerët që mund të përdoren për të qenë më të sigurtë online dhe të mbrojmë privatësinë tonë.

2 SHQYRTIMI I LITERATURËS

Përgjimi është shpesh një shkelje e privatësisë dhe është kundërshtuar nga grupe të ndryshme të lirive civile dhe aktivistë. Demokracitë liberale kanë ligje që kufizojnë qeverinë e brendshme dhe përdorimin privat të përgjimit, zakonisht kufizimin e tij në rrethanat kur siguria publike është në rrezik. Qeveri autoritare rrallë kanë ndonjë kufizim të brendshëm; por spiunazhi ndërkombëtar është e përhapur midis të gjitha llojeve të këtyre shteteve. Nëse flasim më konkretisht për përgjimet e kompjuterëve dhe rrjeteve kompjuterike në përgjithësi, mund të themi që ky lloj i përgjimit ka të bëj me monitorimin e aktivitetit të kompjuterëve dhe të dhënave të ruajtura në hard drive, ose të dhëna që transferohen mbi rrjetet kompjuterike të tilla si Interneti. Programe për përgjimin e kompjuterëve dhe rrjeteve kompjuterike janë të përhapura sot dhe pothuajse i gjithë trafiku në internet mund të monitorohet për veprimtari të paligjshme. Me ardhjen e programeve të tilla si “Vetëdijesimi Total i Informacionit” (Total Information Awareness), teknologjitë si kompjuterët me shpejtësi të lartë të përgjimit dhe softuerët biometrik dhe me akte si “Akti për Asistencën e Komunikimit për Zbatimin e Ligjit” (Communications Assistance For Law Enforcement Act) qeveritë tani posedojnë një aftësi të paparë për të monitoruar aktivitetet e qytetarëve. Shumë të drejta civile dhe grupe të privatësisë, të tilla si “Reporterët Pa Kufi” (Reporters Without Borders), “Electronic Frontier Foundation”, dhe “Bashkimi Lirive Civile Amerikane” (American Civil Liberties Union), kanë shprehur shqetësimin se me rritjen e përgjimit të qytetarëve ne do të përfundojë deri në një shoqëri të përgjimit në masë, me liri të kufizuara politike dhe / ose personale. Frika e tillë ka çuar në padi të shumta të tilla si “Hepting v. AT & T” dhe sulme të ndryshme nga grupi i hacktivistëve Anonymous, një nga të cilat ishte edhe hackimi në faqet e internetit të qeverisë Britanike në shenjë proteste për atë që ata konsideronin "përgjimi drakonian".

2.1 Llojet e përgjimeve

Përgjimet në përgjithësi ndahen në shumë lloje, disa nga to janë si vijojnë:

2.1.1 Përgjimet e shërbimeve postare

Me më shumë njerëz që përdorin faksin dhe e-mail, rëndësia e përgjimit të sistemit postar është duke u reduktuar në favor të përgjimit të uebit dhe telefonit. Megjithatë, agjencitë e zbulimit janë ende në gjendje të përgjojnë postën në rrethana të caktuara. CIA dhe FBI kanë kryer 12 fushata të veçanta të hapjes së postës në shënjestër ndaj qytetarëve amerikanë, prej ku më shumë se 215.000 komunikime u zbuluan, hapën, dhe fotografuan.

2.1.2 Përgjimet e kompjuterëve

Shumica e përgjimeve të kompjuterëve përfshin monitorimin e informacionit dhe trafikut në internet. Për shembull, në Shtetet e Bashkuara, nën Aktin për Asistencën e Komunikimit për Zbatimin e Ligjit, të gjitha thirrjet telefonike dhe trafiku në internet duhet të jenë në dispozicion për monitorim në kohë reale nga agjencitë federale të zbatimit të ligjit. Megjithatë, ka shumë informacion në internet për hetuesit njerëz që të kërkojnë manualisht përmes tij. Kjo është arsyeja pse sistemet e automatizuara kompjuterike përgjojnë në internet sasi të mëdha të trafikut dhe identifikojnë diçka interesante duke përdorur disa fjalë kyçe dhe fraza, duke kontrolluar lloje të caktuara të shërbimeve online, apo biseduar me njerëz të dyshimtë. Në fakt, miliarda dollarë shpenzohen çdo vit nga FBI, Zyra e Vetëdijes së Informacionit, dhe NSA për të krijuar, blerë, zbatuar dhe për të menaxhuar sistemet si Carnivore, NarusInsight dhe ECHELON, në mënyrë që të kapin dhe analizojnë të gjithë këtë informacion.

Kompjuterët personal janë gjithashtu një objektiv vëzhgimi për shkak të informacionit që ata kanë. Nëse dikush është në gjendje të instalojë softuerë Magic Lantern i FBI-së dhe CIPAV në një PC, ata lehtë mund të marrin qasje të paautorizuar në këtë informacion. Në vetëm një muaj në vitin 2013 NSA ka mbledhur 97 miliardë copa të inteligjencës nga rrjetet kompjuterike në mbarë botën dhe ka përgjuar mbi 500 milion lidhje të të dhënave të shtetasve gjermanë. Liberty ka vënë në dukje se shtetet kanë tendencë të kenë lirinë të përgjojnë më shumë jashtë vendit se sa në shtëpi, kështu vërehet një nënkontraktim jashtë punës së tyre të pistë për të tjerët, ku pastaj pretendojnë të jenë duke mbrojtur qytetarët e tyre. E drejta për privatësi dhe e drejta e mbrojtjes me ligj kundër përgjimeve të tilla është e përfshirë në nenin 12 të Deklaratës së OKB-së për të drejtat të njeriut dhe është elaboruar më tej në Konventën e OKB-së për të drejtat civile dhe politike.

2.1.3 Kamerat përgjuese

Në shumicën e rasteve, ato janë të lidhura me një pajisje regjistrimi me IP dhe shikohen nga personeli i sigurimit. Më parë, kamerat dhe pajisjet e regjistrimit ishin mjaft të shtrenjta dhe kërkohej personel njerëzorë për të monitoruar pamjet nga kamerat. Megjithatë, me teknikat moderne të lira të prodhimit, kjo u bë e thjeshtë dhe shumë më pak e kushtueshme për sistemet e sigurisë në shtëpi apo mbikëqyrjen e përditshme. Edhe analizimi i vazhdueshëm i këtyre videove është thjeshtuar pasi që tani ekzistojnë softuerë që pamjet dixhitale video i ruajnë si informacione të shfletueshme në një bazë të të dhënave prej ku mund të analizohen shumë më lehtë.

2.1.4 Telefonia mobile

Përgjimi zyrtarë dhe jozyrtarë i linjave telefonike është shumë i përhapur. Për shembull, në Shtetet e Bashkuara të Amerikës CALEA kërkon që i gjithë komunikimi i telefonisë mobile dhe VoIP të jenë në dispozicion për përgjim në kohë reale nga agjencitë e zbatimit të ligjit. Kjo është arsyeja pse të dy kompanitë më të mëdha të telekomunikacionit në Amerikë, AT&T dhe Verizon, kanë kontrata me FBI-në, të cilat kërkojnë ata të mbajnë të dhënat e tyre të thirrjeve telefonike të arritshme për agjencitë federale. Kompanitë janë paguar $ 1.8 milionë dollarë në vit për këtë. Brenda 2 viteve, FBI ka dërguar mbi 140,000 "Letra të Sigurisë Kombëtare", të cilat urdhëruan kompanitë telefonike të dorëzojnë të dhënat e thirrjeve të klientëve të tyre dhe historitë e shfletimit të internetit. 50% e tyre kanë kërkuar të dhëna për qytetarët amerikanë. Për më tepër, zbatimi i ligjit dhe shërbimet e inteligjencës në Britani të Madhe dhe SHBA kanë teknologji që lejojnë aktivizimin e mikrofonit në telefona nga distanca të largëta duke iu qasur parametrave diagnostikues dhe të mirëmbajtjes të këtyre telefonave dhe duke dëgjuar bisedat rreth personit që mban pajisjen. Përveç kësaj, telefonat celularë janë gjithashtu të përdorur shpesh për të mbledhur informacion mbi vendndodhjen e individëve. Vendndodhja gjeografike e një telefoni dhe personi që mban atë mund të gjenden duke llogaritur dallimet në kohë për një sinjal që të udhëtojë nga telefoni celular në antenat pranë pajisjes. Në Shtetet e Bashkuara, debatet vazhdojnë lidhur me ligjshmërinë e teknikave të tilla dhe në veçanti mbi pyetjen nëse një urdhër gjykate është i nevojshëm. Për shembull, të dhënat nga një operator tregojnë së agjencitë federale kanë kërkuar të dhëna mbi vendndodhjen e këtyre pajisjeve mbi 8.000.000 herë.

2.1.5 Analiza e rrjeteve sociale

Një tjetër formë e përgjimit është krijimi i hartave të rrjeteve sociale mbi bazën e informacionit nga shërbime të tilla si Facebook, Twitter së bashku me të dhënat e analizave të trafikut nga të dhënat e thirrjeve në telefonitë mobile. Pas kësaj, harta të tilla të rrjeteve sociale janë të dhëna të mbledhura në mënyrë që të nxirren detaje të dobishme, duke përfshirë interesat personale, miqësitë dhe përkatësitë, besimet dhe aktivitetet e individëve. Një shumë e agjencive qeveritare amerikane si DARPA, NSA dhe DHS kanë investuar në kërkime që përfshijnë analiza të rrjeteve sociale. Sipas komunitetit të inteligjencës, kërcënimi më i madh për fuqinë amerikane vjen nga grupet e decentralizuara të terroristëve, ekstremistëve dhe disidentët. Kërcënime të tilla mund të gjinden lehtë duke kërkuar për nyje të rëndësishme në rrjete dhe duke i hequr ato. Kjo është arsyeja pse autoriteteve i duhet një hartë e detajuar e rrjetit. AT&T ka zhvilluar një gjuhë programimi të quajtur "Hancock", e cila është në gjendje të analizoj baza të të dhënave të mëdha të thirrjeve telefonike dhe të trafikut të internetit dje të nxjerrin të dhëna për grupe të qytetarëve të cilët rregullisht thërrasin njëri-tjetrin ose vizitojnë faqe të caktuara të internetit. Kompania ka krijuar fillimisht këtë sistem për të zhvilluar lidershipin në marketing, por autoritetet federale kanë kërkuar rregullisht të dhëna të tilla nga kompanitë pa urdhër. Më pas FBI ka ruajtur të gjitha këto të dhëna në bazat e të dhënave të veta, pa marrë parasysh nëse ato ishin të dobishme ndonjëherë në hetime ose jo. Disa vëzhgues të industrisë mendojnë se përdorimi i rrjeteve sociale është një lloj i përgjimit pjesëmarrës/participues, që do të thotë se përdoruesit e këtyre faqeve në të vërtetë janë duke kryer përgjime mbi veten e tyre, duke botuar të dhëna të hollësishme personale të cilat mund të shihen nga të gjithë. Rreth 1/5 e punëdhënësve janë gjithashtu duke përdorur rrjetet sociale për të mbledhur informacion personal mbi punonjësit e ardhshëm ose aktual.

2.1.6 Përgjimi i Korporatave

Përgjimi i korporatave është monitorimi i sjelljes së dikujt nga një korporatë. Informacioni i mbledhur përdoret normalisht për qëllime marketingu ose shitet tek kompani të tjera. Përveç kësaj, ky informacion mund të ndahet edhe me autoritetet. Informacioni i mbledhur mund të përdoret si një formë e zbulimit të biznesit që i mundëson kompanisë të krijojë produkte mirë të menduara apo shërbime të veçanta për nevojat e konsumatorëve. Në rast se informacioni shitet tek kompanitë tjera, ai informacion përdoret nga ana e tyre për të njëjtin qëllim ose për qëllime të marketingut të drejtpërdrejtë, si reklama në motorët e kërkimit, ku reklamat bazohen duke analizuar historinë e tyre të kërkimit dhe email të ruajtura në një bazë të dhënash. Për shembull, Google, motori i kërkimit më i njohur në botë, mban të dhënat identifikuese për secilin kërkim, duke përfshirë një adresë IP dhe frazat e kërkimit në një bazë të dhënash për më shumë se një vit. Google gjithashtu skanon përmbajtjet në Gmail për të krijuar reklama në shënjestër të bazuara në atë që përdoruesit janë duke folur me të tjerët. Deri më tani, Google është e njohur si agjencia më e madhe e reklamave në internet: reklamat e tyre shfaqen në miliona faqe të ndryshme, gjë që ju lejon atyre të fitojnë të holla nga përdoruesit të cilët klikojnë mbi to. Në ndërkohë, çdo faqe që përmban reklama, Google i modifikon "cookies" në PC të çdo përdoruesi, të cilat gjurmojnë vizitorët në të gjithë faqet e internetit dhe mbledhin të dhëna mbi zakonet e tyre në shfletimin e internetit. "Cookies" mbajnë gjurmë të shërbimeve që njerëzit vizitojnë dhe po ashtu mbajnë edhe gjurmë të aktiviteteve të tyre në ato shërbime. Këto të dhëna, së bashku me të dhënat nga llogaritë e-mail dhe historitë nga makinat e kërkimit, mbahen nga motorët e kërkimit që të përdoren më vonë për ndërtimin e një profili të përdoruesit më të saktë dhe sigurojnë reklama më të mira në shënjestër. Anketa për monitorimin elektronik dhe përgjimin me rreth 300 kompani amerikane është kryer nga Shoqata

Amerikane e Menaxhimit dhe Institutit të ePolicy (American Management Association and the ePolicy Institute). Ata zbuluan se mbi 25% e punëdhënësve kanë pushuar nga puna punonjësit e tyre për keqpërdorimin e E-mail dhe rreth 30% kanë pushuar nga puna punonjësit e tyre për keqpërdorimin e uebit. Mbi 40% e kompanive monitorojnë e-mail trafikun e punonjësve të tyre, ndërsa 66% e kompanive monitorojnë lidhje në internet. Për më tepër, shumica e punëdhënësve përdorin softuer për të bllokuar shërbime të ndryshme në internet, duke përfshirë faqet pornografike, faqet e lojërave, rrjetet sociale, dhe faqet sportive. Raporti gjithashtu thekson se disa kompani shkojnë aq larg sa monitorojnë përmbajtjen e shtypur në taste dhe kohën e kaluar në tastierë për të gjetur se çfarë punonjësit e tyre shkruajnë për kompaninë. Autoritetet amerikane shpesh merrnin qasje në këto baza të të dhënave të korporatave, si formalisht dhe joformalisht. Në përgjithësi, agjencitë federale kanë formuar një partneritet për ndarjen e të dhënave me më shumë se 34,000 kompani, si pjesë e programit të tyre Infragard. Qeveria amerikane ka mbledhur edhe të dhëna nga programe të kartelave të blerjes në dyqane, gjë që u lejon atyre të ndjekin modelet e konsumatorëve, blerjet e tyre i ruajnë në baza të të dhënave në mënyrë që të gjejnë terroristë duke analizuar zakonet e tyre të blerjes.

2.1.7 Imazhe satelitore

Në vitin 2007, Zyra Kombëtare e Aplikimeve të DHS është autorizuar për t'u dhënë agjencisë federale një qasje në imazhet satelitore ushtarake të inteligjencës dhe sensorë të aeroplanëve, me qëllim që t'i përdorin ato për të vëzhguar aktivitete të qytetarëve amerikanë. Ndërkohë, satelitët dhe sensorët e avionëve mund të depërtojnë retë, zbulojnë gjurmë kimike dhe identifikojnë objekte në kohë reale me video në rezolucion të lartë.

2.1.8 Pajisjet me radio frekuencë dhe pajisjet me gjeolokacion

Në Shtetet e Bashkuara, policia mund të instalojë fshehurazi pajisje si Sisteme të pozicionimit global në automjete për të monitoruar lëvizjet e pronarëve të tyre, pa një urdhër. 4 vjet më parë, autoritete kanë argumentuar në gjykatë se ata kanë të drejtë për ta bërë këtë. Një numër i qyteteve janë aktualisht duke punuar në pilot projekte që kërkojnë të burgosurit të veshin pajisje GPS në mënyrë që të ndjekin lëvizjet e tyre, pasi ata të dalin nga burgu. Telefonat celularë mund të përdoren gjithashtu shpesh për të mbledhur informacione të vendndodhjes. Kjo mund të përcaktohet mjaft lehtë, pavarësisht nëse telefoni është duke u përdorur apo jo, përmes teknikës të përshkruar më lart, e cila llogarit dallimet në kohë për një sinjal për të udhëtuar nga celulari në antenat përreth.

2.2 Ligje të njohura qeveritare për censurimin dhe përgjimin e Internetit

Bota është e ndarë kur bëhet fjalë për internetin, shumë qytetarë e shohin atë si një rrjet të gjerë të informacionit të lirë, ose gati të lirë ku mund të gjeni informacionin më neutral dhe ndoshta më të mirë. Shumë qeveri e shohin atë si diçka që duhet të kontrollohet, duke shkuar aq larg sa fusin apo përpiqen për të futur ligje rregullative për përdorimin e internetit. Këtu është një pasqyrë e shkurtër e katër ligjeve më të njohura qeveritare, rregulloret dhe çfarë duan të thonë.

2.2.1 SOPA

Stop Online Piracy Act (SOPA) ishte një projekt-ligj sugjeruar në fund të vitit 2011 dhe paraqitur në shtëpinë e bardhë amerikane në fillim të vitit 2012. Në këtë projekt-ligj u propozua t'i jepej Departamentit të Drejtësisë dhe mbajtësit të të drejtave autoriale fuqinë për të rrëzuar (mbyllur) faqe të interneti për shkak të thyerjes së ligjit të copyright dhe kjo pa dëgjuar mbrojtjen nga pronarët e faqjes së internetit. Gjithashtu i jepte autorit fuqinë për të paraqitur ankesa ndaj atyre faqeve si dhe t'i kërkonin kompensim gjithashtu edhe kompanive me të cilat ato faqe kanë bërë biznes. Ata do të mund të mbyllnin faqe interneti, pa pasur nevojës që fillimisht të hiqnin materialin e paligjshëm, e gjitha kjo mund të bëhej pa hyrë fare në procedura gjyqësore. SOPA gjithashtu do të kishte bërë paraqitjen e materialeve pirate krim, me një afat të mundshëm për burgim deri në pesë vjet. Po shikove ndonjë video me muzikë të piratuar youtube (pothuajse çdo video është e tillë), ju mund të shkonit në burg për të. Edhe më keq, postimi i ndonjë lidhjeje të internetit me materiale të paligjshme në një rrjet social mund të rezultonte në mbylljen e të gjithë rrjetit. Problemi i madh me SOPA-s ishte se ajo do të kishte dhënë pushtet Departamentit të Drejtësisë për të mbyllur qasje në faqet vendase dhe të huaja në SHBA.

2.2.2 PIPA

Protect IP Act është versioni i senatit Amerikan për SOPA. Ndërsa pothuajse identike në pothuajse të gjitha aspektet, ka dy dallime kryesore. Fillimisht nuk u kërkonte motorëve të kërkimit të ndalnin punën me faqe të huaja të internetit që thyenin ligjin e copyright. PIPA ende lejonte autorëve të paraqisnin ankesa ndaj vendeve të huaja. E dyta ishte që PIPA kërkonte ndërhyrje më të madhe të gjykatës kur bënte ndjekje për thyerje të ligjit të copyright. Në fund të janarit, senati amerikan pauzoi këtë akt deri sa këto çështje për të të zgjidheshin.

Protestat për kundërshtimin e SOPA dhe PIPA njihen gjithashtu edhe si protestat më të mëdha që janë organizuar ndonjëherë online.

2.2.3 CISPA

Pas që SOPA dhe PIPA nuk arritën të kalojnë, ligjvënësit amerikanë paraqitën një sërë të ligjeve të quajtura Cyber Intelligence Sharing and Protection Act (CISPA). Qëllimi kryesor i CISPA ishte për tu mbrojtur kundër rreziqeve të sulmeve kibernetike dhe ishte zgjeruar për të mbuluar po ashtu edhe sigurinë kombëtare. Në qoftë se CISPA kalonte, agjencitë ushtarake dhe qeveritare do të ishin në gjendje të mblidhnin dhe të ndanin të dhënat private nga kompanitë pa urdhër gjykate. Kompanitë do të ishin në gjendje të ndanin të dhëna me agjencitë qeveritare, për aq kohë sa ka të bëjë me një kërcënim në internet. Këto kërcënime nuk përfshijnë asgjë në lidhje me përpjekjet për të dëmtuar rrjetet publike dhe private, vjedhjet dhe përdorimin e gabuar të të dhënave. Me fjalë të tjera, po të shkarkonit një film nga Youtube apo Google që mbrohej me copyright - pronari i YouTube - do të kishte të drejtë ligjërisht të ndante informacionin tuaj me qeverinë Amerikane. Gjëja më e keqe në lidhje me këtë projekt-ligj ishte se ajo i jepte lejen qeverisë amerikane për të monitoruar të gjitha aktivitetit tuaja në Internetit dhe të përdornin informacionin tuaj pa detyrim.

2.2.4 ACTA

Marrëveshja e Tregtisë kundër falsifikimit është një akt shumëkombësh i krijuar për të ndihmuar në parandalimin e vjedhjes së ideve dhe materialeve që janë të mbrojtura me copyright në çfarëdo mediume përfshirë edhe internetin. Çfarë i bënte ky ligj internetit ishte që i kthente ISP-të në Policë të Uebit. Në atë kohë, ligji ishte i paqartë për masën por do ti jepte pushtet qeverisë dhe kompanive të mëdha të monitoronin dhe të mbronin të drejtat e autorit. Megjithatë, ky është një projekt-ligj ndërkombëtar që është ratifikuar nga pothuajse të gjitha vendet e botës së parë. Ndërsa këto akte kanë origjinën në Shtetet e Bashkuara, në qoftë se ato do të kalonin, vendet e tjera perëndimore me shumë gjasë do të miratonin legjislacione të ngjashme me qëllim të mbrojtjes së interesave të vendit dhe kompanive që operojnë brenda. Një shembull i mirë i kësaj ishte projekt-ligji C-11, që aktualisht po debatohej në Kanada. Ai projekt-ligh kishte shume dispozita të njëjta si SOPA, PIPA dhe CISPA të cilat do mund të ndryshonin fytyrën e internetit në Kanada.

3 DEKLARIMI I PROBLEMIT

Qeveria amerikane, me ndihmën e operatorëve të mëdhenj të telekomunikimit, duke përfshirë AT&T, është angazhuar në përgjime masive të paligjshme të rrjeteve të komunikimit dhe ka përgjuar të dhëna për miliona amerikanë të paktën që prej 2001. Raportet e lajmeve në dhjetor të vitit 2005 për herë të parë zbuluan se NSA po përgjonte telefonatat dhe komunikimet në Internet. NSA po ashtu ka përgjuar komunikimet ndërmjet SHBA-së dhe shtetasve të huaj në internet për një numër vitesh, në kuadrin e një projekti të quajtur PRISM. Disa nga kompanitë më të mëdha të internetit, si Apple, Google e Yahoo ishin poashtu të përfshira. Microsoft ishte kompania e parë që u përfshi, në shtator të vitit 2007. Yahoo ndoqi Microsoft në mars të vitit 2008, Google në janar 2009, Facebook në qershor 2009, YouTube në shtator të vitit 2010, Skype në shkurt të vitit 2011 (para blerjes nga Microsoft), AOL në mars 2011 dhe në fund Apple në tetor të vitit 2012.

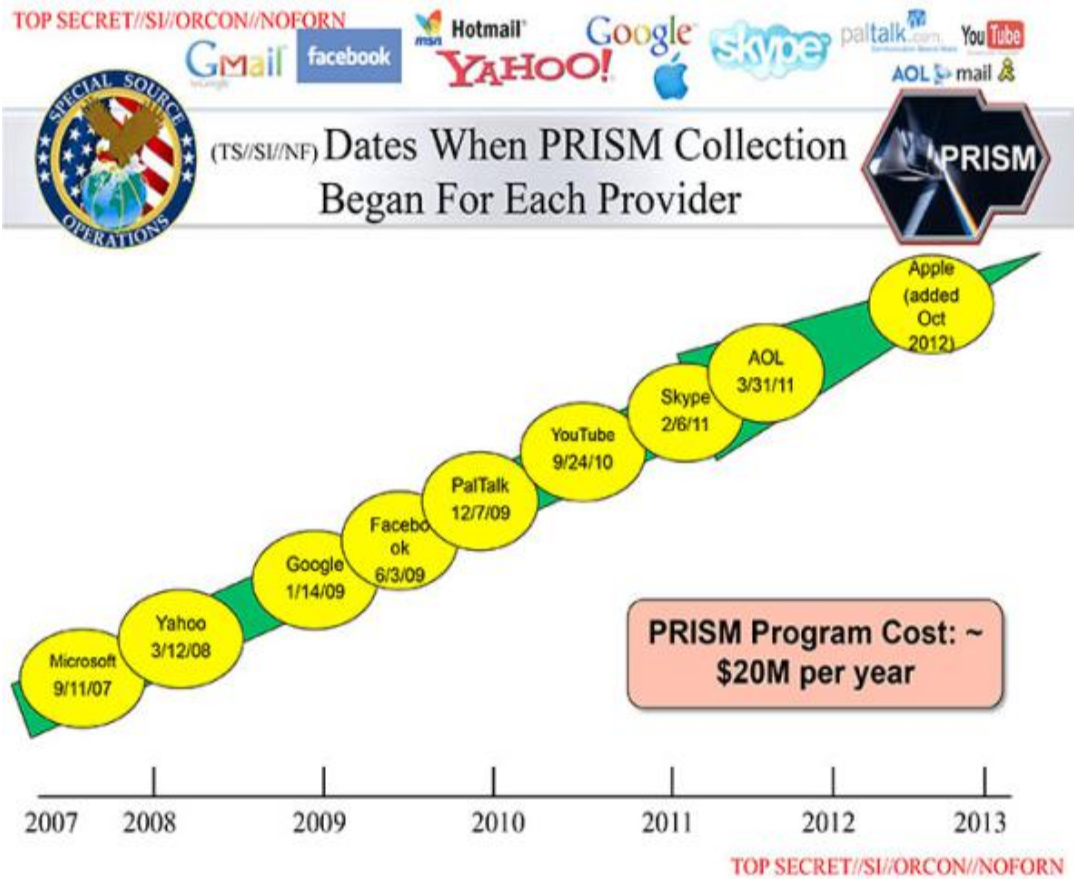

Figura 1: Involvimi i korporatave në programin PRISM

PowerPointi për PRISM thotë se ky program mund të mbledhë email, chat (video, zë), video, foto, të dhënat e ruajtura në PC, VoIP (telefonata në internet), transferimet e fileve, video konferencat, llogaritë në internet dhe rrjetet sociale si dhe një tjetër kategori të quajtur “kërkesat e veçanta".

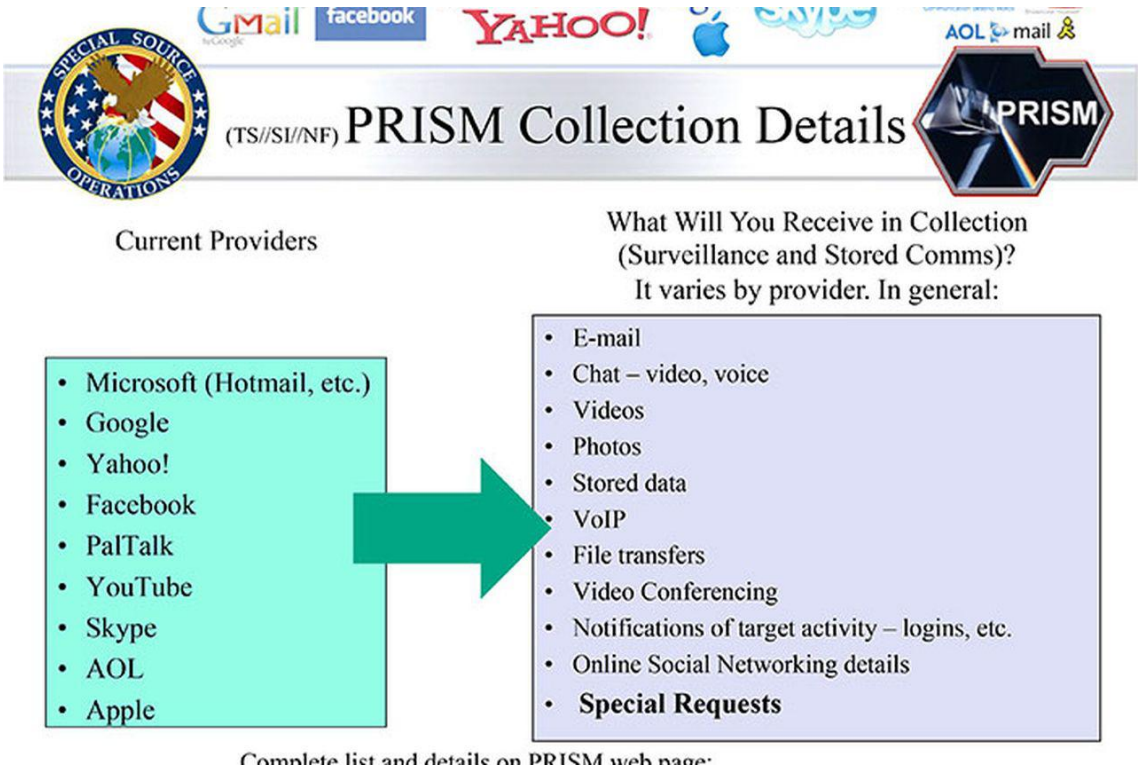

Figura 2: Të dhënat që mblidhen nga programi PRISM

Edward Snowden qytetar Amerikan, 32 vjeç, ish-oficer dhe sinjalizues (anglisht: whistleblower) i komunitetit të inteligjencës amerikane ishte personi që zbuloi dokumente për këto veprimtari të qeverisë amerikane të cilat dhanë një dritare të rëndësishme për publikun mbi NSA-në dhe programet masive të përgjimit në masë të partnerëve të saj ndërkombëtarë të shërbimeve inteligjente.

> ***“Unë nuk dua të jetoj në një botë ku çdo gjë që unë them, çdo gjë që unë bëj, me këdo që unë flas, çdo shprehje e kreativitetit, dashurisë apo miqësisë regjistrohet.” - Edward Snowden***

Këto zbulime në pah të së vërtetës gjeneruan vëmendje të paparë nëpër botë për ndërhyrje të privatësisë dhe sigurisë digjitale, duke çuar në një debat global mbi këtë çështje. Snowden ka punuar në role të ndryshme brenda Komunitetit të Inteligjencës së SHBA, duke u përfshirë dhe duke shërbyer fshehtë për CIA-n jashtë shtetit. Ai më së fundi ka punuar si analist i infrastrukturës në NSA, përmes një kontrate Booz Allen Hamilton, kur ai u largua nga shtëpia e tij dhe familja në Hawaii për të nxjerrë në pah këto sekrete në maj 2013. Pas udhëtimit në Hong Kong, Snowden zbuloi dokumente për publikun amerikan për programet e përgjimit në masë të NSA-së, të cilat treguan të kenë vepruar pa asnjë mbikëqyrje publike dhe jashtë kufijve të kushtetutës amerikane. Qeveria e SHBA ka akuzuar Snowden me vjedhjen e pronës qeveritare dhe dy akuza të mëtejshme sipas Aktit të Spiunazhit të vitit 1917. Çdo dënim i tillë mbart dënim maksimal me burgim deri në 10 vjet. Me SHBA-në në ndjekje të ekstradimit të tij,

Snowden është tani në Rusi, pas një viti azil të përkohshëm në Rusi atij i është dhënë zyrtarisht rezidencë për 3 vjet nga 1 gusht 2014. Gazetarët vazhdojnë të botojnë dokumente nga Snowden që zbulojnë sistemet e fshehta dhe të papërgjegjshme të përgjimeve moderne globale. Hero, tradhtar, geek - pa marrë parasysh se çfarë njerëzit mendojnë për Edward Snowden nuk ka dyshim se ai ka ndryshuar botën. Në qershor të vitit 2013, Snowden vuri në qendër të vëmendjes spiunazhin e brendshëm të Agjencisë Kombëtare të Sigurisë së SHBA. Zbulimet që Snowden ia paraqiti gazetarit Glenn Greenwald - i cili ka punuar në Guardian në kohën e dhënies së informacioneve shpjeguese - kanë bërë njerëzit të pyesin praktikat masive të përgjimit të administratës Obama. Qeveria e SHBA gjithashtu konsiderohet të ketë bërë ndryshime në programet e saj të mbikëqyrjes si PRISM - një program klandestin përgjimi përmes të cilit NSA që nga viti 2007 mbledh komunikime në internetit nga të paktën nëntë kompanitë më të mëdha amerikane të internetit.

Pas këtyre zbulimeve nga Snowden, qeveria gjermane përfundoi lidhjet e saj me kompaninë e wireless Verizon pasi që Snowden deklaroi se SHBA kishte kryer përgjime në masë në Gjermani, duke përfshirë edhe përgjimet në telefonin celularë të kancelares Angela Merkel. Kompani të tjera amerikane pasuan së shpejti në gjurmët e Verizon me Boeing dhe Brazilin që përfundoi kontratën e saj të mbrojtjes mbi 4 miliardë dollarë në vitin 2013. Pas këtyre zbulimeve pati një rritje drastike të përdorimit të enkriptimit në komunikime si dhe rritjen e numrit të kompanive startup që ofronin shërbime të komunikimit me siguri të lartë si p.sh Wickr, Silent Circle e Blackphone etj. Gjigantë të teknologjisë si Google dhe Yahoo rritën sigurinë e tyre pas këtyre informacioneve duke shtuar enkriptimin në email për përdoruesit e tyre. Shumë ekspertë të kibernetikës thonë se Snowden ka pasur një ndikim të stërmadh në komunitet. "Snowden ka arritur të mbledh 1.18 milion ndjekës brenda një periudhe të shkurtër kohore," tha Dodi Glenn, nënkryetar i sigurisë kibernetike në PC Pitstop. Fakti që Edward Snowden ka zbuluar nivele të pabesueshme të përgjimit dhe ka bërë që shumë njerëz të jenë më të kujdesshëm dhe me plot dyshime për gjërat që ata bëjnë në internet.

4 METODOLOGJIA

Qëllimi i këtij hulumtimi është përfitimi i njohurive të reja, apo thellimi i njohurive ekzistuese rreth përgjimeve elektronike në përgjithësi.

Në këtë punim seminarik, hulumtimi është bazuar në të dhëna sekondare si dhe në përvojat e mija gjatë punës me organizata që promovojnë lirinë e përdorimit të internetit, lirinë e shprehjes, burimet dhe njohuritë e hapura në Kosovë dhe më gjerë. Në të dhëna sekondare përfshihen publikime të shumta shkencore nga organizata dhe gazetarë të ndryshëm që punojnë për të drejtat e njeriut dhe demokracinë, video konferenca, ligjërata, shkrime në gazetat botërore dhe publikime tjera që kanë të bëjnë me këtë temë.

5 ANALIZA

Qeveritë në mbarë botën janë duke zgjeruar censurën dhe përgjimin e internetit, me ç’rast liria e përgjithshme në internet po bie për të pestin vit radhazi, sipas një raporti nga një grup që punon në tema mbi të drejtat e njeriut dhe demokracinë. Gati gjysma e 65 vendeve të ekzaminuar kanë parë të bie liria në internet që nga qershori 2014, tha Freedom House në një sondazh vjetor lëshuar muaj më parë. Një nga rëniet më të thepisura ka ndodhur në Francë, shteti i cili miratoi një ligj që shumë vëzhgues e krahasojnë me Aktin Patriotik Amerikan në vazhdën e sulmeve terroriste Charlie Hebdo në fillim të vitit 2015. Ukraina, e zhytur në një konflikt territorial me Rusinë dhe Libia gjithashtu kanë pasur rënie të shpejta. Raporti theksoi Kinën si vendi me kufizimet më të rënda mbi lirinë e internetit, e ndjekur nga Siria dhe Irani. Sri Lanka dhe Zambia, dy nga të cilat kohët e fundit kanë pësuar ndryshime në udhëheqjen e qeverisë, u kredituan me bërjen e përmirësimeve të mëdha në liri të përgjithshme në internet.

Në përgjithësi, në raport përmendet po ashtu që 14 vende kanë miratuar ligje në vitin e kaluar për të zgjeruar përgjimin nga qeveria. Edhe Kosova del të jetë një nga vendet të cilat në vitin 2015 kaloi ligjin për përgjimet elektronike pas tentimeve të shumta që nga viti 2012. Edhe pse ligji kaloi me shumë përmirësime të sugjeruara nga individë, organizata dhe kompani të shoqërisë civile, thuhet që ligji përsëri ka hapësirë për përmirësim. Shtetet e Bashkuara miratuan legjislacionin në qershor që efektivisht terminon mbledhjen e metadata-ve të thirrjeve telefonike nga NSA, një program i ekspozuar në vitin 2013 nga ish-kontraktori i NSA, Edward Snowden. Raporti gjithashtu zbuloi se komentet kritike për autoritetet qeveritare kishin më shumë gjasa për të nxitur censurën dhe se kompanitë private në 42 nga 65 vende u detyruan të fshini apo kufizojnë përmbajtjet në internet. Përveç kësaj, shumë qeveri morën qëndrime më agresive kundër enkriptimit dhe teknologjive për anonimitet online këtë vit.

Me këto të dhëna mbi aktivitetet e përgjimit në botë, është normale që dikush të bëjë pyetjen se “Pse ka rëndësi privatësia ime nëse unë nuk kamë asgjë për të fshehur”? Pyetja pse ka rëndësi privatësia, pyetje që ka lindur në kontekstin e një debati global, shkaktuar nga zbulimet e Edward Snowden-it sipas të cilave SHBA-të dhe partnerët e saj, fshehurazi krejt botës, e kanë shndërruar Internetin, dikur të mbajtur si një mjet të paparë çlirimi dhe demokratizimi, në një zonë të paparë përgjimi masiv dhe pa dallim. Ka një ndjesi të rëndomtë që lind nga ky debat, madje edhe mes personave që nuk ndihen rehat me përgjimin në masë, sipas të cilës nuk ka rrezik të njëmendtë që vjen prej kësaj mësymjeje në shkallë të gjerë, ngaqë vetëm ata që merren me krime kanë arsye për të dashur të fshihen dhe të merakosen për privatësinë e tyre.

Ky botëkuptim bazohet heshtur në tezën se në botë ka dy lloje njerëzish, njerëz të mirë dhe të këqij. Të këqij janë ata që thurin sulme terroriste ose që kryejnë krime të dhunshme, ndaj ka arsye të duan të fshehin atë që bëjnë, kanë arsye të merakosen për privatësinë e tyre.

Përkundrazi, njerëzit e mirë janë ata që shkojnë në punë, kthehen në shtëpi, rrisin fëmijë, shohin televizor. Internetin e përdorin jo për të thurur sulme me bomba por për të lexuar lajme dhe shkëmbyer receta gatimesh apo për të planifikuar lojërat e fëmijëve dhe këta nuk bëjnë asgjë të dëmshme ndaj nuk kanë se ç'të fshehin, as arsye për të pasur frikë se mos i përgjon qeveria. Njerëzit që shprehen kështu i kanë hyrë një valleje tejet të skajshme vetë-nënvlerësimi. Që faktikisht duhet kuptuar kështu, "Kam rënë dakord ta bëj veten një person kaq të padëmshëm dhe për të mos u pasur frikë, sa në fakt nuk trembem se mos qeveria e merr vesh se ç'po bëj." Kjo mendësi, gjeti shprehjen e saj më të kulluar, në një intervistë të 2009-s me CEO-n e Google-it, Eric Schmidt, i cili, i pyetur mbi tërë ato rrugë me të cilat kompania e tij po shkakton mësymjen ndaj privatësisë së qindra milionë njerëzve anembanë botës, u shpreh: "Nëse bëni diçka që s'doni ta marrin vesh të tjerët, ndoshta më mirë s'duhet ta bënit fare."

Argumenti "Asgjë për të fshehur" thotë se programet qeveritare të përgjimit nuk kërcënojnë privatësinë, përderisa ato zbulojë aktiviteteve të paligjshme dhe në qoftë se zbulohen veprimtari të paligjshme, personi që ka kryer aktiviteteve të tilla nuk ka të drejtë t'i mbajë ato private. Për këtë arsye, një person i cili favorizon këtë argument mund të deklarojë "Unë nuk kam asgjë për të fshehur" dhe në këtë mënyrë nuk shpreh kundërshtim ndaj mbikëqyrjes së qeverisë. Një individ që përdor këtë argument mund të themi se nuk duhet të ketë shqetësime nëse qeveria e mbikëqyrë atë pasi që ai / ajo nuk ka "asgjë për të fshehur". Për këtë argument flet edhe Edward Snowden, i cili në një prej sesioneve "Më pyesni çfarë të doni" (Ask me anything) në uebsajtin Reddit i përgjigjet një komentuesi që përdori argumentin "asgjë për të fshehur" duke i thënë:

“Argumenti se juve nuk ju intereson e drejta e privatësisë sepse ju nuk keni asgjë për të fshehur nuk është më ndryshe se kur thoni që nuk ju intereson liria e fjalës sepse ju nuk keni asgjë për të thënë.” - Edward Snowden

Në fjalë të tjera shpjegon se si e drejta e privatësisë duhet të jetë po aq e rëndësishme sa e drejta e fjalës së lirë dhe personat që përdorin këtë argument nuk i njohin mirë themelet e të drejtave të njeriut. Nëse një person zgjedh të mos marrë parasysh të drejtën e tij për privatësi, kjo nuk do të thotë automatikisht që të gjithë duhet të ndjekin shembullin, ose ju nuk mund të hiqni dorë nga të drejtat në emër të të tjerëve vetëm nëse ato nuk janë të dobishme për ju personalisht. Më thjesht, shumica nuk mund të votojë kundër të drejtave natyrore të pakicës. Arsyeja më e rëndësishme është se një sistem i përgjimit masiv shtyp lirinë tonë në të gjitha drejtimet. Na i bën të ndaluara të gjitha zgjedhjet mbi mundësitë e sjelljeve pa e ditur ne se çfarë ka ndodhur.

“Ai që nuk luan vendit nuk i vë re vargonjtë e tij.” - Rosa Luxemburg

Mund të orvatemi për t’i bërë të padukshëm ose të pakapshëm vargonjtë e përgjimit në masë, por kufizimet që imponojnë mbi ne nuk bëhen më pak të fuqishme.

6 DISKUTIME DHE PËRFUNDIME

Dy nga shpikjet ndoshta më të mëdha të brezit tonë janë Interneti dhe telefonat celularë. Këto kanë ndryshuar botën. Megjithatë, për habi të të shumtëve nga ne ato dolën të jenë mjeti i përsosur për përgjim nga ana e shtetit. Doli në pah që aftësia e tyre të mbledhin të dhëna, informacione dhe ndërlidhje thelbësisht rreth secilit nga ne dhe nga të gjithë ne është ekzaktësisht ajo që kemi dëgjuar nga zbulesat dhe rrjedhjet e informacionit rreth agjencive perëndimore të inteligjencës kryesisht agjencitë amerikane të zbulimit, që përgjonin pjesën tjetër të botës. Privatësia është një element themelorë i demokracisë tonë.

"Shtetet e Bashkuara trajtojnë sot Internetin siç mund të trajtonin një nga kolonitë e tyre. Pra po kthehemi mbrapsht në kohën e kolonizimit, dhe ne, përdorues të huaj të internetit, duhet të konsiderojmë amerikanët si mjeshtrat tanë." - Marcus Ranum

Përgjimi në masë është gjë e gabuar, është e vrazhdë dhe nuk duhet bërë. Por kjo me të vërtetë nuk do të ndryshojë situatën. Çfarë do të ndryshojë situatën për pjesën tjetër të planetit, është të rrihet larg nga sistemet e ngritura në SHBA. Kjo është më e lehtë të thuhet sesa të bëhet. Si është e mundur? Një shtet, cilido shtet në Evropë nuk mund të ndërtojë dhe të zëvendësojë shërbimet e cloud dhe sistemet operativë të prodhuar në SHBA. Megjithatë, mbrojtja nga kjo situatë nuk duhet të bëhet vetëm. Mbase duhet ta bëjmë së bashku me shtetet e tjera. Zgjidhja janë programet me kod burimorë të hapur. Duke ndërtuar së bashku sisteme të sigurta, të hapura dhe të lira, ne mund të anashkalojmë këtë përgjim dhe një shtet nuk duhet ta zgjidhë këtë problem vetëm. Duhet të zgjidhë vetëm një problem të vogël.

"Një shtet i vogël duhet të bëjë një dallgë të vogël dhe këto dallga të vogla së bashku krijojnë një baticë, batica do të ngrejë lart të gjitha anijet njëkohësisht, dhe batica duhet të ndërtohet me sisteme me burim të hapur të sigurt dhe pa pagesë, ne do të bëhemi batica që do na ngrejë të gjithëve lart dhe më lart mbi përgjimin shtetëror." - Haroon Meer

6.2 Siguria dhe Privatësia juaj personale

Në qoftë se ju jeni shënjestër nga një agjenci e fuqishme e inteligjencës si NSA, është shumë, shumë e vështirë për të mbrojtur veten. Por, me disa hapa të vegjël, ju mund të bëni atë lloj të përgjimit shumë më të vështirë dhe të shtrenjtë kundër jush individualisht dhe në përgjithësi kundër të gjithëve. Më poshtë janë dhënë disa hapa që ju mund të ndërmerrni për të bërë pajisjet tuaja dhe komunikimin tuaj më të sigurt. Kjo nuk është një listë e plotë dhe nuk do të bëjë që ju plotësisht të siguroheni, por çdo hap që ndërmerrni do të ju bëjë më të sigurt se mesatarja.

6.2.1 Përdorni enkriptim end-to-end

Shoku juaj më i mirë për këtë janë sistemet me kod burimor të hapur. Ndaloni përdorimin e Viber, Whatsapp, Skype e disa aplikacione për komunikim që janë të pasigurta.

Figura 3: Softuerë për komunikim që nuk kanë end-to-end enkriptim.

Në vend të këtyre aplikacioneve ju mund të përdorni alternativat si ChatSecure, Signal, Silent Phone, Text Secure, Pidgin me OTR etj.

Figura 4: Softuerë për komunikim që kanë end-to-end enkriptim.

6.2.2 Përdorni enkriptim sa më shumë që të mundeni në komunikime

Edhe nëse nuk mund të përdorni enkriptim end-to-end, ju përsëri mund të enkriptoni shumicën e trafikut tuaj duke përdorur protokolle si HTTPS. P.sh mund të instaloni një add-on të quajtur HTTPS Everywhere në shfletuesin tuaj të internetit Firefox ose Chrome.

Përdorni VPN kur jeni në një rrjetë që nuk i besoni, p.sh brenda një kafeneje. VPN shërbime të mira dhe sigurta konsiderohen AirVPN, HideMe, Proxy.sh, IVPN etj.

6.2.3 Enkriptoni diskun tuaj të shënimeve dhe mbani fjalëkalime të sigurta

Tani shumë nga sistemet operative mundësojnë enkriptimin e diskut të shënimeve pa pasur nevojë të përdorni softuerë të tjerë. Këtë mund ta bëni duke përdorur vegla si VeraCrypt, GNU Privacy Guard, PeaZip etj.

Përdorni fjalëkalime të gjata që të jetë e vështirë për krekerët që të gjejnë fjalëkalimin tuaj. Përdorni karaktere të ndryshme dhe nëse ruani fjalëkalimet tuaja në kompjuter, atëherë më mirë përdorni një menaxhues të fjalëkalimeve si KeePass, Master Password, Encryptr etj.

6.2.4 Ndërroni shfletuesin e internetit

Përdorni shfletuesit të internetit me kod burimor të hapur si Mozilla Firefox apo edhe Tor - një program me kod burimor të hapur që mbron anonimitetin tuaj online duke bërë shuffle të dhënat tuaja nëpërmjet një rrjeti global të serverëve. Përdorni shtojca që ndihmojnë privatësinë në internet si dhe sigurohuni që shfletuesi juaj është sa më unik. Nga shtojcat më të mira për ruajtjen e privatësisë tuaj online janë: Disconnect, uBlock Origin, Random Agent Spoofer, HTTPS Everywhere etj.

6.2.5 Mbani softuerët të përditësuar

Mbajtja e softuerëve të përditësuar ndihmon që siguria e tyre të jetë gjithmonë më e lartë, dhe shanset se ju mund të eksploatoheni nga gabimet e softuerëve të vjetër janë shumë më të vogla.

6.2.7 Përdorni two-factor authentification

Google dhe Gmail e kanë atë; Twitter e ka atë; Dropbox e ka atë. Two-step authentication mundëson që përveç fjalëkalimit të shkruani po ashtu edhe një shifër tjetër që ndryshon rregullisht, me çrast kjo ju ndihmon ju që të mbroheni nga sulmet në ueb dhe cloud shërbime.

6.2.8 Rekomandime të tjera

- Mos përdorni Windows 10, Windows 10 është tmerr kur vije puna tek privatësia. Mikrosoft mbledh të dhënat tuaja përmes serviseve të lëshuara by default në sistemin tuaj operativ, përmes cortana, duke ju etiketuar me ID promovuese e duke i shpërndarë të dhënat tuaja me ose pa vetëdijen tuaj me softuere të tjera third-party.
- Përdorni ofrues të shërbimeve të email si GhostMail, OpenMailbox, ProtonMail ose klientë për e-mail si Thunderbird e Claws Mail.
- Në vend të makinave kërkuese si Bing, Google e Yhoo, përdorni makina kërkuese që kujdesen për privatësinë tuaj si DuckDuckGo e privatesearch.io
- Për shërbime cloud të sigurta, konsideroni përdorimin e OwnCloud e Seafile
- Në vend se të përdorni sisteme operative si Microsoft Windows, Mac OS X ju mund të përdorni sisteme operative të lira dhe me kod burimor të hapur si GNU/Linux , p.sh një nga distribucionet si Debian, Trisquel, Fedora etj.
- Në vend se të përdorni sisteme operative për telefon si Apple iOS, Windows phone e Android, konsideroni përdorimin e CyanogenMod, Firefox OS e Ubuntu Touch

REFERENCAT

[1] Lyon, David. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.

[2] EFF. Timeline of NSA Domestic Spying [https://www.eff.org/nsa-spying/timeline]

[3] Anne Broache (2014). FBI wants widespread monitoring of 'illegal' Internet activity, data e publikimit: 24.04.2014 [http://www.cnet.com/news/fbi-wants-widespread-monitoring-of-illegal-internet-activity/]

[4] Jay Stanley & Barry Steinhardt Bigger Monster (2003). Weaker Chains, data e publikimit: janar 2003 [https://www.aclu.org/sites/default/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf]

[5] Wsystems.com. Surveillance. Types of surveillance: cameras, telephones etc. [http://www.wsystems.com/news/surveillance-cameras-types.html]

[6] Nsa.gov1.info. Surveillance Techniques: How Your Data Becomes Our Data [https://nsa.gov1.info/surveillance/]

[7] Daniel J. Gallington (2013). The Case for Internet Surveillance, data e publikimit: 18.06.2013. [http://www.usnews.com/opinion/blogs/world-report/2013/09/18/internet-surveillance-is-a-necessary-part-of-national-security]

[8] Hangthebankers.com (2012). Is this the end of the internet? (SOPA, PIPA, ACTA and CISPA), data e publikimit: 22.04.2012. [http://www.hangthebankers.com/is-this-the-end-of-the-internet-sopa-pipa-acta-and-cispa/]

[9] Techadvisory.org (2012). What are SOPA, PIPA CISPA and ACTA?, data e publikimit 07.08.2012.

[http://www.techadvisory.org/2012/08/what-are-sopa-pipa-cispa-and-acta/]

[10] EFF. SOPA/PIPA: Internet Blacklist Legislation [https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill]

[11] BBC (2012). Sopa and Pipa anti-piracy bills controversy explained, data e publikimit 08.03.2012 [http://www.bbc.com/news/technology-16596577]

[12] Charles Arthur (2013). NSA scandal: what data is being monitored and how does it work?, data e publikimit: 07.05.2013. [http://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions]

[13] Dan Seifert (2013). Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data, data e publikimit: 06.05.2013 [http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism]

[14] Dustin Voltz (2015). Global Internet surveillance, censorship on rise: report, data e publikimit: 28.10.2015. [http://www.reuters.com/article/us-cybersecurity-report-idUSKCN0SM1M220151028]

[15] Arianit Dobroshi (2014). Kosovo's experience with data retention: A case of adopting negative EU standards, data e publikimit: 2014. [http://www.giswatch.org/en/country-report/communications-surveillance/Kosovo]

[16] Privacy Tools. [https://www.privacytools.io/]

[17] EFF. Secure Messaging Scoreread [https://www.eff.org/secure-messaging-scorecard]

[18] EFF. Panoptiplick [https://panopticlick.eff.org/tracker]

[19] Daniel J. Solove (2011). Nothing to Hide: The False Tradeoff Between Privacy and Security, data e publikimi: 31.05.2011

[20] Ben Schouten (2008). Biometrics and Identity Management, data e publikimit: 18.11.2008