Tallinna Ülikool

Digitehnoloogiate instituut

Privaatsus internetis

Seminaritöö

Autor: Risto Ruuben

Juhendaja: Edmund Laugasson

Autor: ..... ,, ... ,, 2015

Juhendaja:..... ,, ... ,, 2015

Instituudi direktor:..... ,, ... ,, 2015

Tallinn 2015

Sisukord

Sissejuhatus 3

1. Internetis surfamine 4

1.1. Interneti teenusepakkuja 4

1.2. Privaatsus veebis 5

1.2.1 Seadme sõrmejälg 7

1.2.2 Küpsised 8

1.2.3 Flash küpsised 9

1.2.4 Otsingumootori kasutamine 10

1.3. Asukoha jälgimine 11

1.4. Mobiilsed rakendused 12

2. Info ning andmete vahetamise teenused 13

2.1 Pilveteenused 13

2.2 Sotsiaalvõrgustik 15

2.3 Kiirsõnumid 16

2.4 Elektronpost 17

Kokkuvõte 18

Kasutatud kirjandus 19

Sissejuhatus

Internetprivaatsus on privaatsuse ja turvalisuse tase isikuandmete kohta, mida on avaldatud Interneti kaudu. See on lai mõiste, mis viitab erinevatele teguritele, et milliseid tehnikaid ja tehnoloogiaid kasutatakse, et kaitsta tundlikke ning privaatseid andmeid.

Privaatsus internetis tagab selle, et ilma kasutaja loata ei pääseks keegi ligi isikuandmete nagu näiteks veebiajalugu, paroolid, otsitud terminid, elektronpostile ning muudele andmetele, mis võivad rikkuda kasutaja privaatsust.

Internetiprivaatsus ja anonüümsus on aina olulisem kasutajale tänu eriti kiirele interneti kasutuse kasvule. Aina rohkem viiakse igapäevaseid toimetusi täide üle interneti, näiteks nagu panganduse ja internetipoodidega seotud teenused ning vanad meetodid unustatakse.

Nende mugavustega on kaasnenud ka miinused. Nimelt on inimesi võimalik palju kergemini jälgida kui kunagi varem. Suured reklaamifirmad ning ettevõtted on leidnud, et jälgides inimeste interneti kasutamist on lihtne leida kasutaja hobid ja huvid ning selle põhjal teha igale interneti kasutajale oma isiklik profiil, mille põhjal kasutajale personaalseid reklaame tehakse.

Seminari töö eesmärk on uurida millist infot on võimalik internetis olles kasutaja kohta saada ning leida võimalike lahendusi, kuidas kasutaja oma privaatsust internetis kaitsta saaks.

1. Internetis surfamine

1.1. Interneti teenusepakkuja

Internetile ligipääsemiseks kasutatakse interneti teenusepakkujat (ISP), kes kasutajale internetti pakub, seda kas mobiiltelefonile, kodu-, süle- või tahvelarvutile.

Kõik arvutid, mis on internetiga ühendatud, omavad unikaalset interneti protokolli aadressi ehk IP aadressi. See on number, mis võimaldab tuvastada võrgus oleva seadme. Olenevalt kasutaja teenuse tüübist, võib IP aadress olla dünaamiline, mis tähendab, et see on pidevalt muutuv ning kehtib niikaua, kuni ruuteris on määratud liisinguaeg. Teine variant on staatiline ehk andmesideühendus luuakse alati ühendudes ühe ja sama IP-aadressiga. (Whatismyipaddress, kuupäev puudub)

Kasutaja IP aadress iseenesest ei anna isikut tuvastavat informatsiooni, kuid kuna internetiteenuse pakkuja on teadlik kasutaja IP aadressist, siis on see võimalik nõrkus privaatsuse kaitsmise juures. Internetiteenuse pakkujatel on erinevaid eeskirju, mis määravad kui kaua nad IP aadresse andmebaasides hoiavad ning kahjuks paljud internetiteenuse pakkujad seda ei avalikusta, mis teeb usaldusväärse internetiteenuse pakkuja otsimise suhteliselt keerukaks. (Craig Desson, 2015)

Samuti levivad internetis kuuldused, et mõned teenusepakkujad nuhivad oma kasutajate järele, käies läbi kõik andmepaketid, mida kasutajale saadetakse või kasutaja saadab. Peamiselt tehakse seda valitsuste või suurte korporatsioonide palvel. (Alex Wawro, kuupäev puudub)

Lisaks internetiteenuse pakkujatele näeb külastatav veebileht kasutaja IP aadressi, mis võib veebilehele väljastada kasutaja umbkaudse asukoha, mille täpsus oleneb internetiteenuse pakkujast. (Lincoln Spector, 2014)

1.2. Privaatsus veebis

Liikudes internetis veebilehelt veebilehele kasutatakse erinevaid keerukaid meetmeid, mis võivad kasutaja asukoha välja uurida ning kasutaja nimepidi tuvastada. Enamik tuntumad veebilehitsejad annavad kasutajale teatud määrani kontrolli selle üle, kui palju informatsiooni avaldatakse ning säilitatakse. Näiteks saab muuta seadeid, mis blokeerivad küpsiseid.

Enamus tuntuimad veebilehitsejad pakuvad "Privaatne Surfamine" tööriista, et suurendada privaatsust. Kuigi uurijad on leidnud, et tööriistal ei õnnestu täielikult kogu veebi aktiivsust hävitada, kuna paljude populaarsete brauserite laiendused ja pluginad kahjustavad "Privaatne Surfamine" tööriista turvalisust ning kuigi selle kasutamisel kasutaja ajalugu ei salvestata, on ikkagi võimalik kasutaja IP aadressi jälgida. (Sylvan Lane, 2014)

"Ära jälgi" (DNT) on seade, mis on olemas enamus tuntumates brauserites. Seade ütleb veebilehtedele, et ei soovi asukohta uurimist. DNT töötamiseks on vajalik, et leheküljed, kus te olete, peavad austama teie jälitamise vastast soovi, kuna selle jälgimine pole kohustuslik. Kuigi mõned suuremad firmad on lubanud DNT'd austada, on ka palju neid kes selle jälgimisest keelduvad, kuna see kahjustab reklaamidest sisse tulevat kasumit. (Universal Web Tracking Opt Out, kuupäev puudub)

Teenused nagu Tor aitavad kasutajal anonüümselt internetis ringi liikuda. Tegu on tugevalt muudetud Firefoxi veebilehitsejaga, mille käigus on see tehtud palju turvalisemaks ning ka privaatsemaks, kui Firefox esialgselt on. Kõik liiklus käib selles veebilehitsejas läbi Tori serverite, mis on omakorda krüpteeritud. (Tor, kuupäev puudub)

Tänu sellele, et Tor seadistab peaaegu kõik seaded kasutaja eest ise ära, on selle kasutamine väga lihtne ja turvaline. Silmas tuleb pidada, et alati tuleb olla uuenduste osas viimase versiooni juures, kuna vanemates versioonides võivad olla turvaaugud, mida saadakse ära kasutada.

Suure privaatsuse tagamisel kaasneb Toriga ka suur miinus, millega tuleb kindlasti arvestada. Nimelt on Tor palju aeglasem harjumuspärasest. See tähendab, et seda ei ole mõistlik kasutada näiteks videote vaatamiseks ja kuna skriptid on blokeeritud, siis võivad vastavaid komponente vajavad veebilehed kasutamatud olla ning seega vajab kasutaja ümberharjumisaega. (Ronald Liive, 2014)

Selleks, et kiiremaid kiirusi nautida ning samas hoida ka privaatsuse element alles, on olemas virtuaalne privaatne võrk ehk VPN. Selle eeliseks on kiiremad kiirused, kuid kiirus siiski oleneb teenusepakkujast ning üldjuhul kiired kiirused maksvad. Lisaks saab VPN'i abil mitte ainult oma brauseris olevat infot kaitsta vaid absoluutselt kõiki kasutaja tegevusi võrgus.

VPN teenuse pakkuja valimisel tuleks uurida, kas teenusepakkuja on usaldusväärne, kuna on olnud juhtumeid, kus VPN teenuse pakkujad on oma klientide tegevused üles andnud, seega tasub arvestada et VPN ei pruugi olla sama turvaline kui Tor. (Alan Henry, 2012)

Võimaluse korral tasub kasutada krüpteeritud ühendusi igal pool, kus võimalik. Näiteks HTTPS, mis krüpteerib veebiühenduse olemasoleval lehel ära, tagades suurema privaatsuse ja turvalisuse, kui seda on krüptimata veebiühendusel nagu HTTP. See vähendab ohu võimalust, et mõni kolmas osapool kasutaja teavet kopeerib ja kasutab ilma loata. Seega tasub alati veenduda, et tegu on HTTPS ühendusega, kui tundlike andmeid on vaja kasutada või lihtsamal juhul interneti poes makstes. (HTG Explains, kuupäev puudub)

1.2.1 Seadme sõrmejälg

Seadme sõrmejälg on info, mis on kogutud seadmest endast. Igal seadmel on erinev tarkvara, kell, fondid ning teised omasused on igale seadmele omamoodi unikaalsed. Ühenduse loomisel edastab seade need andmed, mida on võimalik koguda ning omavalt liita. Selle tulemusel saame unikaalse sõrmejälje seadmele, millele saadakse määrata kindel number selle tuvastamiseks. (Ben Richmond, 2013)

Seadme sõrmejälje loomine on küpsiseid kiiresti asendamas. Suured firmad võtavad seda aina enam kasutusele tänu selle blokeerimise raskuse tõttu võrreldes küpsistega. Küpsised on kaitsetud kustutamise ning aegumise vastu ja muutuvad kasutuks, kui kasutaja otsustab uut brauserit kasutada. Mõned brauserid blokeerivad kolmanda osapoole küpsiseid automaatselt, ning samuti brauserite laiendused võimaldavad nende kustutamist ning blokeerimist. (Ben Richmond, 2013)

Erinevalt küpsistest, ei jäta seadme sõrmejälg kasutaja seadmetesse ühtegi jälge ning seetõttu on võimatu teada, millal tegevusi jälgitakse. Sellele on siiski olemas mõned võimalused privaatsuse säilitamiseks. Näiteks saab oma ainulaadsust kontrollida. Ühte sellist teenust pakub Panopticlick, mis annab unikaalsuse tulemuse, võimaldades kasutajatel näha, kui kergesti äratuntavad on kasutajad veebis. (Panopticlick, kuupäev puudub)

Kahjuks on sõrmejälje loomised peaaegu nähtamatud ning peaaegu püsivad. Pole ühtegi lihtsat viisi, kuidas neid kustutada. Kasutajad, kes on kindlameelsed sõrmejälje vältimise osas, võivad kasutada Tor-i või keelata Javascripti käivitumist oma arvutis, kuid see võib muuta mõned lehed kasutuskõlblikuks, jättes tähtsaid elemente laadimata. (Jennifer Valentino-Devries, 2010)

JavaScripti blokeerimiseks võib kasutada brauseri laiendust nimega NoScript, mis võib peatada JavaScripti töötamise veebilehtedel. (NoScript, kuupäev puudub)

1.2.2 Küpsised

Külastades erinevaid veebilehti, salvestavad veebilehed samuti infot külastuse kohta kõvakettale. Seda infot nimetatakse küpsisteks. Küpsised on andmeosad, mis on saadetud veebi serveri poolt kasutaja veebilehitsejale. Need sisaldavad kasutajate eelnevaid valikuid ja eelistusi. Minnes tagasi eelnevalt külastatud veebilehele, saadetakse see info veebiserverile. Veebiserver võib seda infot kasutada veebilehe kohandamiseks, et kasutajale lehekülje kasutamine mugavamaks teha. Lisaks kasutatakse neid külastatud veebilehtede jälgimiseks. (Aboutcookies, kuupäev puudub)

Korralikud veebilehed kasutavad küpsiseid naasvatele kasutajatele erinevate pakkumiste tegemiseks ning reklaamide tulemuste jälgimiseks, selliseid küpsiseid nimetatakse esimese osapoole küpsisteks. (Aboutcookies, kuupäev puudub)

On olemas ka küpsiseid mida nimetatakse kolmanda osapoole küpsisteks, mis jagavad kasutaja andmeid reklaamifirmadele. Selliste küpsiste alla kuuluvad ka jälitusküpsised, mis kasutavad kasutaja veebi surfamisajalugu sobivate reklaamide edastamiseks. (Aboutcookies, kuupäev puudub)

Tavaliselt suudavad brauserid ning kõrvalised tarkvarad avastada ja kustutada küpsised. Disconnect on üks programm, mis takistab tuntud kolmandatel osapooltel veebi aktiivsuse jälgimist. Iga kord kui veebilehte külastatakse, tuvastab Disconnect automaatselt seda kui veebilehitseja proovib saada ühendust muude allikatega peale veebilehe enda. (Disconnect, kuupäev puudub)

Ghostery on samuti tuntumate veebilehitsejate laiend, mis otsib üles küpsised ja teatab teile firmade kohta, mille kood veebilehel ilmub. “Ghostery” laseb kasutajal selliste firmade kohta rohkem õppida, ning nende jälitusküpsiseid blokeerida. (Ghostery, kuupäev puudub)

Veel saab kasutaja loobuda küpsiste info jagamisest Network Advertising Initiative liikmetega. Selleks tuleb minna nende lehele ning avaldada selleks soovi. (Networkadvertising, kuupäev puudub)

1.2.3 Flash küpsised

Paljud leheküljed kasutavad sellist küpsise tüüpi nagu Flash küpsised, mis on palju vastupidavamad kui tavalised küpsised, kuna tavalised meetodid nende eemaldamiseks ei tööta. Isiklike andmete, ajaloo ning vahemälu tühiendamine ei mõjuta selliseid küpsiseid. Selle tulemusena on nendest lahtisaamine palju keerukam, neid ei saa kustutada mitte ühegi kättesaadava viirustõrje programmiga (Aboutcookies, kuupäev puudub)

Siiski on olemas Firefox brauseris laiend nimega BetterPrivacy ning Adobe lehel olev rakendus, mis aitavad kaasa Flash küpsiste kustutamisele. (Macromedia, kuupäev puudub ja IKRG, 2012)

1.2.4 Otsingumootori kasutamine

Otsingumootoritel on võimalus jälgida kõiki kasutaja tehtuid otsinguid. Need võivad salvestada kasutaja otsitud termineid, IP aadressi, aega ning muud informatsiooni. Näiteks on suur võimalus avaldada kasutaja kohta tohutul hulgal informatsiooni otsingute käigus. (Vijay Prabhu, 2015)

Suured otsingumootorid on väitnud, et nad säilitavad isikute isikliku informatsiooni parema teenuse pakkumiseks ning samuti säilitavad sellised andmeid üle aasta, mis on palju pikem ajaühik kui tegelikult vajalik. Seega tasub olla otsingumootorite valikul ettevaatlik. (Vijay Prabhu, 2015)

DuckDuckGo on üks otsingumootoritest, mis väidab, et ei salvesta ega jaga isikliku informatsiooni ja ei kasuta küpsiseid ning IP aadressi, et kasutajat tuvastada. Seega pole DuckDuckGo otsingumootoril aimu, kas isegi samast arvutist tulnud otsingud on omavahel kuidagi seotud. (Chris Hoffman, 2012)

Samuti on olemas Startpage otsingumootor, mis on asutatud Hollandis. Selle privaatsuse eeskirjad olid loodud vastulöögiks firmade poolt informatsiooni pahatahtliku kasutamise vastu. Firma tuli järeldusele, et kui kasutajate informatsiooni ei salvestata, pole võimalust privaatsuse rikkumiseks, seega kasutab Startpage otsingu tulemuseks Google otsingumootorit, kuid enne tulemuse otsimist eemaldab kõik tuvastava informatsiooni kasutaja päringutest. Ixquick on veel üks otsingumootor, mis töötab samal põhimõttel nagu Startpage, aga erinevuseks on see, et otsingu tulemused ei ole ainult Google'lt saadud. (Chris Hoffman, 2012)

1.3. Asukoha jälgimine

Iga veebileht või rakendus võib määrata kasutaja arvuti või seadme ligikaudse asukoha, kasutades mitmeid tehnoloogiaid. Näiteks interneti kasutades saab IP-aadressi põhjal leida ligikaudse asukoha. IP-aadressi põhjal saab tavaliselt teada linnaosa, kuid on võimalik leida ka täpsem asukoht.

Selleks, et varjata oma IP-aadressi, on olemas mitmeid erinevaid meetmeid. Üks populaarsemaid ja lihtsamaid lahendusi on kasutada teenust nimega Tor, mis peidab kasutaja IP-aadressi ära. Teine lahendus on kasutada Virtuaalset privaatset võrgustiku ehk VPN teenust, mis asendab kasutaja IP-aadressi mõne enda omaga. (Tor, kuupäev puudub ja Ronald Liive, 2014)

Kui interneti ligipääsuks kasutakse traadita ühendust ehk Wi-Fi, siis on kasutajat võimalik leida läbi Wi-Fi triangulatsiooni, uurides lähedal olevaid Wi-Fi võrke. Samamoodi saab kasutaja tuvastada ka üleilmse asukoha määramise süsteemi kaudu ehk läbi GPS-i. Viimane meetod, millega kasutaja asukohta saab jälgida, on läbi mobiilse võrgu mastide. (David Chartier, 2008)

Kasutaja asukoha infot võidakse kasutada kasulikul otstarbel, näiteks näidates telefonis hetkel oleva linna ilmaennustust. Samas võib see osutuda suureks privaatsuse riskiks, kui kasutaja asukohainfot hoopis andmebaasi kogutakse ja teiste allikatega liidetakse. Selle põhjal saab välja selgitada kasutaja liikumisharjumused, kus ollakse enamus ajast või mis marsruuti kasutakse koju või tööle sõitmiseks. Selle info põhjal on võimalik ennustada, kus kasutaja praegu on, isegi siis, kui teda hetkel jälgida pole võimalik. (Matt, 2014)

1.4. Mobiilsed rakendused

Tänapäeval on mobiilseadmetesse võimalik tõmmata kümneid tuhandeid mobiilseid rakendusi. Mida paljud aga ei mõtle on see, et need rakendused on võimelised koguma väga palju infot kasutaja kohta ja edastama seda kolmandatele osapooltele ning rakenduse tegijale, mida kasutatakse, kas oma otstarbeks või edasimüügiks.

Mobiilirakendused üldiselt ei anna reklaami edasimüüjatele võimalust kasutajat jälgida läbi küpsiste, kuid selle asemel võivad reklaami edasimüüjad kasutada unikaalset identifikaatorit, mis aitab seadet tuvastada. Et sellest mõõda saada tuleb reklaami edasimüüjale anda oma unikaalne identifikaator, et nad seda enam ei jälgiks. (Samuel Gibbs. 2014)

Kui kasutaja rakenduse enda telefoni paigaldab, annab see rakendusele õiguse teadud informatsioonile kasutaja telefonis ning samuti ei ole kuskil kirjas, milleks neil seda vaja on ning, mis infot kogutakse. Asja teeb veel hullemaks see, et paljudel rakendustel pole privaatsuspoliitikat ollagi. Info, mida on telefonist võimalik kätte saada läbi rakenduse, on kõnelogi, kontaktid, interneti andmed, seadme id, telefoni asukoht, kalendris olev info ning ka kasutusinfo rakenduse enda kasutamise osas. (Lucian Constantin, 2014)

Tavaliselt enne rakenduse installeerimist võib seade küsida konkreetseid õigusi rakenduse suhtes. Etteantud õigused tasub alati läbi lugeda ning mõelda, kas ja miks see rakendus seda õigust tahab. Näiteks kui leiad, et taskulambi rakendus tahab saada sinu kontakte ja asukohta, siis ei tasu seda telefoni installeerida, kuna taskulambil pole töötamiseks kontakte ja asukohta vaja. Kui aga leiad, et kohe kindlalt on seda rakendust vaja, aga selle õigused on kahtlased, siis tasub uurida selle rakenduse kohta, või rakenduse arendaja enda käest selgitusi küsida. (Lucian Constantin, 2014)

2. Info ning andmete vahetamise teenused

2.1 Pilveteenused

Pilveteenused annavad kasutajale mugava viisi failide jagamiseks erinevate seadmete vahel nii, et näiteks kui koduarvutis tehtud dokument salvestada pilve, saab sama faili jätkata sülearvutis kodust eemal ilma, et peaks kasutama andmekandjat. Samuti pakuvad need kindlat kohta andmete hoidmiseks juhul kui midagi peaks juhtuma kasutaja andmekandjaga.

Kuna internet on tänapäeval väga kiireks ja kättesaadavaks muutunud, on samuti liikunud ka paljud teenused pilve, võimaldades jooksutada oma teenuseid läbi pilve võimsate arvutite, et kulusid kokku hoida.

Kuigi mugavus pilve teenuste kasutamisel on suur, on sellel siiski riskid privaatsuse osas. Kuna kasutaja hoiustab oma isiklike faile kellegi teise riistvara peal, kaotab sellega mingil määral kontrolli andmete üle ning tekkib küsimus, kes tegelikult neid andmeid omab. Vastutus kaitsta kasutaja andmeid teiste eest nagu näiteks küberkurjategijate eest langeb teenuse pakkujale ning mitte kasutajale endale. (Vic (J.R.) Winkler, 2013)

Et kindlaks teha, mida teenuse pakkuja saab, või ei saa kasutaja andmetega teha, tuleb alati lugeda läbi privaatsuspoliitika ja kasutustingimused. Samuti tuleb arvestada sellega, et privaatsuspoliitika ja kasutustingimused muutuvad aja möödudes, ning muutused võivad sisse tulla ilma kasutaja teadmata, kuna tavaliselt lisatakse tingimustesse juurde punkt, kus kasutaja nõustub automaatselt kõigi muudatustega teatud aja möödudes. (Vic (J.R.) Winkler, 2013)

Lisaks mängib veel pilveteenuste osas rolli teenusepakkuja asukoht, kuna igas riigis on omad seadused, mida nad jälgima peavad. Valitsus või uurijad võivad kahtluse korral taotleda politseilt luba kasutaja tegevuste uurimiseks, ning pilve teenuse pakkujal ei pruugi olla motivatsiooni kasutaja andmete kaitsmise vastu, kuna hirm valitsuse ees on suurem, kui maine rikkumine. (Vic (J.R.) Winkler, 2013)

Kui on soov kasutada pilveteenuse mugavusi, on mõistlik kasutajal võimaluse korral installeerida isiklik pilveserver. Isikliku serveri puhul on võimalik teha kindlaks, kellel on reaalne ligipääs pilveteenusele, kuid selle privaatsuse tagamine on kulukam, kuna kasutajal on vaja muretseda vastav riistvara serveri jooksutamiseks ning ülevalpidamiseks. Veel üks võimalus on enne andmete pilve laadimist need ära krüpteerida, et isegi siis kui keegi peaks andmetele ligi saama, poleks neil sellega midagi peale hakata.

2.2 Sotsiaalvõrgustik

Sotsiaalvõrgustikud võimaldavad kasutajatel luua seoseid ja suhteid teiste internetikasutajatega ning on hetkel üks populaarsemaid viise, kuidas end kursis hoida sõpradega ning leida inimesi, kellel on sarnased huvid ja ideed.

Kasutajate poolt postitatud info ärakasutamine on sotsiaalvõrgustikus suur. See on tingitud kahest asjaolust: kasutajad ei tunne sageli huvi privaatsusseadete vastu vastavas keskkonnas ning samuti kiputakse mõtlematult avaldama isiklikke andmeid sotsiaalvõrgus. Näiteks kasutaja postitatud pilt või pildi kommentaar, mis oli mõeldud ainult sõpradele võib nähtav olla nendele, kellele see mõeldud pole. Teada on et paljud inimesed peale sõprade ja tuttavate kasutavad sotsiaalvõrgustikku, et leida infot vastava kasutaja kohta.

Samuti on sellest infost huvitatud ka vargad, petturid, jälitajad, ettevõtted ja riigiasutused. Näiteks võib sotsiaalvõrgustikust saadud info põhjal uuritava kasutaja identiteedi varastada ning tema nimel oste teha. Lisaks kasutavad ettevõtted sotsiaalvõrgustikus saadud infot, et oma toodet arendada kasutajale kohasemaks. (Privacyrights, 2015)

Paljud inimesed lisaks sõpradele ja tuttavatele on huvitatud infost, mida inimesed postitavad sotsiaalvõrgustikesse. Identiteetivargad, petturid, võlakollektsionäärid, varitsejad, ja ettevõtted kasutavad sotsiaalvõrgustikke, et koguda teavet kasutajate kohta. Ettevõtted, mis tegutsevad sotsiaalvõrgustikes, koguvad ka andmeid kasutajate kohta, et personaliseerida teenuseid kasutajate ja müüa neid edasi reklaamiandjatele. (Privacyrights, 2015)

Õnneks infot, mida kasutajatelt saadakse on võimalik piirata, muutes privaatsuse seadeid oma sotsiaalvõrgustikus kõrgeimale tasandile. Kuid kõige lihtsam viis info piiramiseks on teenust kas mitte kasutada või piirata ise infot, mida sotsiaalvõrgustikus jagad (Privacyrights, 2015). Lisaks on võimalus võtta kasutusele ka sotsiaalvõrgustikke, mis austavad kasutaja privaatsust nagu näiteks Seen , Diaspora ning Minds. (Seen, kuupäev puudub, Minds, kuupäev puudub ja Diaspora, kuupäev puudub)

2.3 Kiirsõnumid

Kiirsõnumite vestlused on tavaliselt mitteametlikud, mistõttu suheldakse üsna vabalt, kuid millele tavaliselt ei mõelda on see, et vestlused salvestatakse tavaliselt kasutaja enda arvutisse, või isegi välisesse andmebaasi. Tavaliselt tehakse seda selleks, et kasutajal oleks mugav vaadata vestluste ajalugu, kuid seda infot võidakse ka sinu vastu kasutada.

Lisaks on kiirsõnumid sihtmärk rämpssõnumite saatmiseks, mille abil võidetakse kiirelt raha teenida. Tavaliselt lisatakse tekstile kaasa ka veebilehekülg kuhu ei tohiks kunagi minna, kuna suure tõenäosusega sisaldab see leht pahavara, mis kasutaja arvutisse installeeritakse ja mis seejärel kasutaja kohta kas infot kogub või reklaamib kasutajale mittesoovivaid tooteid. Peale nende sõnumite eiramise, on neid veel võimalik vältida muutes oma privaatsusseadmeid selliseks, et ainult kindlad isikud saavad sõnumeid kasutajale saata. (Andrew Brandt, kuupäev puudub)

Samuti nagu elektronpostide puhul, sõnumi kustutamine ei tähenda selle reaalset kustutamist, kuna suurem osa kiirsõnumite teenusepakkujad arhiveerivad sõnumid. Õnneks pakuvad mõned kiirsõnumite teenusepakkujad selle funktsiooni välja lülitamist, kuid kahjuks on enamustel, kes seda võimalust pakuvad see funktsioon vaikimisi sees. (Lucian Constantin, 2012)

Valides kiirsõnumite teenuse, tasub kindlaks teha, et valitud teenus pakuks krüpteerimist. Sellega väldib ootamatuid pealtvaatamisi kolmandate osapoolte poolt, kes muidu kirjutatud sõnumeid näeksid teksti kujul. Hea lehekülg, kust saab võrrelda erinevaid teenuseid on https://www.eff.org/secure-messaging-scorecard, kus on selgelt välja toodud populaarsemad teenused ning nende tugevused ja nõrkused. (Josh Robert Nay, 2013)

2.4 Elektronpost

Kui kasutaja kellegi elektronkirjale vastab või saadab kellelegi elektronkiri, saab elektronkirja saaja kasutaja kohta mingil määral infot. Samuti võib kasutaja informatsiooni anda ka teistele isikutele olgu sellest kas elektronposti teenusepakkuja või valitsus. (Nolo, kuupäev puudub)

Krüpteerimata elektronkiri võib teoreetiliselt nähtav olla suvalistele isikutele seni, kuni see teel on. Samuti saab tööandja ligi kasutaja kirjadele, kui see on tööandja seadmega saadetud või saadetud läbi töö elektronposti aadressi. (Nolo, kuupäev puudub)

Lisaks on enamus elektronposti teenusepakkujatel õigus kasutaja elektronkirjad läbi skaneerida. Seda tehakse tavaliselt selleks, et leida rämpsposti või pakkuda reklaami sisu (Samuel Gibbs, 2014). Et elektronposti kasutaminevõimalikult turvaliseks muuta, tasub kasutada turvalise elektronposti teenusepakkujaid nagu näiteks Tutanota ning Protonmail, mis kasutavad krüpteerimise tehnikaid, kus krüpteerimise võti on kasutaja käes ning teenusepakkujal see võti puudub. Sellist metoodikat kasutavad teenused tunneb tavaliselt ära selle järgi, et nad ei paku parooli taastamise võimalusi, kuna neil puudub võti selle tagamiseks. (Douglas Crawford, 2015)

Kokkuvõte

Töö käigus leidis autor, et internetis kasutaja kohta infot saada on tänapäeval vägagi kerge. Peaaegu iga liigutus annab mingil määral kasutaja andmeid edasi. Isegi internetiga ühenduses olles on võimalik tuvastada kasutaja ligikaudne asukoht. Interneti kasutamisel on peaaegu võimatu jääda anonüümseks.

Siiski on olemas erinevaid lahendusi, kuidas andmete lekkimist piirata. Üheks võimaluseks on kasutada virtuaalset privaatselt võrku ehk VPN-i. Lisaks on olemas erinevaid programme, mis aitavad privaatsust hoida nagu Tor veebilehitseja ning enamustel populaarsetel veebilehitsejatel on olemas seaded, mis samuti aitavad info lekkimist vähendada. Lisaks on olemas ka veebilehitsejate laiendused nagu NoScript, Disconnect ning Ghostery, mis aitavad hoida ära infoleket.

Peale erinevate programmide kasutamist on kõige parem viis kuidas kasutaja privaatsust kaitsta kasutusharjumuste muutmine. Lugedes läbi kasutavate teenuste tingimused ning selle põhjal teha otsus selle kasutamiseks. Näiteks on Google otsingumootori asemel võimalik kasutada hoopis privaatsust austavaid otsingumootoreid või muutes kasutuses olevate teenuste privaatsuse sätteid.

Kasutatud kirjandus

1. Whatismyipaddress. (Kuupäev puudub). Dynamic IP vs Static IP. Loetud 02.10.2015 aadressil: http://whatismyipaddress.com/dynamic-static
2. Craig Desson. (2015). Are internet service providers keeping tabs on your browsing? Loetud 02.10.2015 aadressil: http://www.thestar.com/news/privacy-blog/2015/03/are-internet-service-providers-keeping-tabs-on-your-browsing-.html
3. Alex Wawro. (Kuupäev puudub). Will Your ISP Protect Your Privacy? Loetud 02.10.2015 aadressil: http://www.pcworld.com/article/241591/faq_will_your_isp_protect_your_privacy_.html
4. Lincoln Spector. (2014). Your IP address: Who can see it and what you can do about it. Loetud 02.10.2015 aadressil: http://www.pcworld.com/article/2105405/your-ip-address-who-can-see-it-and-what-you-can-do-about-it.html
5. Sylvan Lane. (2014). Private Browsing Settings Aren't as Private as You Think. Loetud 05.10.2015 aadressil: http://mashable.com/2014/07/21/how-private-browsing-works/#T2rND2r8kSqS
6. Donottrack. (Kuupäev puudub). Universal Web Tracking Opt Out. Loetud 05.10.2015 aadressil: http://donottrack.us/
7. Torproject. (Kuupäev puudub). Tor: Overview. Loetud 05.10.2015 aadressil: https://www.torproject.org/about/overview.html.en
8. Ronald Liive. (2014). Kuidas internetis võimalikult anonüümseks jääda? Loetud 05.10.2015 aadressil: http://kiip.ee/kuidas-internetis-voimalikult-anonuumseks-jaada/
9. Alan Henry. (2012). Why You Should Start Using a VPN (and How to Choose the Best One for Your Needs). Loetud 05.10.2015 aadressil:http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs
10. Chris Hoffman. (2014). HTG Explains: What is HTTPS and Why Should I Care?. Loetud 07.10.2015 aadressil: http://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/
11. David Chartier. (2008). Where GPS won’t do, Wi-Fi triangulation might Loetud 09.10.2015 aadressil: http://arstechnica.com/uncategorized/2008/01/where-gps-wont-do-Wi-Fi-triangulation-might/

12. Matt. (2014).Google’s Location History is Still Recording Your Every Move. Loetud 09.10.2015 aadressil: http://www.howtogeek.com/195647/googles-location-history-is-still-recording-your-every-move/
13. Aboutcookies (Kuupäev puudub). Cookies: Frequently Asked Questions. Loetud 09.10.2015 aadressil: http://www.aboutcookies.org/default.aspx?page=5
14. Disconnect. (Kuupäev puudub). Loetud 09.10.2015 aadressil: https://disconnect.me/
15. Ghostery. (Kuupäev puudub). Loetud 09.10.2015 aadressil: https://www.ghostery.com/
16. Networkadvertising. (Kuupäev puudub). Opt Out of Interest-Based Advertising. Loetud 09.10.2015 aadressil: http://www.networkadvertising.org/choices/
17. Macromedia. (Kuupäev puudub). Website Storage Settings panelLoetud 09.10.2015 aadressil: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html
18. IKRG. (2012). BetterPrivacy. Loetud 09.10.2015 aadressil: https://addons.mozilla.org/en-us/firefox/addon/betterprivacy/
19. Ben Richmond. (2013). How "Device Fingerprinting" Tracks You Without Cookies, Your Knowledge, or Consent. Loetud 15.10.2015 aadressil: http://motherboard.vice.com/blog/device-fingerprinting-can-track-you-without-cookies-your-knowledge-or-consent
20. Panopticlick. (Kuupäev puudub). Loetud 15.10.2015 aadressil: https://panopticlick.eff.org/
21. Jennifer Valentino-Devries. (2010). How To Prevent Device Fingerprinting. Loetud 15.10.2015 aadressil: http://blogs.wsj.com/digits/2010/11/30/how-to-prevent-device-fingerprinting/
22. NoScript. (Kuupäev puudub). Loetud 15.10.2015 aadressil: https://noscript.net/
23. Vic (J.R.) Winkler. (2013). Cloud Computing: Privacy, confidentiality and the cloud. Loetud 20.10.2015 aadressil: https://technet.microsoft.com/en-us/magazine/dn235775.aspx
24. Vijay Prabhu. (2015). Loetud 20.10.2015 aadressil: http://www.techworm.net/2015/10/worried-about-privacy-forget-google-and-try-these-search-engines.html
25. Chris Hoffman. (2012). Alternative Search Engines That Respect Your Privacy. Loetud 20.10.2015 aadressil: http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your-privacy/

26. Privacyrights. (2015). Social Networking Privacy: How to be Safe, Secure and Social. Loetud 22.10.2015 aadressil: https://www.privacyrights.org/social-networking-privacy
27. Andrew Brandt. (Kuupäev puudub). Privacy Watch: Cut Off Instant Messaging Spam. Loetud 22.10.2015 aadressil: http://www.pcworld.com/article/115602/article.html
28. Lucian Constantin . (2012). New AIM instant messaging client poses privacy risks, says EFF. Loetud 22.10.2015 aadressil: http://www.infoworld.com/article/2618285/internet-privacy/new-aim-instant-messaging-client-poses-privacy-risks--says-eff.html
29. Josh Robert Nay. (2013). Security Issues With Mobile Messaging Apps and Maintaining Safety and Privacy. Loetud 22.10.2015 aadressil: http://www.trutower.com/2013/08/05/mobile-messaging-app-security-flaws/
30. Nolo. (Kuupäev puudub). If you want privacy, don't count on email. Here's why. Loetud 22.10.2015 aadressil: http://www.nolo.com/legal-encyclopedia/email-privacy-29610.html
31. Samuel Gibbs. (2014). Gmail does scan all emails, new Google terms clarify. Loetud 22.10.2015 aadressil: http://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify
32. Samuel Gibbs. (2014). What Are Mobile Device Identifiers?. Loetud 22.10.2015 aadressil: https://www.aerserv.com/mobile-device-identifiers/
33. Lucian Constantin. (2014). Privacy lapses riddle majority of mobile apps, data protection authorities find. Loetud 22.10.2015 aadressil: http://www.pcworld.com/article/2682712/data-protection-authorities-find-privacy-lapses-in-majority-of-mobile-apps.html
34. Seen. (Kuupäev puudub). Loetud 29.10.2015 aadressil: https://www.seen.is/
35. Diaspora. (Kuupäev puudub). Loetud 29.10.2015 aadressil: https://diasporafoundation.org/
36. Minds. (Kuupäev puudub). Loetud 29.10.2015 aadressil: https://www.minds.com/
37. Douglas Crawford. (2015). Tutanota private email review (+ vs ProtonMail). Loetud 29.10.2015 aadressil: https://www.bestvpn.com/blog/16671/tutanota-private-email-review-vs-protonmail/