Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoverkot ja tietoturva

2018

Hemmo Roivas

YKSITYISYYDEN HINTA

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoverkot ja tietoturva

2018 | 33

Hemmo Roivas

YKSITYISYYDEN HINTA

Opinnäytetyön tavoitteena oli tutkia yksityisyyden roolia nykymaailmassa, missä sosiaalinen media on tullut jäädäkseen ja perinteisiä palveluja siirretään sähköiseen muotoon. Jo nyt suuret yritykset ovat ongelmissa käyttäjien yksityisyyden takaamiseksi. Siksi on erityisen tärkeää huolehtia itse omasta yksityisyydestä ja varmistaa ettei oman huolimattomuuden tai tietämättömyyden takia joudu esimerkiksi identiteettivarkauden uhriksi.

Tarkoitus oli selvittää, onko omaa yksityisyyttä mahdollista suojata, kun yksityisyydestä on tullut uusi kaupankäynnin väline. Väitteiden tutkimiseen on käytetty alan artikkeleita, lainsäädäntöä sekä ajankohtaisia uutisia osoittamaan ilmiön laajuus ja vakavuus. Opinnäytetyössä on käytetty kvalitatiivista tutkimusmenetelmää.

Lopputuloksena on tilannekatsaus yksityisyyden tilasta digitalisoituvassa nykymaailmassa. Työssä tarkastellaan missä asioissa pystyy omalla aktiivisuudella parantamaan tilannetta, ja missä asioissa täytyy hyväksyä, ettemme pysty vaikuttamaan asiaan. Esineiden internetin yleistyessä, yksityisyyden hinta tulee kasvamaan entisestään ja siihen liittyvä hyväksikäyttö tulee lisääntymään ilman ajan tasalla olevaa lainsäädäntöä. Varmaksi ei pysty sanomaan miten paljon suuret yritykset keräävät käyttäjistään tietoa, mutta käyttämällä salattuja yhteyksiä ja poistamalla turhia tunnuksia, voi omaa yksityisyyttä suojata mahdollisen tietomurron tai identiteettivarkauden sattuessa.

ASIASANAT:

tietoturva, tietosuoja, yksityisyys, sosiaalinen media, identiteettivarkaus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2018 | 33

Hemmo Roivas

PRICE OF PRIVACY

Aim of the thesis is to study the role of privacy in today's world. Social media is here to stay and more services are shifted into digital format. Even now big companies are struggling keeping their users safe. Therefore it is especially important to take care of your own privacy and makes sure one's identity, for example, or other information is not stolen due to careless actions.

The goal is to examine whether it is possible to control and protect one's privacy as it has become a tool of trade. Articles, legislation and hot topics were used to show the severity of the phenomenon. Qualitative research method is used in the thesis.

The final result is an overview of the state of privacy in more digitalizing world, what can one do to make the situation better and in which areas we need to accept there is nothing we can do. As Internet of Things gets bigger the price of privacy will increase because it will be more abused due to legislation lacking behind. We cannot tell for sure how vastly big companies are collecting data about their users but using secure connections and removing outdated accounts we can protect our own privacy in case of hacking or identity theft.

KEYWORDS:

Information security, data protection, privacy, social media, identity theft

SISÄLTÖ

LIITTEET

KUVAT

1 JOHDANTO

Internet on mahtava keksintö. Internetin tuoma sosiaalinen media on mahdollistanut uudenlaisen tavan kommunikoida ympäri maailmaa kenen tahansa kanssa koska tahansa. Se on nopeuttanut palveluiden saatavuutta: esimerkiksi laskut voi maksaa kirjautumalla omaan verkkopankkiin, ja useimmat viralliset hakemukset voi täyttää sähköisesti. Potilastiedot ovat jokaisen itse nähtävissä ja reseptit löytyvät omien tietojen takaa. Internet on tuonut palvelut kaikkien saataville ja mahdollistanut paljon uutta.

Internetin aikaan kuuluu vahvasti sosiaalinen media. Tapahtumat leviävät ympäri maailmaa minuuteissa sosiaalisen median ansiosta. Enää ei tarvitse odottaa seuraavan päivän sanomalehteä lukeakseen, mitä maailmalla tapahtuu. Sosiaalisessa mediassa oleva tieto on heti julkisesti kaikkien saatavilla, mutta siinä piilee myös asian suurin riski yksityisyyden näkökulmasta ajateltuna. Väärä painallus voi aiheuttaa sen, että yhdelle henkilölle tarkoitettu sisältö leviää kaikille. Väärään osoitteeseen lähetettyä sisältöä ja sitä, mitä sille tapahtuu, ei pysty hallitsemaan.

Tietoa, mikä näkyy julkisesti kaikille, pystyy rajoittamaan, mutta vain palvelutarjoajan hyväksymillä tavoilla omissa yksityisyysasetuksissa. Oman osoitteen tai puhelinnumeron voi asettaa yksityiseksi, mutta itsestään ei voi tehdä näkymätöntä. Niin kauan, kuin kukaan ei halua pahaa, on yksityisyys turvassa, mutta miten käy, jos pahaa haluava pystyy loukkaamaan tuota yksityisyyttä?

Opinnäytetyön tarkoituksena on selvittää sosiaalisen median ja internetin roolia nykymaailmassa, ja sitä, onko omaa yksityisyyttä mahdollista suojata vai onko se pelkkää toiveajattelua, kun kaikki palvelut siirtyvät sähköiseen muotoon ja uudet älylaitteet ovat jatkuvasti yhteydessä internetiin. Pitääkö meidän hyväksyä se tosiasia, että käyttämällä internetin mahdollistamia palveluita aina Googlesta Facebookiin, joudumme luopumaan omasta yksityisyydestämme? Voiko kukaan olettaa, että osa tiedosta on yksityistä, pysyy yksityisenä ja tulee aina olemaan yksityistä?

Työssä käydään läpi, mitkä elementit kuuluvat vahvasti yksityisyyteen ja mikä on sosiaalisen media merkitys arjessa. Tämän jälkeen työ keskittyy yksityisyyttä uhkaavien asioiden läpikäyntiin, keinoihin hallinnoida meistä saatavilla olevaa tietoa sekä tapoihin suojata itseämme. Lopussa luodaan katse nykytilanteeseen kerätyn tiedon perusteella sekä keinoihin parantaa yksityisyyttä tulevaisuudessa.

2 YKSITYISYYS JA YKSITYISYYDEN SUOJA

Yksityisyydestä puhutaan joka vuosi enemmän ja enemmän. Mitä enemmän tietoa on sähköisesti saatavilla, sitä suuremmaksi yksityisyyden merkitys kasvaa tulevaisuudessa. Yksityisyys ja lainsäädäntö ovat vahvasti sidoksissa toisiinsa, koska lainsäädännöllä määritetään mihin tietoon esimerkiksi viranomaisilla on pääsy. Tiedustelulait ja uudet tietosuoja-asetukset ovat ajankohtaisia ja niiden sisällöllä tulee olemaan, tai on jo nyt, merkittävä vaikutus jokaisen yksilön yksityisyyden suojaan tulevaisuudessa.

2.1 Yksityisyys

Yksityisyys terminä käsittää meidän henkilökohtaisen elämän, minkä haluamme pitää joko kokonaan tai osittain piilossa muilta. Kaikilla on oikeus yksityisyyteen. Suomen perustuslaki turvaa perusoikeutena jokaiselle kansalaiselle oikeuden yksityiselämään, kotirauhaan ja kunniaan (Suomen perustuslaki 731/1999).

Yksityisyydestä puhuttaessa keskeinen käsite on henkilötieto. Kaikki tieto, mistä yksittäinen henkilö on tunnistettavissa, kutsutaan henkilötiedoksi (Laki24 2018). Vuonna 2013 TED-konferenssissa puhunut Alessandro Acquisti esitti, miten ”kaikki henkilötieto voi olla arkaluontoista tietoa” (Acquisti 2013).

Viime vuosina median välityksellä on tullut varsin selväksi, miten suurvallat harrastavat laajaa vakoilua ja ovat kehittäneet valvontajärjestelmiä seuraamaan yksilöiden elämää ja internetin välityksellä tapahtuvaa viestintää. Jokaisella on oikeus yksityisyyteen ja tämä tiedon kerääminen riitelee yksityisyyden periaatetta vastaan. Kun tiedämme olevamme valvonnan alaisia, käytöksemme poikkeaa normaalista. Tämä puolestaan johtaa vapauden rajoittamiseen ja yksityisyydestä luopumiseen (Yksityisyydensuoja 2017). Suomessa on aloitteilla oma tiedustelulaki, mikä antaisi viranomaisille lisää valtaa verkkotiedustelua tehdessä. Tämä on herättänyt keskustelua, miten käy kansalaisten yksityisyyden, mikä on määritelty Suomen perustuslaissa. Esityksessä tiedostetaankin, miten ehdotus rajoittaisi yksittäiselle kansalaiselle turvattua yksityiselämän suojaa sekä luottamuksellisen viestin salaisuutta (Siviilitiedustelulaki 2018).

Sosiaalinen media aiheuttaa ongelmia ihmisten yksityisyydelle. Yksityisyyden käsitteestä on tullut häilyvä, koska käyttämällä sosiaalisen median palveluita, olemme itse

tuotteita. Meidän täytyy sokeasti luottaa palvelun tarjoamiin yksityisyyttä koskeviin asetuksiin, ja meistä saattaakin tuntua että hallitsemme tilanteen, vaikka todellisuudessa tilanne on toinen.

2.2 Tietosuoja

Siinä missä yksityisyys on itsestä lähtevää yleistä tiedon jakamisen rajoittamista, tietosuojaan ei pääse itse vaikuttamaan. Sillä tarkoitetaan ”henkilötietolain henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi.” (Yleistä tietosuojasta 2014.) Henkilötietoja ja henkilörekistereitä käsiteltäessä vastuu on rekisterinpitäjällä, jotta tietoja käsitellään ja suojataan oikein.

EU:n uusi tietosuoja-asetus, voimassa 25.5.2018 alkaen, takaa kansalaisille enemmän oikeuksia ja rekisterinpitäjille enemmän velvollisuuksia. Uusia oikeuksia on esimerkiksi omia henkilötietoja koskeva tiedonsaantioikeus, oikeus saada tiedot oikaistua, oikeus tulla unohdetuksi, oikeus tietojen poistamiseen ja tietojenkäsittelyn vastustamiseen ja ilmoitusvelvollisuus viranomaisille 72 tunnin kuluessa tietoturvaloukkauksen tapahtumisesta (Ylipartanen & Andreasson 2015). Käytännössä yrityksiltä vaaditaan entistä tarkempaa suhtautumista tietoturvaan ja esimerkiksi tietotilinpäätöksen tekemistä, minkä tarkoituksena on antaa kuva yrityksen tietojenkäsittelyn nykytilasta.

Jo tällä hetkellä kuka tahansa käyttäjä voi pyytää esimerkiksi Facebookilta yhteenvetoa omasta profiilista siitä, mitä tietoa heillä on kerättynä. Google on myös tarjonnut mahdollisuutta tulla unohdetuksi jo vuodesta 2014 (Junttila 2014). Uuden tietosuoja-asetuksen suurin vahvuus on yhtenäiset säännöt EU:n alueella toimiville yrityksille. Tämä sitoo myös EU:n ulkopuolisia yrityksiä, jos ne haluavat toimia EU:n markkina-alueella (Wahlqvist 2017).

2.3 Tietoturva

Tietoturvan keskeiset käsitteet ovat luottamuksellisuus, eheys ja saatavuus. Tätä voidaan kutsua nimellä CIA-malli. Lyhenne tulee sanoista confidentiality, integrity ja availability. Mallissa luottamuksellisuus tarkoittaa, että vain henkilöt joilla on oikeus käsitellä tietoa, saavat käsitellä tietoa. Ulkopuolisilla ei ole mahdollisuutta muuttaa tai tuhota

tietoa. Eheys tarkoittaa, että tiedot ovat luotettavia ja oikeita, eikä tieto saa muuttua sen olemassa olon aikana vahingossa tai ulkoisen tekijän toimesta. Saatavuudella tarkoitetaan, että tieto on käytettävissä silloin kun sitä tarvitaan henkilöiden toimesta, jotka sitä tarvitsevat. (Infosec Institute 2016.)

Voi helposti ajatella, että tietoturva on vain tietokoneella pyörivä virustorjunta ja palomuuri, jotka pitävät tietomme turvassa. Tietoturvaan on kuitenkin vahvasti sidoksissa myös ihmisluonne ja ajattelemattomuus. Tietoturvaan voi olla panostettu voimakkaasti, esimerkiksi yrityksessä, mutta jos työntekijät eivät noudata ohjeistuksia, ei siitä ole apua.

Yksi yleisimmistä tavoista suojata tietoa ja rajoittaa siihen pääsyä on pyytää salasanaa henkilöltä, joka yrittää päästä tietoon käsiksi. Salasanojen pituuksista on puhuttu vuosia ja se, mikä on joskus ollut tarpeeksi pitkä salasana, ei ole sitä enää nykyään tietokoneiden laskentakyvyn kasvaessa. Esimerkiksi Valtionvarainministeriön Sisäverkko -ohjeistuksessa (2010, 77-78) suositellaan vähintään 10 merkin pituista salasanaa. Vain neljä vuotta myöhemmin, Viestintävirasto (2014) suositteli jo vähintään 15 merkin salasanaa lauseen muodossa. Salasanan pituus tuleekin yhdistää monimutkaisuuteen, jolloin salasanalauseen murtamisesta tulee käytännössä mahdotonta (Crambler 2018).

Vielä nykyään eri ohjelmat ja yritykset pyytävät käyttäjää vaihtamaan salasanansa säännöllisin väliajoin. Esimerkiksi aiemmin mainitussa Valtionvarainministeriön Sisäverkko -ohjeistuksessa (2010, 78) määritellään salasanan enimmäisiäksi 90 päivää. Säännöllisen vaihdon tarkoituksena on ollut lisätä turvallisuutta, mutta itse asiassa se lisää riskiä, koska usein uusi salasana muistuttaa vanhaa ja siihen on esimerkiksi vaihdettu numero muistamisen helpottamiseksi. Jos hyökkääjällä on vanha salasana tiedossa, on uusi helppo arvata. (National Cyber Security Centre 2018.)

Kaikki nämä on ehdottomasti oikeita ohjeistuksia, mutta koska kukaan meistä ei voi muistaa kaikkien sivustojen monimutkaisia salasanoja ulkoa, yleisin ratkaisu on kirjoittaa niitä kootusti muistilapulle. Jopa F-Secure on aikanaan ohjeistanut ihmisiä tekemään niin (Sean 2009). Kun tämä muistilappu joutuu vääriin käsiin tai yksinkertaisesti unohtuu näkyville, on turha ihmetellä, miten joku pääsi kalliiden suojausten ohi. Koko ajan yleistyvä moderni vaihtoehto muistilapuille on salasanojen hallintaohjelmat. Ohjelmaa käyttäessä tarvitsee muistaa vain pääsalasana, ja muut salasanat, osoitetiedot, pankkitunnukset ja PIN-koodit pysyvät muistissa sen takana (F-Secure KEY 2017).

3 SOSIAALINEN MEDIA

Sosiaalinen media on tullut jäädäkseen. Palvelut kuten WhatsApp, Snapchat, Facebook, VKontakte, Instagram, Twitter, Kik, Skype ja WeChat ovat enemmän tai vähemmän tuttuja kaikille. Niitä käyttävät miljardit ihmiset päivittäin maanosaan, ikään, sukupuoleen tai sosiaaliseen asemaan katsomatta. Nykyään voidaankin pitää jopa outona, jos henkilöä ei löydy esimerkiksi Facebookista tai VKontaktesta. Näissä palveluissa käyttäjä esiintyy omalla nimellä, kun taas monessa muussa nimimerkin takana. Juuri omalla nimellä esiintymistä voidaan pitää yksityisyyden kannalta hankalana, koska palveluiden sähköistyessä sosiaalisella medialla on merkittävä rooli myös rikollisessa toiminnassa. Potentiaalisesti arkaluontoista tietoa kannattaa olla mahdollisimman vähän julkisesti saatavilla. Tämän takia on erityisen tärkeää tutustua jokaisessa palvelussa tarjolla oleviin yksityisyysasetuksiin ja tarkistaa, että ne ovat kunnossa.

3.1 Facebook

Facebook on kasvanut 2000-luvulla yhdeksi vaikutusvaltaisimmista sivustoista kiitos yli 2 miljardin käyttäjän ympäri maailmaa (Constine 2017). Facebook sai alkunsa vuonna 2004 kun Mark Zuckerberg julkaisi palvelun Harvardin yliopiston opiskelijoille ja opettajille suunnattuna. Syyskuusta 2006 lähtien sivustolle pystyi rekisteröitymään kuka tahansa. (Phillips 2007.) Vuonna 2008 Facebookista saatiin ensimmäinen suomenkielinen versio (Liekki 2014). Suomessa Facebook on neljänneksi vierailluin sivusto (Alexa 2017).

Facebookin suurin arvo on yhteisöllisyys. Pitämällä yhteyttä kavereihin ja lisäämällä tekstiä ja kuvia ihmiset voivat kommunikoida toistensa kanssa pitkistä välimatkoista huolimatta. Toisten julkaisuihin voi reagoida ja muiden ihmisten aikajanalle voi kirjoittaa viestejä. Facebookin Messenger-palvelun avulla käyttäjät voivat keskustella toistensa kanssa reaaliaikaisesti myös mobiilissa.

3.2 VKontakte

VKontakte on venäläinen sosiaalinen yhteisö, jota varsinkin aiemmin pidettiin venäläisenä vastineena Facebookille. Se on perustettu syyskuussa 2006 Pavel Durovin toimesta ja alun perin se oli tarkoitettu ainoastaan opiskelijoille. Heinäkuussa 2007 sivusto ylitti miljoonan käyttäjän rajan ja huhtikuussa 2008 10 miljoonan. Sen pääpaikka on Pietarissa, Venäjällä. Tänä päivänä VKontaktessa on yli 470 miljoonaa käyttäjää (VK 2018). Nykyään sivusto on käännetty myös yli 83 kielelle.

VKontaktessa kommunikoivat pääasiassa vain venäläiset muiden venäläisten kanssa. Verkkoliikennettä seurattaessa VKontakte on vierailluin sivusto Venäjällä, mutta kahdeksanneksi vieraillun sivu Suomessa (Alexa 2017).

Yksi VKontakten suurimmista eduista alusta asti on ollut tilapäivitysten lisäksi musiikin ja videoiden jakaminen. Tämä on osaltaan aiheuttanut myös ongelmia, ja VKontaktea pidetään yhtenä maailman pahamaineisimmista piratisminlähteistä (Andy 2016).

Saksalaisessa yliopistossa vuonna 2014 tehdyssä tutkimuksessa haluttiin selvittää, miksi venäläiset käyttäjät pitävät VKontaktesta enemmän kuin Facebookista. Tutkimukseen osallistujat olivat 18-25 vuotiaita nuoria venäläisiä. 54 osallistujasta kaikki olivat aktiivisia VKontakten käyttäjiä, mutta vain 2 osallistujaa oli aktiivisia Facebook käyttäjiä. 79,6 % viihtyi vähintään 2 tuntia päivässä VKontaktessa, kun taas 61,1 % viihtyi alle 15 minuuttia Facebookissa. (Baran & Stock 2015.) Tutkimuksen tuloksista selvisi, että VKontakte on hauskempi ja helpompi käyttää, ja sitä pidetään yleisesti luotettavampana käyttää.

4 YKSITYISYYTTÄ UHKAAVAT TEKIJÄT

Omien tietojen edelleen jakelua, muuttamista tai käyttämistä on mahdotonta estää. Eri yhteisöpalvelut voivat paljastaa sijaintitietoja ja mahdollistaa käyttäjän jäljittämisen hänen sitä tajuamatta. Jo pelkät kuvat saattavat paljastaa arkaluontoista tietoa esimerkiksi sijaintiin liittyen, joten aina tulisi harkita mitä internetissä julkaisee. On suositeltavaa olettaa, etteivät yksityisyyttä suojaavat asetukset hoida tehtäväänsä niiden mainostamalla tavalla.

4.1 Identiteettivarkaus

Identiteettivarkaus tarkoittaa toisen henkilön tietojen oikeudetonta käyttöä. Tätä voi olla esimerkiksi toisen nimi, valokuva, henkilötunnus tai käyttäjätunnus. Identiteettivarkaudessa henkilö esiintyy toisena henkilönä ilman hänen lupaansa.

Identiteettivarkaudesta tuli Suomessa rangaistavaa vuonna 2015. Muutamaa vuotta myöhemmin, vuonna 2017, se oli jo yleisempää kuin pyörävarkaudet (mySafety 2017). Identiteettivarkaus on asianomistajarikos ja uhrin on vaadittava rangaistusta rikoksen tekijälle. Rangaistavaa identiteettivarkaudesta tekee, jos siitä koituu uhrille taloudellista tai vähäistä suurempaa haittaa. Useimmiten identiteettivarkaus tulee esille muita rikoksia tutkittaessa. Haitallisen identiteettivarkaudesta tekee tietämättömyys mitä henkilön nimissä on tehty. Vahinkojen selvittäminen vie paljon aikaa epätietoisuuden ja tilanteen aiheuttaman stressin lisäksi. (Rikosuhripäivystys 2018.)

Varkauden seurauksista saattaa joutua kärsimään vuosia. Esimerkiksi kadonneen ajokortin avulla pystyy avaamaan pankkitilin, minkä avulla puolestaan voi nostaa pikavippejä (Mattila 2017). Identiteetin menettämisestä kertookin monesti vasta postiluukusta tullut lasku, kun henkilötunnusta on käytetty esimerkiksi verkkokaupasta ostamiseen.

4.2 Doksaus

Doksaus (alun perin docs, dokumentit) on yksityiselämää loukkaavan tiedon levittämistä ilman lupaa ja tarkoittaa lyhyesti toisen henkilötietojen etsimistä, kokoamista ja julkaisua ilkeämielisillä motiiveilla. Tällä pyritään pelottelemaan uhria kuin myös osoitta-

maan ettei yksityisyyttä ole olemassa (Quodling 2015). Doksaus juontaa juurensa 1990-luvun hakkerikulttuuriin, missä hakkerin ainoa tapa kostaa toiselle hakkerille oli murtaa tämän anonymiteetti (Honan 2014). Kyseessä on kiusanteko, mikä pahimmillaan johtaa maineen tahraamiseen ja sitä kautta esimerkiksi työpaikan menettämiseen. Mitä enemmän tietoa henkilöstä on saatavilla, sitä pelottavampi tilanne on. Hyvä doksaus voikin sisältää osoitetietoja, puhelinnumeron, sähköpostin, eri sosiaalisen median tilit, kuvia uhrista, hänen perheenjäsenistä sekä heistä kerättyä tietoa. (Liite 1. Dox.)

Suomessa doksaus on melko harvinaista. Toimittaja Juha Vainio kirjoitti kriittisen tekstin liittyen MV-lehden toimintaan. Seuraavassa hetkessä MV-lehden sivulla oli juttu Vainosta, missä hänen Twitter-tilin valokuvaan oli liitetty vanhoja twiittejä, työpaikan osoite, puhelinnumero sekä sähköposti. MV-lehti tarjosi vinkkipalkkioita ihmisille, jotka kertovat arkaluontoisia asioita valtamedioiden toimittajista. MV-lehti perusteli tiedonkeruuta ”puolustautumisella mahdollisia tulevia valheita kohtaan”. (Sallinen 2015.)

Arkaluotoisen tiedon keruu ei itsessään täytä minkään rikoksen tunnusmerkkejä, mutta niiden julkaiseminen on yksityiselämää loukkaavan tiedon levittämistä, mikä puolestaan on rangaistavaa. Toimittajaa uhkailemalla kyse on myös pyrkimyksestä rajoittaa sananvapautta.

Heinäkuun viidentenä päivänä uutiskanava CNN julkaisi uutisen, kuinka he löysivät Reddit-käyttäjän Trump-painianimaation takana. Uutinen itsessään on politiikkaa, mitä presidentti Trumpin valinnan jälkeen valtamediassa on nähty, mutta merkittävän uutisesta teki maininta, että CNN ei julkaise henkilön nimeä, mutta pidättää oikeuden julkaisuun jos tilanne muuttuu. (Kaczynski 2017.)

Henkilön identiteetti saatiin selville tutkimalla hänen viestihistoriaa Reddit-palvelussa. Reddit on verkkosivusto, missä käyttäjät voivat jakaa linkkejä, ajatuksia ja uutisia sekä keskustella niistä. Redditiä voi kuulla kutsuttavan internetin kotisivuksi. Henkilö, joka käytti nimimerkkiä HanAssholeSolo, oli maininnut viestissään asuinpaikkansa. Käyttämällä tätä ja muuta viesteistä saatua informaatiota identiteetti nimimerkin takana saatiin lopulta selville yksinkertaisella Facebook-haulla. (DeFranco 2017.)

Maailmalla doksaus on johtanut jopa kuolemantapauksiin, kun kerättyä tietoa on käytetty haitalliseen toimintaan. Joulukuussa 2017 nuori mies kuoli kotiovelleen jouduttuaan swattingin uhriksi. Swattingissa viranomaisille tehdään perätön uhkaus mihin heidän on pakko reagoida. Nimen alkuperä on Yhdysvalloissa, missä uhkatilanteisiin vastataan lähettämällä paikalle SWAT-joukot. Hätäpuhelussa miehen väitettiin olevan

aseistettu ja pitävän perhettään panttivankina. Saavuttuaan ulko-ovelle, poliisi ampui miehen. Myöhemmin selvisi, että kyseessä oli kahden pelaajan välisen riidan tuloksena tapahtunut uhkaus tuntemattoman ihmisen osoitteeseen. Uhriksi joutunut mies ei edes pelannut videopelejä ja oli tapaukseen täysin ulkopuolinen. (Krebs 2017.)

4.3 Verkkotunnuksen omistajatiedot

Whois-tieto kertoo domainin eli verkkotunnuksen omistajan tiedot. Se kertoo muun muassa verkkotunnuksen omistajan, hänen puhelinnumeron ja osoitetiedot, tunnuksen rekisteröinti- ja vanhenemispäivän sekä nimipalvelimet. Whois-tietokannasta voi kuka tahansa hakea verkkotunnuksen omistajan tietoja. Tietokanta mahdollistaa läpinäkyvyyden kuka verkkotunnuksen omistaa ja tarjoaa yhteyshenkilön keneen ottaa yhteyttä, mutta mahdollistaa myös tiedon hyväksikäytön. (Domaintools 2018.)

Useimmille verkkotunnuksille on mahdollista hankkia Whois -suojaus, missä omistajan yhteystiedot on mahdollista piilottaa (Kuva 1). Tällöin omistajan tiedot eivät ole julkisesti saatavilla, mutta olemassa pyydettäessä.

Kuva 1. Whois -tiedot esimerkki (Zoner 2018).

Tämän lisäksi on olemassa sivustoja, mitkä arkistoivat verkkotunnusten omistajatietoja. Joskus omistetun verkkotunnuksen omistajatiedot saattavat olla edelleen tällaisen sivuston arkistoissa aiheuttaen omien yhteystietojen löytämisen vielä vuosienkin päästä. Aihetta tutkiessa löysin kaksi vuotta sitten omistamani verkkosivun tällaisesta arkistosta mistä en ollut tietoinen. Sivuston Whois-tiedoista löytyikin oma nimi, puhelinnumero sekä sen aikainen osoite (Website Informer 2018). Asiasta voi tehdä poistopyynnön, jolloin tiedot saa poistettua arkistosta.

5 TIEDONKERUUN RAJOITTAMINEN

Olemme kaikki rekisteröityneet joskus sivustolle vain jotakin tiettyä asiaa varten, minkä jälkeen unohdamme kyseisen käyttäjätunnuksen. Pahimmassa tapauksessa olemme saattaneet kertoa paljonkin tietoa rekisteröitymisen yhteydessä. Ajan kuluessa olemme unohtaneet sivuston olemassaolon, mutta kyseinen sivusto ei ole unohtanut meidän olemassaoloa. Kaikki rekisteröitymisen yhteydessä annetut tiedot ovat edelleen olemassa palvelimella jossakin päin maailmaa.

On sanonta ”what happens on the internet, stays on the internet”, eli mikä kerran päätyy internetiin, säilyy internetissä. Tähän vedoten turhien tunnuksien olemassaolo on tietoturvariski. Jos yhden palvelun tietoturva pettää, on vuodetut tiedot mahdollista kohdentaa yksilöihin ja sitä kautta muihin palveluihin ja alkaa rakentaa uhrien identiteettiä. Vuodetut tiedot ovat käyttökelpoisia vielä vuosien päästä ja niitä voidaan käyttää osana tietomurtoa myöhemmin tulevaisuudessa (F-Secure Business Security Insider 2017). Mitä enemmän aikaa kuluu, sitä vaikeampi on kohdentaa alkuperäistä tiedonlähdettä mistä tieto on vuotanut.

Tiedonkeruun rajoittaminen ei kuitenkaan ole niin yksinkertaista. On mahdollista, että edes palveluntarjoaja ei tiedä mitä tietoja he jakavat eteenpäin, tai mihin tietoihin kolmansilla osapuolilla on pääsy. Tästä varoittavana esimerkki on Facebookin ja Cambridge Analytican tapaus, missä Cambridge Analyticalla oli pääsy miljoonien käyttäjien tietoihin luvatta.

Cambridge Analytica keräsi luvatta käyttäjien tietoja käyttäen sovellusta ”thisisyourdigitallife”. Ongelmalliseksi tilanteen tekee, että ainoastaan 270,000 käyttäjää oli sallinut sovelluksen pääsyn omiin tietoihin. Sovellus keräsi kuitenkin tietoa myös käyttäjien kavereista heidän suostumustaan kysymättä. Facebook ilmoitti asiasta omassa blogissaan ja uskoo jopa 87 miljoonan käyttäjän joutuneen luvattoman tiedonkeruun uhriksi, ja myöntää, ettei tiedä tarkalleen mihin dataan Cambridge Analyticalla oli pääsy, tai kuinka montaa henkilöä tapaus on koskettanut (Facebook 2018). Tapahtuneeseen reagoitiin voimakkaasti, ja Facebookin arvosta katosi viikossa lähes 60 miljardia dollaria (Martin 2018). Muutamaa kuukautta myöhemmin Cambridge Analytica ajautui konkurssiin asiakkaiden siirryttyä muualle tapauksen seurauksena (Confessore & Rosenberg 2018).

Seuraavaksi uutisoitiin kuinka Facebook poisti käytöstä hakuominaisuuden, millä käyttäjiä pystyi etsimään joko puhelinnumeron tai sähköpostiosoitteen avulla, jos henkilö oli sallinut niillä itsensä löydettävän. Paljastui, että kyseistä ominaisuutta oli hyväksikäytettyä vuosien ajan syöttämällä tietovuotojen yhteydessä vuodettuja puhelinnumeroita ja sähköpostiosoitteita Facebookin hakutoimintoon. Tällä menetelmällä hakkerit onnistuivat löytämään puhelinnumerolle tai sähköpostiosoitteelle kasvot saaden tietoonsa uhrin nimen, asuinpaikan, kuvat ja muun julkisen tiedon. (Timberg ym. 2018.)

Yksittäisellä, irrallaan merkityksettömällä, tiedonmurulla oli mahdollista rakentaa ja varastaa identiteettejä käyttämällä hyväksi julkisesti saatavilla olevia palveluita. Näitä varastettuja identiteettejä voidaan puolestaan käyttää rikolliseen toimintaan. Poistamalla turhat tilit ja rajoittamalla julkisesti saatavilla olevaa tietoa madallamme riskiä siitä, että tietomme joutuvat vääriin käsiin tai niitä käytetään hyväksi.

5.1 Deseat.me-palvelu

Deseat.me on palvelu, missä kuka tahansa voi tarkistaa omien tiliensä olemassaolon. Palvelu on tehty erittäin yksinkertaiseksi ja sivustolle kirjaudutaan sillä sähköpostiosoitteella, mitä halutaan tutkia. Palvelu listaa löytyneet sivustot sekä tarjoaa ohjeet ja suorat linkit tilien poistoon. Palvelun etuna on tuoda jo kerran unohdetut tunnukset uudelleen käyttäjän tietoisuuteen.

5.2 Stalkscan-palvelu

Stalkscan.com on palvelu mikä näyttää kenen tahansa henkilön Facebook-tilin julkisen sisällön. Etenkin Facebookin varhaisessa historiassa, palvelu sai reilusti kritiikkiä, kun käyttäjämäärien kasvaessa yksityisyysasetukset eivät pysyneet perässä. Tieto minkä luuli olevan piilossa, ei välttämättä ollut. Stalkscanin ideana on, että kuka tahansa voi tarkistaa mitä tietoa hänen sivuillaan on julkisesti saatavilla - jopa tieto mitä Facebook ei näytä sinulle. Palvelu on erinomainen apuväline tarkastellessa yksityisyysasetusten pitävyyttä.

5.3 Fonecta-yhtiö

Fonecta on suomalainen yhteystieto- ja mediayhtiö. Fonecta tarjoaa tietoa henkilöistä, yrityksistä, ajoneuvoista, palveluista ja puhelinnumeroista. Palveluun kirjaudutaan omalla sähköpostiosoitteella ja rekisteröityminen maksaa 0,25 euroa. (Fonecta 2018.) Palvelu on erinomainen, kun ystävän tai tuttavan numero tai osoite on hukassa. Teoriassa kuka tahansa voi löytää kenen tahansa yhteystiedot pelkän nimen tai numeron perusteella, mikä on erinomainen etu esimerkiksi tarkistettaessa onko henkilö kuka hän väittää olevansa. Valitettavasti tämä avaa mahdollisuuden myös rikollisille selvittää uhrin sijainti. Fonecta saa yhteystiedot suoraan operaattoreilta ja ainoa tapa piilottaa osoitetietonsa on kieltää se operaattorin kautta ja asettaa oma numero salaiseksi.

5.4 Trafi – Liikenteen turvallisuusvirasto

Liikenteen turvallisuusvirasto Trafi vastaa muun muassa liikenteen sääntely- ja valvontatehtävistä. Ajoneuvoliikennerekisteristä on mahdollista saada minkä tahansa ajoneuvon tiedot rekisteri- tai valmistenumeron perusteella (Trafi 2018). Ajoneuvon omistajatiedot nimen ja osoitteen kera ovat maksullisia, mutta kaikkien saatavilla. Kuka tahansa voi selvittää ajoneuvon omistajan tietämällä ajoneuvon rekisteritunnuksen, ellei omistaja ole tehnyt osoitteenluovutuskieltoa.

6 YKSITYISYYDEN SUOJAAMINEN

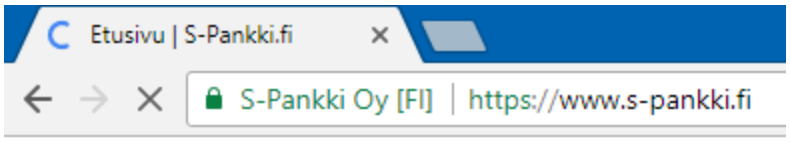
Yksityisyyden hintaa tutkittaessa, ensimmäisenä tulee tarkastella miten paljon ihmiset arvostavat omaa yksityisyyttään internetissä. Kysymykseen arvostavatko ihmiset omaa yksityisyyttään lyhyt vastaus on kyllä, ihmiset arvostavat omaa yksityisyyttään. Vuonna 2013 julkaistussa tutkimuksessa 86 % osallistujista oli tehnyt valintoja suojatakseen omaa yksityisyyttään verkossa esimerkiksi käyttämällä salattua yhteyttä tai tyhjentämällä selainhistoriansa (Williams ym. 2016). Samalla huomattiin, että korkeamman koulutuksen omaavat henkilöt pitävät paremmin huolta yksityisyydestään. Toisessa tutkimuksessa ihmiset olivat kuitenkin valmiita myymään selainhistoriansa 7 eurolla, osoitetietonsa 25 eurolla sekä sosiaalisen median kuvansa 12 eurolla (Carrascal ym. 2013). Vaikuttaakin siltä, että ongelma ei ole välittävätkö käyttäjät omasta yksityisyydestään, vaan miten arvokkaana he pitävät tietoa itsestään. Emme välttämättä tajua miten arvokasta meistä kerätty tieto on nykyaikana. Data on uusi öljy, ja koska isot yhtiöt tienaavat miljardeja sillä, kaikki haluavat kerätä dataa ja olla ensimmäisiä markkinoilla tarjoamassa uusia tuotteita ja palveluita (Linnake 2018). Onneksi on tapoja edesauttaa omaa yksityisyyttä ja varmistaa, ettei arvokas tieto päädy ulkopuolisille tahoille ainakaan oman huolimattomuuden seurauksena.

6.1 HTTPS

Salattu yhteys eli HTTPS pitää huolen, että kaikki verkossa siirretty data on salattua ja kukaan muu paitsi sinä ja vastaanottava taho ei pysty sitä lukemaan. HTTPS on yleistynyt viime vuosina voimakkaasti ja nykyään puolet kaikesta liikenteestä on salattua (Kuva 2). “Man in the Middle” -hyökkäyksessä uhrin ja verkkopalvelun välinen hyökkäys kaapataan ja siinä liikkuvaa tietoa voidaan lukea tai muokata (Viestintävirasto 2011). Kaikista yksinkertaisin tapa joutua uhriksi on käyttää julkista WLAN-verkkoa. Jos verkkosivu ei käytä salattua yhteyttä, on kaikki kirjoitettu data suoraan luettavissa kenen tahansa muun verkkoon liittyneen henkilön toimesta. Verkkoliikennettä voi seurata esimerkiksi ohjelmalla Wireshark, mikä on vapaasti ladattavissa.

Kuva 2. 68 % kaikista Firefox-käyttäjien yhteyksistä oli salattua 15. tammikuuta 2018 (Let's Encrypt 2018).

Varmin tapa suojautua Man in the Middle – hyökkäykseltä on käyttää salattua yhteyttä ja varmistaa, että verkkosivulla on se käytössä. Tämän voi tarkistaa, että osoiterivillä lukee *https* eikä pelkästään *http* (Kuva 3). Lisäksi osoiterivillä on vihreä lukko osoittamassa, että yhteys on salattu.



Kuva 3. Salattu yhteys Google Chromessa.

Jos yhteys ei ole salattu, on selaimeen mahdollista asentaa lisäosana esimerkiksi HTTPS Everywhere -laajennus, mikä ensisijaisesti vaihtaa yhteystyypiksi salatun yhteyden. Laajennus on saatavilla Firefoxiin, Chromeen, Operaan sekä Firefox for Androidiin (EFF 2018). Sovelluksen on kehittänyt Electronic Frontier Foundation, joka tunnetaan kansalaisten oikeuksia tietoyhteiskunnassa puolustavana järjestönä.

6.2 Cookies - evästeet

Evästeitä on olemassa kahdenlaisia: istuntokohtaisia ja pysyviä. 50 % verkkosivustoista käyttää evästeitä, eng. cookies, seuratakseen käyttäjiensä toimia. Tästä puolet (25%) seuraa käyttäjiään pysyvästi. (W3techs 2018.) Evästeiden avulla voidaan tunnistaa IP-osoite, kellonaika, käytetyt sivut, selaintyyppi, ja mistä verkko-osoitteesta, palvelimelta ja verkkotunnuksesta käyttäjä on saapunut kyseiselle verkkosivulle (Viestintävirasto 2018).

Evästeet itsessään ovat hyödyllisiä verkkoselailussa. Vieraillessasi esimerkiksi verkkokaupassa, sinun ei tarvitse kirjautua uudelleen sisään katsottuasi tuotetta, vaan verkkosivu pitää sinut kirjautuneena koko vierailun ajan. Lisätessäsi tuotteen ostoskoriin, verkkosivu säilyttää tuotteen ostoskorissa. Parhaiten evästeiden olemassaolon, sekä haitallisuuden, huomaa, kun verkkosivulla ilmestyy mainos esimerkiksi hotellista, jonka sivulla vierailit vain muutamaa minuuttia aiemmin.

Evästeiden välttämiseksi kannattaa käyttää verkkoselaimen Yksityistä selausta. Tätä käyttämällä vieraillut sivut eivät tallennu selaushistoriaan ja verkkosivustot saavat tiedon, ettei käyttäjä halua evästeitä tallennettavan. Kaikkien verkkoselainten asetuksista pystyy nykyään määrittämään etteivät verkkosivut saa seurata käyttäjän liikkeitä.

6.3 VPN

VPN (Virtual Private Network) tarkoittaa virtuaalista erillisverkkoa. VPN-yhteyden avulla käyttäjä muodostaa salatun yhteyden internetiin ja mahdollistaa turvallisen selaamisen estämällä esimerkiksi urkinnan ja hakkerien hyökkäykset. (VPN-yhteys 2018.)

VPN tarjoaa myös muita etuja. Käyttäjä voi esimerkiksi piilottaa oman IP-osoitteen sekä kiertää mahdollisia maakohtaisia rajoituksia. Tästä yksinkertaisena esimerkkinä mainittakoon Netflix. Suomen ja USA:n tarjonnassa on suuria eroja ja käyttämällä VPN:ää, on mahdollista katsoa toisen maan tarjontaa. Tästä ei Netflix pitänyt, vaan kuultuaan asiasta, yritys alkoi keksiä tapoja estää maarajoitusten kiertäminen (Hern 2016).

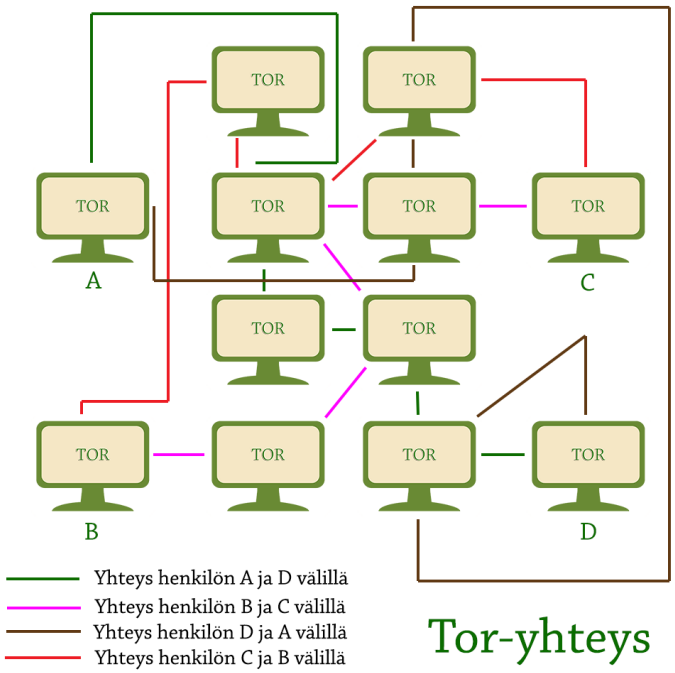
Yksityisen selaamisen varmistamiseksi, kannattaa VPN pitää päällä aina. Erityisesti aiemmin mainitun julkisten verkkojen tietojenkaappauksen pystyy välttämään VPN-yhteyttä käyttämällä. Myös yksittäisten ohjelmien on mahdollista määrittää reitti VPN-yhteyden kautta, jotta kaikki tieto pysyy suojassa.

On yleistä, että VPN -tarjoaja väittää kaiken liikenteen olevan salattua ja mitään lokeja ei säilytetä, mutta todellisuudessa näin ei välttämättä ole (Vänskä 2017). Täysin varmoja siitä, pitääkö luvatut asiat paikkansa ei voi olla ja kyse on enemmän luottamuksesta palveluntarjoajan ja käyttäjän välillä. 18 % Androidille saatavista VPN -sovelluksista ei todellisuudessa edes salannut käyttäjiensä yhteyttä (Ikram ym. 2016). Käyttäjien luottamuksen saamiseksi TunnelBear mainostaa itseään ainoana VPN -tarjoajana maail-

massa, joka on ulkopuolisen kolmannen osapuolen auditoima ja luvatut asiat pitävät paikkansa (Ryan D 2017).

6.4 Tor-verkko

Tor eli The Onion Router, suom. ’sipulireititin’, viittaa nimensä tavoin kerrokselliseen salaustekniikkaan. Perustarkoituksena on piilottaa oma identiteetti verkossa, ja näin ollen mahdollistaa verkon selaaminen ja sisällön lataaminen anonyymisti. (Krohn 2017). Luotu yhteys kulkee useiden palvelinten kautta häivyttäen yhteyden alkuperän (Kuva 4). Tästä syystä henkilöä yhteyden takana on lähes mahdotonta jäljittää. Pelkästään tieto, että yhteys on muodostettu käyttäen Tor-verkkoa, saattaa herättää viranomaisten mielenkiinnon (Brandom 2013). Alkuperän selvittäminen on kuitenkin erittäin työlästä, joten viranomaisilla täytyy olla polttava tarve saada selville identiteetti salatun yhteyden takana.



Kuva 4. Yhteyden muodostaminen Tor-verkossa (Krohn 2017).

Tor-verkon aktiivisen käytön suurimpana esteenä on sen hitaus. Koska tieto kulkee useiden palvelinten kautta, on verkkoselaaminen hidasta puhumattakaan videoiden katselusta. Koska on mahdollista, että erilaiset lisäosat vuotavat oikean IP-osoitteen, ei niitä ole Tor-selaimessa ollenkaan oletuksena (Tor 2018). Tämä asettaa omia haittoja

verkkoselaamiseen, eivätkä kaikki sivustot välttämättä toimi oikein. Tor ei korvaa VPN:ää, mutta yhdessä niiden käyttö mahdollistaa paremman turvallisuuden ja yksityisyyden hallinnan.

6.5 Have I Been Pwned

haveibeenpwned.com on palvelu, joka perustuu julkisesti vuodettuihin tietokantoihin ja mahdollistaa käyttäjälle tilaisuuden tarkistaa, onko hän joutunut tietomurron uhriksi oman sähköpostin syöttämällä. Käyttäjä voi halutessaan tilata sähköposti-ilmoituksen, jos hänen tietojaan käsitellyt verkkosivu on joutunut tietomurron kohteeksi. Tämä auttaa pysymään ajan tasalla, mikäli omat tiedot päätyvät yleiseen jakeluun internetissä. Mainitussa tilanteessa salasanan vaihto on äärimmäisen tärkeää suorittaa mahdollisimman nopeasti ennen kuin joku muu alkaa hyväksikäyttää murron yhteydessä saatua tietoa.

6.6 Julkisen tiedon salaaminen

Doksaamiselta suojautumisen ongelmalliseksi tekee, ettei siihen ole keinoa suojautua. Suurimman osan tarvittavasta tiedosta löytää nykyään julkisista lähteistä ja mitä julkisemmassa asemassa henkilö toimii, ja mitä aktiivisempi hän on sosiaalisessa mediassa, sitä enemmän tietoa hänestä on vapaasti saatavilla. Käytännössä pelkkä nimen ja kaupungin tietäminen riittää identiteetin selvittämiseen yksinkertaisella Facebook-haulla. Numerotiedustelusta saa useimmiten osoitetiedot. Google kertoo ja muistaa asioita, mistä emme välttämättä olleet tietoisia.

Yksi suojautumistapa on tehdä omasta kotiosoitteesta ja puhelinnumerosta salainen. Omaa asuinpaikkaa on mahdotonta pitää salassa, mutta riskiä, että täysin tuntematon henkilö selvittää asian, pystyy laskemaan. Kyseiset tiedot salaamalla puhelinnumerolla ei voi tehdä numerotiedustelua eikä selvittää asuinpaikkaa.

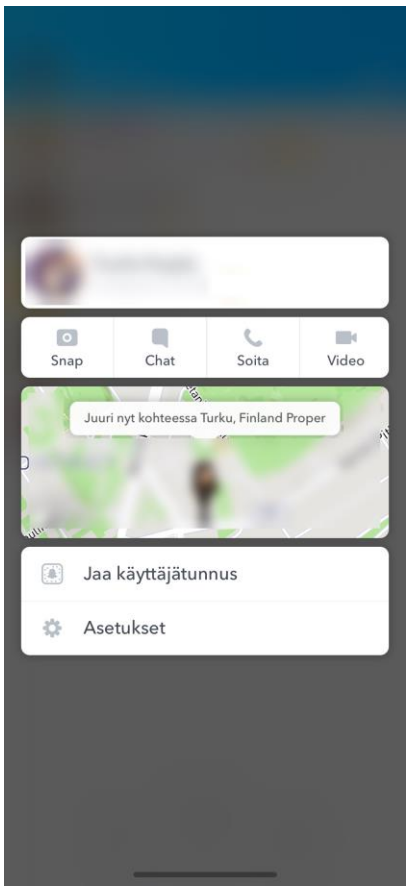
Vaikka oman numeron olisi asettanut salaiseksi ja piilottanut yhteystietonsa, voi omat henkilötiedot vuotaa myös ajoneuvorekisteristä. Yle uutisoi, miten asuntomurtajat vahtivat lentokenttien ja satamien parkissa ja käyttävät ajoneuvorekisteriä murtojen suunnittelussa (Mansikka 2016). Ajoneuvorekisteri on lähtökohtaisesti julkinen. Rekisterinumerolla on mahdollista selvittää omistajan tiedot nimen ja osoitteen kera. Osoitetie-

dot voi salata osoitteenluovutuskielto tekemällä ja ilmoituksen saa tehtyä joko täyttämällä lomakkeen Trafin sivuilla tai soittamalla Trafin asiakaspalveluun.

6.7 Psykologia

Erilaisten ohjelmien ja salattujen yhteyksien lisäksi yksityisyyden suojaamiseen tarvitaan tervettä järkeä. Yksinkertaisin keino tarkistaa mitä tietoa itsestään on saatavilla, on kirjoittaa oma nimi hakukoneisiin. Eri hakukoneet näyttävät hieman erilaista tietoa, joten pelkkä Googlen käyttö ei riitä. Jos hakutuloksista paljastuu asioita mistä ei ollut tietoinen, kannattaa tutkia mahdollisuus tiedon poistamiseen.

Varmin tapa suojata omaa yksityisyyttään internetin aikakaudella on yksinkertaisesti jakaa mahdollisimman vähän tietoa julkisesti. Silti joka viides henkilö kertoo jakavansa omaa sijaintiaan sosiaalisessa mediassa (Williams ym. 2016). Sijaintia ei välttämättä tarvitse edes päivittää, vaan se päivittyy joka kerta sovellusta käytettäessä (Kuva 5).



Kuva 5. Tuntemattoman henkilön sijainti Snapchatissä jaettuna.

Vaikka omaa GPS-sijaintia ei jakaisi, voi pelkkä valokuva paljastaa enemmän kuin tulee ajatelleeksi. Tästä esimerkkinä on lokakuussa 2016 tapahtunut ryöstö Pariisissa, missä varkaat veivät Kim Kardashianilta miljoonien arvosta koruja. Varkaat olivat myöntäneet poliisikuulusteluissa sosiaalisen median tehneet Kimin seurannasta helppoa, kuin myös sen, mitä hänellä oli päivittäin mukanaan. (Reilly 2017.)

7 POHDINTA

Opinnäytetyön tarkoituksena on ollut tarkastella käyttäjän yksityisyyttä internetin maailmassa sekä siihen liittyviä vaaroja ja ratkaisuja. Koska suuret yhtiöt tienaavat miljardeja käyttäjiensä tiedoilla, tulisi kaiken olla tiukasti säädeltyä. Tutkiessa yksityisyyteen liittyviä riskejä kävi varsin nopeasti selväksi, miten esimerkiksi lainsäädäntö kulkee digitalisaation perässä. Esimerkiksi identiteettivarkauden rangaistavuus vasta vuonna 2015 osoittaa lainsäädännön hitauden. Uuden polkupyörän voi ostaa rahalla, mutta puhdasta mainetta ei. Identiteettivarkauden seurauksista voi joutua kärsimään vuosia tapahtuneen jälkeen.

Suuret yhteisöpalvelut kuten Facebook ja VKontakte ovat mullistaneet maailman niin hyvässä kuin pahassa. Toisesta henkilöstä ei tarvitse tietää juuri mitään ja hän on silti löydettävissä. Tämä puoltaa väitettä, miten kaikki henkilötieto voi olla arkaluontoista tietoa.

Soittamisen ja tekstiviestin rinnalle ovat tulleet WhatsApp, Snapchat, Instagram, Twitter, Kik, Skype ja monet muut palvelut. Salauksen ansiosta esimerkiksi viestin lähettäminen WhatsApissa on turvallisempaa kuin perinteisen tekstiviestin. Palvelut tarjoavat samoja ominaisuuksia, mutta kaikilla on omat asetukset käyttäjän yksityisyyden hallintaan. Täydellä varmuudella ei voi sanoa mitä kaikkea tietoa kerätään, tai mihin kaikkeen tietoon kolmansilla osapuolilla on pääsy.

Internetiä käytettäessä meihin pyritään jatkuvasti vaikuttamaan. Ilmaisia palveluita käytettäessä tuskin miettii olevansa itse tuote. Esimerkiksi monet kahvilat tarjoavat ilmaista langatonta verkkoa, mutta tiedämmekö, että verkon asetukset ovat kunnossa, ettei kukaan seuraa liikennettämme?

Korkeamman koulutuksen omaavat henkilöt pitävät paremmin huolta yksityisyydestään ja paljastivat vähiten tietoa itsestään. Voidaan esittää kysymys, onko yksityisyys tarkoitettu vain parempiosaisille? Tämä olisi mielenkiintoinen näkökulma jatkotutkimukselle. Onko heikompiosaisilla edes mahdollisuutta yksityisyyteen? On olemassa työkaluja, kuten VPN-yhteys, joiden avulla voidaan edesauttaa tietojen pysymistä salattuna esimerkiksi epäluotettavissa verkoissa, mutta enemmistö niistä on kerta- tai kuukausimaksun takana. Yksityisyyden tarve on luonut uudet markki-

nat, mikä todistaa ilmiön laajuudesta. Henkilökohtaisesta tiedosta on tullut kauppatavaraa, minkä suojaamisessa jopa isot palveluntarjoajat ovat ongelmissa. Siksi on erityisen tärkeää huolehtia itse omasta yksityisyydestä ja varmistaa ettei oman huolimattomuuden tai tietämättömyyden takia joudu esimerkiksi identiteettivarkauden uhriksi.

Esineiden internet on tulevaisuudessa suurin yksittäinen uhka yksityisyydelle. Vaikka laite ei välttämättä tarjoa asetuksia tai toimintoja käyttäjälle, se voi kuitenkin lähettää erinäistä tietoa valmistajalle. Kun nykymaailma sekoittuu virtuaalisuuteen, riski käyttäjien hyväksikäytöstä kasvaa. Ohjelmien ja asetusten yksinkertaistaminen valmistajien toimesta sekä tietosuojan parantaminen ovat välttämättömyys tulevaisuudessa. Tämä tarkoittaa viime kädessä viranomaisten vastuuta säätää uusia lakeja ja säädöksiä, tajuamaan tilanteen vakavuus tietoyhteiskunnassa ja pitämään huoli siitä, että käyttäjien yksityisyys tulee säilymään myös tulevaisuudessa.

LÄHTEET

Acquisti, A. 2013. What will a future without secrets look like? Viitattu 10.10.2017. https://www.ted.com/talks/alessandro_acquisti_why_privacy_matters#t-68767.

Alexa. 2017. Top sites in Finland. Viitattu 30.1.2018. https://www.alexa.com/topsites/countries/FI .

Andy. 2016. vKontakte Responds to US Notorious Pirate Market Allegations. Viitattu 13.9.2017. https://torrentfreak.com/vkontakte-responds-us-notorious-pirate-market-allegations-161223/ .

Baran K. & Stock W. 2015. Acceptance and Quality Perceptions of Social Network Services in Cultural Context: Vkontakte as a Case Study. Systemics, Cybernetics and Informatics. Heinrich Heine University Düsseldorf, Germany. Viitattu 13.9.2017. https://www.phil-fak.uni-duessel-dorf.de/fileadmin/Redaktion/Institute/Informationswissenschaft/heck/Baran___Stock_Vkontakte.pdf.

Brandom R. 2013. FBI agents tracked Harvard bomb threats despite Tor. Viitattu 17.1.2018. https://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor .

Carrascal J., Riederer C., Erramilli V., Cherubini M. & de Oliveira R. 2013. “Your browsing behavior for a big mac: Economics of personal information online,” in 22nd International Conference on World Wide Web, 2013, pp. 189–200. Viitattu 26.2.2018. http://jpcarrascal.com/docs/publications/WWW2013-Browsing_behavior_big_mac.pdf.

Confessore N. & Rosenberg M. 2018. Cambridge Analytica to File for Bankruptcy After Misuse of Facebook Data. Viitattu 17.5.2018. https://www.nytimes.com/2018/05/02/us/politics/cambridge-analytica-shut-down.html.

Constine J. 2017. Facebook now has 2 billion monthly users… and responsibility. Viitattu 28.9.2017. https://techcrunch.com/2017/06/27/facebook-2-billion-users/ .

Crambler. 2018. Password Security – Why Secure Passwords Need Length Over Complexity. Viitattu 12.5.2018. http://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/.

DeFranco P. 2017. WOW! CNN Update Gets Ugly, Kardashian Revenge Porn Takes Over The Internet, and More... Viitattu 24.9.2017. https://www.youtube.com/watch?v=Pzz4GKvmLJo .

Domaintools. 2018. What is Whois information and why is it valuable? Viitattu 25.4.2018. https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable.

EFF. 2018. HTTPS Everywhere. Viitattu 22.4.2018. https://www.eff.org/https-everywhere .

F-Secure Business Security Insider. 2017. ”Älä käytä samaa salasanaa useilla sivustoilla” ja yhdeksän muuta neuvoa, joilla turvaat käyttäjätilisi. Viitattu 10.10.2017. https://fi.business.f-secure.com/ala-kayta-samaa-salasanaa-useilla-sivustoilla-ja-yhdeksan-muuta-neuvoa-joilla-turvaat-kayttajatilisi .

F-Secure KEY. 2017. Kätevä sovellus salasanojen hallintaan. Viitattu 10.10.2017. https://www.f-secure.com/fi_FI/web/home_fi/key .

Fonecta. 2018. Käyttöehdot. Viitattu 26.5.2018. https://www.fonecta.fi/info/hyodyllista-tietoa/kayttoehdot/.

Hern A. 2016. Netflix announces crackdown on VPN users. Viitattu 17.1.12018. https://www.theguardian.com/technology/2016/jan/15/netflix-announces-crackdown-on-vpn-users .

Honan M. 2014. What is doxing? Viitattu 24.4.2017. https://www.wired.com/2014/03/doxing/ .

Infosec Institute. 2016. Viitattu 22.4.2018. http://resources.infosecinstitute.com/cia-triad/#gref .

Ikram M., Vallina-Rodriguez N., Seneviratne S., Kaafar M. & Paxson V. 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. Viitattu 22.4.2018. https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf .

Junttila J. 2014. Kuningaskuluttaja selvitti: Näitä suomalaisia hakutuloksia Google ei suostu unohtamaan. Viitattu 26.5.2018. https://yle.fi/aihe/artikkeli/2014/12/17/kuningaskuluttaja-selvitti-naita-suomalaisia-hakutuloksia-google-ei-suostu.

Kaczynski A. 2017. How CNN found the Reddit user behind the Trump wrestling GIF. Viitattu 26.9.2017. http://edition.cnn.com/2017/07/04/politics/kfile-reddit-user-trump-tweet/index.html .

Krebs B. 2017. Kansas Man Killed In 'SWATting' Attack. Viitattu 8.1.2018. https://krebsonsecurity.com/2017/12/kansas-man-killed-in-swatting-attack/ .

Krohn D. Kaikki mitä sinun tulee tietää Tor-selaimen käyttämisestä. Päivitetty 11/2017. Viitattu 17.1.2018. https://fi.vpnmentor.com/blog/tor-selain-mika-se-miten-se-toimii-ja-miten-se-liittyy-vpn-yhteyden-kayttoon/ .

Laki24. 2018. Henkilötieto: määritelmä. Viitattu 17.5.2018. https://www.laki24.fi/henkilotieto-maaritelma/.

Let's Encrpyt. 2018. Let's Encrypt Stats. Viitattu 15.1.2018. https://letsencrypt.org/stats/.

Liekki T. 2014. Facebook täyttää 10 vuotta – kerro meille, miten se on vaikuttanut sinun elämääsi. Viitattu 28.9.2017. https://yle.fi/uutiset/3-7065700.

Linnake T. 2018. Mikko Hyppönen: Salakavala uhka valtaa kotisi – nyt on viimeinen hetki toimia. Viitattu 29.1.2018. https://www.is.fi/digitoday/tietoturva/art-2000005543929.html .

Martin J. 2018. Viitattu 11.4.2018. http://www.bbc.com/news/business-43517995 .

Mansikka H. 2016. Asuntomurtajat kyttäävät autoja lentokenttien ja satamien parkissa – Trafi: Osoitetietojen luovutuksen voi helposti estää. Viitattu 24.4.2017. https://yle.fi/uutiset/3-9026468 .

Mattila R. 2017. Identiteettivarkaus piinasi Mikkoa viisi vuotta: "Sain kymppitonnin laskut ja osoitteeni siirrettiin Kilpisjärvelle". Viitattu 23.4.2018. https://op.media/teemat/Ihmiset/Identiteettivarkaus-piinasi-Mikkoa-viisi-vuotta:-

%22Sain-kymppitonnin-laskut-ja-osoitteeni-siirrettiin-Kilpisjarvelle%22-ed9e37ac7f6048e884ec9c9987413cda .

mySafety. 2017. Identiteettivarkaudet ovat Suomessa yleisempiä kuin pyörävarkaudet. Lehdistötiedote. Viitattu 27.2.2018. https://www.mysafety.fi/ajankohtaista/identiteettivarkaudet-ovat-suomessa-yleisempia-kuin-pyoravarkaudet .

National Cyber Security Centre. 2018. The problems with forcing regular password expiry. Viitattu 22.4.2018. https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry .

Pastebin. 2017. Viitattu 27.2.2018. https://pastebin.com/wdC1BM6q .

Phillips S. 2007. A brief history of Facebook. Viitattu 28.9.2017. https://www.theguardian.com/technology/2007/jul/25/media.newmedia .

Quodling A. 2015. Doxxing, swatting and the new trends in online harassment. Viitattu 24.4.2017. http://theconversation.com/doxxing-swatting-and-the-new-trends-in-online-harassment-40234 .

Reilly K. 2017. Kim Kardashian's Robber Admits Social Media Helped Him Commit The Crime. Viitattu 3.1.2018. http://www.refinery29.com/2017/01/138551/kim-kardashian-robber-used-social-media .

Rikosuhripäivystys. 2018. Identiteettivarkaudessa esiinnytään toisen henkilöllisyydellä. Viitattu 23.4.2018. https://www.riku.fi/fi/erilaisia+rikoksia/identiteettivarkaus/ .

Sallinen P. 2015. Paskamyrsky. Viitattu 24.4.2017. https://www.journalisti.fi/artikkelit/2015/7/paskamyrsky/ .

Schroepfer M. 2018. An Update on Our Plans to Restrict Data Access on Facebook. Viitattu 11.4.2018. https://newsroom.fb.com/news/2018/04/restricting-data-access/.

Sean. 2009. Put Your Passwords on a Post-it. Julkaistu 26.5.2009. Viitattu 12.5.2018. https://www.f-secure.com/weblog/archives/00001691.html.

Siviilitiedustelulaki. 2018. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. Annettu 25.1.2018. Viitattu 26.2.2018.

http://intermin.fi/documents/1410869/3723672/siviilitiedustelulaki_he_25012018.pdf/a39a0e3e-881f-453f-9c5e-f7dd56012990.

Suomen Perustuslaki 731/1999. Annettu eduskunnan päätöksen mukaisesti. Viitattu 10.10.2017. http://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P10.

Timberg C., Romm T., Dwoskin E. 2018. Facebook: 'Malicious actors' used its tools to discover identities and collect data on a massive global scale. Viitattu 11.4.2018. https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.08e038993c2d.

Tor. 2018. Viitattu 12.5.2018. https://www.torproject.org/download/download.html.en.

Trafi. 2018. Ajoneuvotiedot ja veron maksu. Viitattu 26.5.2018. https://asiointi.trafi.fi/web/asiointi/henkiloasiakkaat/tieliikenne/ajoneuvotietopalvelut.

Valtiovarainministeriö. 2010. Sisäverkko-ohje. Viitattu 12.5.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=5084ce47-32bf-4025-bcc1-73fc2de4edad&groupId=10229.

Viestintävirasto. Evästeet. Päivitetty 3.10.2017. Viitattu 17.1.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet/palveluidenturvallinenkaytto/evasteet.html .

Viestintävirasto. Man in the Middle -hyökkäyksen torjunta. Julkaistu 28.9.2011. Viitattu 26.5.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2011/09/ttn201109281253.html.

Viestintävirasto. Salasanalla on väliä. Julkaistu 3.12.2014. Viitattu 12.5.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/12/ttn201412031257.html.

VK. 2018. Viitattu 30.1.2018. https://vk.com/catalog.php .

VPN-yhteys. 2018. Viitattu 17.1.2018. https://www.vpnyhteys.fi/ .

Wahlqvist H. 2017. GDPR tulee – onko taloushallintosi valmis? Viitattu 22.4.2018. https://www.palettesoftware.com/fi/gdpr/ .

Website Informer. 2018. Viitattu 12.5.2018. http://website.informer.com/Hemmo+Roivas.html.

Wikipedia. 2017. VK. Viitattu 13.9.2017. https://en.wikipedia.org/wiki/VKontakte .

W3techs. Viitattu 17.1.2018. https://w3techs.com/technologies/details/ce-persistentcookies/all/all .

Yksityisyydensuoja. 2017. Viitattu 10.10.2017. https://www.yksityisyydensuoja.fi/yksityisyydensuoja.

YKSITYISYYS, MIKÄ SE ON? Viitattu 10.10.2017. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqO1Qzf/Tietoverkon_yhteisopalvelujen_yksityisyys_mika_se_on.pdf.

Yleistä tietosuojasta. 2014. Artikkeli opitietosuojaa.fi www-sivulla 27.11.2014. Viitattu 10.10.2017. https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja .

Ylipartanen A. & Andreasson A. 2015. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 10.10.2017. https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus

Zoner. 2018. Domain whois suojaus. Viitattu 25.4.2018.https://www.zoner.fi/domain-whois-suojaus/.

Liite 1. Dox

```
>[Personal Information:]<

Full Name:
Phone Number:
DOB: November
Email:
Picture:
Alias:

Education:

>[Location Information:]<

Address:


(Old Address)

Zip:
City:
State:
Country:

>[IP Information:]<

IP: (Current + Live)
ISP:
Name on Account:
Address on Account:
Email on Account:
Phone on Account:

PIA IP Address:
ISP:
PIA IP Address:
ISP:

>[Social Media Accounts/Useful Links:]<

Skype:
Facebook:


>[Family:]<

Mother's Name:
    DoB:
    Linkedin:
    Phone Number:
    Address:
    Email:

Father's Name:
    Facebook:
    Phone Number:
    Email:
```