Jouni Ali-Kovero

YKSITYISYYSONGELMAT GEOSOSIAALISISSA VERKOSTOPALVELUISSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Ali-Kovero, Jouni
Yksityisyysongelmat geososiaalisissa verkostopalveluissa
Jyväskylä: Jyväskylän yliopisto, 2016, 37 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Koskelainen, Tiina

Sosiaalisen median suosion kasvu on jatkunut jo pitkään. Viime vuosina erilaisia sosiaalisen median palveluja on alettu käyttää yhä enemmän mobiililaitteilla ja samalla paikkatiedon hyödyntäminen palveluissa on yleistynyt. Voidaankin todeta, että sosiaalisen median alle on syntynyt uusi alakategoria, paikkatietoa hyödyntävät mobiilit sosiaaliset verkostopalvelut, eli toisin sanoen geososiaaliset verkostopalvelut. On yleisessä tiedossa, että sosiaalisen median palvelut keräävät erilaisia tietoja käyttäjistään. Paikkatietoa hyödyntävien palveluiden yleistymisen myötä myös kerätyn tiedon määrä kasvaa ja näin ollen kasvaa myös uusien yksityisyysongelmien mahdollisuus. Tässä tutkielmassa tarkastellaan kirjallisuuskatsauksen keinoin, minkälaisia yksityisyysongelmia geososiaalisiin verkostopalveluihin liittyy käyttäjien näkökulmasta. Kirjallisuuskatsauksen perusteella todettiin, että yksityisyysongelmat johtuvat pääosin käyttäjien toiminnasta, sovellusten toiminnasta ja erilaisista ulkoisista tekijöistä. Tutkielman tavoitteena on tuottaa lukijalle käsitys yksityisyydestä, sosiaalisesta mediasta, sosiaalisista verkostopalveluista ja paikkatiedon hyödyntämisestä käsitteinä. Lisäksi tutkielma pyrkii esittämään tyypilliset geososiaalisiin verkostopalveluihin liittyvät yksityisyysongelmat.
Asiasanat: yksityisyys, yksityisyysongelma, mobiili sosiaalinen verkostopalvelu, paikkatieto, geososiaalinen verkostopalvelu

ABSTRACT

Ali-Kovero, Jouni
Privacy issues in geosocial networks
Jyväskylä: University of Jyväskylä, 2016, 37 p.
Information systems, Bachelor's Thesis
Supervisor: Koskelainen, Tiina

Growth in the popularity of social media has been on the rise for a long time. During recent years it has become more and more common to use different social media applications via mobile devices and therefore the use of location information has also increased. It can be said, that a new sub-category of social media has emerged: location based mobile social networks, also known as geosocial networks. It is widely known that social media services collect data about their users. With the rising popularity of location based services, the amount of collected data is also on the rise and therefore the probability of new kinds of privacy issues is increasing. The purpose of this bachelor's thesis is, by means of a literature review, to research the privacy issues users might face when using location based mobile social networks. Based on the literature review, it can be stated that privacy issues are typically caused by the user's actions, the services themselves and different external factors. The aim of this bachelor's thesis is to provide the readers with an understanding of the concepts of privacy, social media, social networking services and the use of location information. The thesis also aims to present the most typical privacy issues related to the use of location based mobile social networks.

Keywords: privacy, privacy issue, mobile social network, location information, geosocial network

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Sosiaalinen media on käsitteenä laajasti käytössä, mutta sen määrittely ei kuitenkaan ole kovin yksinkertaista. Kietzmannin, Hermkensin, McCarthyn ja Silvestren (2011) mukaan se voidaan ymmärtää verkkoon perustuvina teknologioina, joiden avulla luodaan interaktiivisia alustoja. Alustoilla käyttäjät ja yhteisöt voivat jakaa, tuottaa ja muokata käyttäjälähtöistä sisältöä. Kaplanin ja Haenleinin (2010) mukaan keskiössä on käyttäjälähtöinen sisältö (User Generated Content), lyhyemmin UGC ja sen jakaminen. Näin ollen sosiaalisen median voidaan nähdä toimivan eräänlaisena yläkäsitteenä, jonka alle kuuluvat erilaiset sisällönjakopalvelut, keskustelupalstat, blogit ja sosiaaliset verkostopalvelut. Tämän tutkielma käsittelee ensisijaisesti sosiaalisten verkostopalvelujen mobiilisovelluksia, joten muiden sosiaalisen median ilmentymien tarkastelu jää vähemmälle. Kaplanin (2012) mukaan sitä mobiilisovellusten joukkoa, joka mahdollistaa käyttäjälähtöisen sisällön luomisen ja jakamisen, voidaan kutsua mobiiliksi sosiaaliseksi mediaksi (Mobile Social Media).

Sosiaaliset verkostopalvelut vetävät puoleensa miljardeja käyttäjiä. Statistan (2016) tilastojen mukaan kaksi suurinta länsimaissa käytettyä sosiaalista verkostopalvelua ovat Facebook ja Twitter. Aasiassa on muutamia suuriakin palveluja, mutta ne eivät ole länsimaissa juurikaan käytössä, joten niiden tarkastelu jätetään tarkoituksella tämän tutkielman ulkopuolelle. Yhteensä Facebookilla ja Twitterillä oli vuoden 2016 syyskuussa 2,025 miljardia kuukausittaista kävijää, joista Facebookin käyttäjiä oli 1,712 miljardia ja Twitterin käyttäjiä 0,313 miljardia. Facebookin käyttäjistä noin 57 % käyttää palvelua ainoastaan mobiililaitteilla. Twitterin vastaava luku on yhtiön oman tilastoinnin perusteella 82 % (Twitter, 2016). Näin ollen voidaankin todeta, että valtaosa sosiaalisia verkostopalveluja käyttävistä ihmisistä käyttää palveluja yksinomaan mobiililaitteilla.

Sosiaalisille verkostopalveluille on ominaista, että käyttäjät luovat itselleen profiilin, johon lisäävät henkilökohtaisia tietoja itsestään (Kaplan & Haenlein, 2010). Profiileihin lisättävät tiedot vaihtelevat käyttäjien ja palveluiden mukaan, mutta tyypillisesti profiilin luomiseksi tarvitaan ainakin käyttäjän nimi ja sähköpostiosoite. Palveluntarjoajat usein rohkaisevat käyttäjiä lisäämään itsestään mahdollisimman yksityiskohtaisia tietoja (Acquisti & Gross, 2006). Selkeästi

suurin osa ihmisistä julkaiseekin itsestään nimen lisäksi esimerkiksi sukupuolen, iän ja kotikaupungin (Debatin, Ann-Kathrin Horn, & Hughes, 2009). Nimensä mukaisesti sosiaalisten verkostopalveluiden ytimessä ovat ihmisten väliset sosiaaliset verkostot. Verkostot koostuvat käyttäjien välisistä yhteyksistä, joita luodaan lähettämällä muille käyttäjille ”kaveripyyntöjä”. Hyväksytty kaveripyyntö antaa käyttäjille pääsyn toistensa profiileihin ja näin ollen he tulevat osaksi toistensa sosiaalista verkkoa (Dwyer, Hiltz, & Passerini, 2007).

Kuten aiemmin mainittiin, sosiaalisia verkostopalveluja käytetään nykyään tyypillisimmin mobiililaitteilla. Useimmat mobiililaitteet sisältävät paikkatietoa hyödyntävää teknologiaa, kuten GPS-paikannuksen. Tämä on mahdollistanut sen, että käyttäjät voivat jakaa henkilötietojensa lisäksi myös tietoja sijainnistaan (Wagner ym., 2010). Paikkatiedolla tarkoitetaan Kantolan (2013) mukaan sijaintitietoa, eli toisin sanoen tietoa, jolle voidaan osoittaa sijainti. Wun ja Schulzrinnen (2005) mukaan se voidaan jakaa kahteen pääkategoriaan, joita ovat sijaintitieto ja attribuuttitieto. Ensin mainittu viittaa tietoon siitä, missä jotakin on ja jälkimmäinen puolestaan tietoon siitä, mitä jossakin on.

Sosiaalisen median tavoin myös yksityisyyden tarkka määrittely voidaan nähdä ongelmallisena. Warrenin ja Brandeisin (1890) artikkelissa sen todetaan olevan ”The right to be let alone”, eli vapaasti käännettynä ”Oikeus tulla jätetyksi rauhaan”. Sittemmin käsitteelle on ehdotettu useita erilaisia määritelmiä. Tässä tutkielmassa keskitytään erityisesti informaation yksityisyyteen online ympäristössä. Stonen, Gueutalin, Gardnerin, ja McCluren (1983) mukaan informaation yksityisyydellä tarkoitetaan yksilön oikeutta kontrolloida itseään koskevaa informaatiota.

Keskeisiä käsitteitä tässä tutkielmassa ovat informaation yksityisyys ja siihen liittyvät ongelmat, paikkatiedon hyödyntäminen ja sosiaalisten verkostojen mobiilisovellukset. Englanninkielinen termi ’Geosocial Networks’ viittaa paikkatietoja hyödyntäviin sosiaalisiin verkostoihin. Tutkielmassa termi on suomennettu *Geososiaalisiksi verkostoiksi,* sillä termille ei löytynyt mitään yleisesti käytettyä suomenkielistä vastinetta.

Tutkielman tavoitteena on kirjallisuuskatsauksen keinoin selvittää, minkälaisia yksityisyysongelmia geososiaalisissa verkostopalveluissa ilmenee. Aihe on rajattu koskemaan erityisesti sosiaalisten verkostopalveluiden mobiilisovelluksia, eli mobiileja sosiaalisia verkostopalveluja, joten muut sosiaalisen median mobiilisovellukset jätetään tarkastelun ulkopuolelle. Aihetta tutkitaan sovellusten käyttäjien näkökulmasta, jolloin myös mahdolliset yksityisyysongelmat yritysten ja organisaatioiden osalta jäävät tutkinnan ulkopuolelle.

Tutkielman toisessa luvussa tarkastellaan sosiaalista mediaa ja sosiaalisia verkostopalveluja käsitteinä. Kolmas luku käsittelee yksityisyyttä. Yksityisyyden suhteen selvitetään, miten käsitettä on tarkasteltu eri aikoina ja minkälaista tutkimusta sen piirissä on tehty. Neljännessä luvussa puolestaan vastataan tutkielman tutkimusongelmaan, eli *minkälaisia yksityisyysongelmia geososiaalisten verkostopalveluiden käyttöön liittyy?*

Kirjallisuuskatsauksena tehtyä tutkielmaa varten haettiin lähteitä IEEE Xplore ja Google Scholar –tietokannoista. Lisäksi tarkasteltiin eri artikkeleiden lähdeluetteloja ja etsittiin relevanttia informaatiota niiden perusteella. Hakusanoina käytettiin seuraavia termejä: *social media, social networking, mobile social*

network, geosocial network, location based social network, privacy, privacy online, privacy issues, location privacy, paikkatieto, paikkatiedon hyödyntäminen ja sosiaalinen media.

Kirjallisuuskatsauksen perusteella havaittiin, että geososiaalisiin verkostopalveluihin liittyy useita yksityisyysongelmia. Ongelmien syyt liittyvät tyypillisimmin käyttäjien ja sovellusten toimintaan, sekä ulkoisiin tekijöihin, kuten kyberrikollisiin. Käyttäjistä johtuvat ongelmat perustuvat usein käyttäjien huolimattomuuteen. Sovelluksista johtuvat ongelmat taas liittyvät ongelmiin sovellusten toimintalogiikassa, kuten käyttäjien heikkoon identifikaatioon. Ulkoisten tekijöiden toiminta puolestaan perustuu sekä käyttäjien hyväuskoisuuden, että sovellusten toimintaan liittyvien heikkouksien hyväksikäyttöön.

2 SOSIAALISET VERKOSTOPALVELUT

Tässä luvussa tarkastellaan sosiaalisia verkostopalveluita ja sosiaalista mediaa yleensä. Myöhemmin tarkastelun kohteeksi otetaan sosiaalisen median mobiilisovellukset, joista Kaplanin (2012) mukaan voidaan käyttää käsitettä *mobiili sosiaalinen media* (mobile social media). Tämän tutkielman kannalta oleellisempi käsite on kuitenkin *mobiilit sosiaaliset verkostotpalvelut* (mobile social networks), jotka Najafloun, Jedarin, Xian, Yangin ja Obaidatin (2013) mukaan voidaan nähdä erityisenä sosiaalisen median osana, joka muusta sosiaalisesta mediasta poiketen on käyttäjilleen aina läsnä ja joka mahdollistaa käyttäjälähtöisen sisällön jakamisen siitä kiinnostuneiden käyttäjien kesken. Lopuksi käsitellään paikkatiedon ja mobiilien sosiaalisten verkostopalveluiden yhteyttä.

2.1 Sosiaalinen media

Sosiaalinen median suosio on kasvanut valtavasti kuluneen vuosikymmenen aikana. Kuten johdantokappaleessa mainittiin, erilaiset sosiaalisen median palvelut vetävät puoleensa miljardeja käyttäjiä. Suosiota kuvaavaa on, että muiden muassa Paavi Fransiscus kommunikoi Twitterissä 10 miljoonan seuraajansa kanssa. Suuren suosion myötä sosiaalinen media tutkimusaiheena on luonnollisesti kiinnostanut tutkijoita, jotka ovat paitsi pyrkineet antamaan käsitteelle mahdollisimman kattavan määritelmän, myös tutkineet sille ominaisia piirteitä.

Vaikka sosiaalista mediaa on vuosien varrella tutkittu paljon, ei käsitteen määritelmästä ole kuitenkaan päästy täysin yksimielisyyteen. Tutkijat ovat tarjonneet omia määritelmiään, joissa pääpiirteittäin korostuvat samat asiat. Tyypillisesti määritelmät sisältävät jonkinlaisen viittauksen käyttäjälähtöiseen sisältöön (UGC) ja Web 2.0-teknologiaan (Kietzmann ym., 2011; Kaplan & Haenlain, 2010). Kietzmann ym. (2011) määrittelevät sosiaalisen median verkkoon perustuvina teknologioina, joiden avulla luodaan interaktiivisia alustoja. Alustoilla käyttäjät ja yhteisöt voivat jakaa, tuottaa ja muokata käyttäjälähtöistä sisältöä.

Yleisesti ottaen voidaan nähdä, että sosiaalisessa mediassa on kyse nettiyhteisöissä tapahtuvasta osallistumisesta, vuorovaikutuksesta ja jakamisesta.

Sanaparissa ”sosiaalinen” viittaa ihmisten väliseen vuorovaikutukseen ja ”media” tämän vuorovaikutuksen mahdollistaviin alustoihin. Sen sovelluksille ominaista on käyttäjien aktiivinen osallistuminen, sekä avoin ja käyttäjälähtöinen sisältö. Onnistuneet sosiaalisen median sovellukset ovat paitsi helppokäyttöisiä, myös helposti ymmärrettäviä ja luotettavia (Heinonen, 2009.)

Sosiaalisen median sovelluksia on tutkimuksessa pyritty jakamaan erilaisiin kategorioihin. Lietsala ja Sirkkunen (2008) määrittelevät Sosiaalisen median palvelut viiteen kategoriaan niiden toiminnallisuuksien mukaan: sisällön tuottamiseen ja julkaisuun keskittyvät palvelut (blogit), sisällön jakamiseen keskittyvät palvelut (Youtube), sosiaaliset verkostopalvelut (Facebook), yhteisöpalvelut (Wikipedia), virtuaalimaailmat (Second Life) ja sosiaalisen median liitännäiset (Facebookin & Twitterin ”Tykkää”-nappi). Lietsalan ja Sirkkusen (2008) jaottelu on kuitenkin nykypäivänä tarkasteltuna liian karkea, sillä eri sovellukset ja palvelut ovat lähentyneet toisiaan omaksumalla toisistaan toiminnallisuuksia ja toki myös uusia palveluja on syntynyt.

Kietzmann ym. (2011) puolestaan jakavat sovellusten toiminnallisuudet seitsemään rakennuspalikkaan (functional building blocks), joita ovat identiteetti, keskustelut, jakaminen, läsnäolo, suhteet, maine ja ryhmä. Jokainen rakennuspalikka viittaa palveluiden toiminnallisuuksien lisäksi erilaisiin tapoihin käyttää sosiaalisen median palveluita. Jaottelussa jokainen sosiaalisen median palvelu koostuu ainakin yhdestä ja yleensä useammasta palikasta. Jaottelun avulla voidaan helposti havainnollistaa erilaisten palveluiden ominaisia piirteitä, mutta toisaalta myös alleviivata niissä piileviä yhtäläisyyksiä.

Taulukossa 1 esitetään Kietzmannia ym. (2011) mukaillen kunkin rakennuspalikan merkitys ja annetaan esimerkki sosiaalisen median sovelluksesta, jossa kyseisen palikan toiminnot ovat tärkeässä roolissa. Niiden sovellusten nimet, joissa kunkin palikan toiminnallisuudet painottuvat, on lihavoitu.

TAULUKKO 1 Sosiaalisen median rakennuspalikat (Kietzmann ym., 2011)

Rakennuspalikka	Merkitys	Palvelu
Identiteetti	Missä määrin henkilökohtaisten tietojen paljastaminen painottuu palvelussa.	**LinkedIn**, Facebook, Twitter, Foursquare
Keskustelut	Kuinka käyttäjien väliset keskustelut painottuvat palvelussa.	**Twitter**, Facebook
Jakaminen	Miten sisällön jakaminen painottuu palvelussa.	**Flickr**, **Youtube**, Facebook
Läsnäolo	Miten tieto siitä, kuinka muut käyttäjät ovat tavoitettavissa painottuu palvelussa.	**Foursquare**, Twitter, Facebook
Suhteet	Missä määrin palvelu painottuu käyttäjien välisten suhteiden luomiseen ja ylläpitoon.	**Facebook**, LinkedIn, Twitter, Foursquare
Maine	Onko käyttäjän asemalla suhteessa muihin käyttäjiin merkitystä.	Twitter, Facebook, LinkedIn
Ryhmä	Kuinka vahvasti käyttäjien muodostamat ryhmät ovat palvelun keskiössä.	Facebook, Flickr, Youtube

Sosiaalisille verkostopalveluille on tyypillistä, että käyttäjät luovat itselleen profiilin, lisäävät sinne henkilökohtaisia tietoja itsestään ja luovat verkostoja muiden käyttäjien kanssa (Dwyer ym., 2007; Huang & Liu, 2009; Kaplan & Haenlain, 2010). Ne voidaan myös määritellä palveluiksi, jossa käyttäjien on mahdollista luoda julkinen profiili, ilmaista omaan sosiaalisen verkostoonsa kuuluvat käyttäjät ja tarkastella muiden käyttäjien verkostoja (Boyd & Ellison, 2008). Niille on siis yhteistä, että käyttäjät ilmentävät yksilöllisyyttään omien profiiliensa kautta ja toisaalta tuovat julki omat sosiaaliset verkostonsa. Näin ollen voidaan taulukkoon 1 viitaten todeta, että sosiaalisissa verkostopalveluissa painottuvat ainakin ”Identiteetti”- ja ”Suhteet” –palikat, sillä palveluille ominaisimmat piirteet ovat henkilökohtaisen informaation jakamista varten luodut profiilit ja omien sosiaalisten verkostojen luominen ja julkistaminen.

Kietzmannin ym. (2011) rakennuspalikoiden avulla on mahdollista kuvata erilaisille palveluille ominaisia piirteitä, mutta niiden avulla tehty jaottelu on epätarkka, sillä monet palvelut jakavat samanlaisia piirteitä. Esimerkiksi Facebook on nykyään niin laaja palvelu, että sillä voidaan nähdä olevan piirteitä jokaisesta palikasta. Palvelussa on profiilin luomisen ja sosiaalisen verkoston ylläpidon lisäksi mahdollista esimerkiksi keskustella yksityisviestein, jakaa sisältöä muille käyttäjille, kertoa muille olevansa palvelussa kirjautuneena ja muodostaa ryhmiä ja yhteisöjä muiden käyttäjien kanssa. Lisäksi taulukkomuodossa esitetyt palikat saattavat vääristää eri toiminnallisuuksien painotuksia. Esimerkiksi Facebookissa käyttäjien identiteetti on tärkeässä osassa, mutta LinkedIn:in kohdalla palvelu suorastaan perustuu sille, sillä kyseessä on työnhakuun keskittyvä palvelu, jossa oman työhistorian julkistaminen on oleellista. Näin ollen LinkedIn on lihavoitu identiteetti –palikan kohdalla ja Facebook ei.

Kuten johdantokappaleessa mainittiin, tämä tutkielma keskittyy ensisijaisesti yhteen sosiaalisen median osaan; mobiileihin sosiaalisiin verkostopalveluihin. Mobiilista sosiaalisesta verkostopalvelusta riippuen, viitaten taulukon 1 rakennuspalikoihin, painottuvat ’palikat’ hieman eri tavoin. Suurimassa osassa palveluita paikkatiedon hyödyntäminen on kuitenkin hyvin oleellista ja näin ollen niissä painottuu varsinkin *Läsnäolo.*

2.2 Mobiilit sosiaaliset verkostopalvelut

Kaplanin (2012) mukaan sosiaalisen median mobiilisovelluksista voidaan käyttää termiä *mobiili sosiaalinen media.* Näin ollen sosiaalisten verkostopalveluiden mobiilisovellukset voidaan puolestaan määritellä mobiileiksi sosiaalisiksi verkostopalveluiksi; siinä missä sosiaaliset verkostopalvelut ovat osa sosiaalista mediaa, ovat mobiilit sosiaaliset verkostopalvelut osa mobiilia sosiaalista mediaa. Souzan ja Frithin (2010) mukaan mobiileja sosiaalisia verkostopalveluja voidaan kuvata neljän niille ominaisen elementin avulla: niiden käyttäjiä yhdistää jokin fyysisen maailman tila, kuten saman kaupungin keskusta, niissä olevat

verkostot ovat olemassa digitaalisessa maailmassa ja muodostuvat mobiililaitteiden avulla, ne ovat lyhytikäisiä ja niissä kommunikointi tapahtuu monelta monelle (many-to-many). Mobiilit sosiaaliset verkostopalvelut siis mahdollistavat sosiaalisten verkostojen syntymisen ja ylläpidon mobiiliympäristössä.

Sosiaalisia verkostopalveluita käytetään yhä useammin paikkatietoa hyödyntävillä mobiililaitteilla (Wagner ym., 2010). Tällöin voidaan siis puhua *paikkatietoa hyödyntävistä mobiileista sosiaalisista verkostopalveluista,* eli geososiaalisista verkostopalveluista. Termeille ei ole vakiintuneita suomenkielisiä käsitteitä, mutta englanninkielisessä keskustelussa niihin viitataan usein esimerkiksi käsitteillä ”Location Based Social Networks” (Roick & Heuser, 2013), ”Locative Mobile Social Networks” (Souza & Frith, 2010) ja ehkä tyypillisimmin ”Geosocial Networks” (Carbunar & Potharaju, 2012; Najaflou ym., 2013; Smith, Syed, Thaw, & Wong, 2011). Yleisesti hyväksytyn suomenkielisen käsitteen puuttuessa, tullaan tässä tutkielmassa kaikkiin ylläoleviin englanninkielisiin käsitteisiin jatkossa viittaamaan termillä *geososiaaliset verkostopalvelut.*

Roickin ja Heuserin (2013) mukaan geososiaalisilla verkostopalveluilla tarkoitetaan sosiaalisia verkostopalveluja, joissa jaettuun sisältöön liitetään paikkatietoja. Niitä voidaan myös kuvata neljän niille tyypillisen elementin kautta: (1) ne ovat ihmisistä koostuvia verkostoja, (2) ne ovat mobiileja, koska niihin kuuluvat ihmiset kommunikoivat mobiililaitteiden välityksellä ja heidän on mahdollista liikkua fyysisessä maailmassa kommunikoinnin aikana, (3) niihin osallistuvilla käyttäjillä on matkapuhelin ja (4) ne hyödyntävät paikkatietoa visualisoidakseen verkon käyttäjille toistensa fyysisen sijainnin kartan avulla. Gao ja Liu (2014) puolestaan määrittelevät geososiaaliset verkostopalvelut palveluina, jotka hyödyntävät GPS- ja WEB 2.0 –teknologioita, mahdollistavat käyttäjien jakaa tietoa sijainnistaan, etsiä mielenkiintoisia fyysisen maailman paikkoja ja kommentoida niitä, sekä olla yhteydessä ystäviinsä. Paikkatiedon hyödyntäminen erottaa geososiaaliset verkostopalvelut mobiileista sosiaalisista verkostopalveluista (Souza & Frith, 2010). Nykyään termien välille on kuitenkin hieman hankalaa tehdä selkeää eroa, sillä monissa mobiileissa sosiaalisissa verkostopalveluissa on mahdollista hyödyntää paikkatietoa. Esimerkiksi Twitterin mobiilisovellus voidaan nähdä mobiilina sosiaalisena verkostopalveluna, mutta toisaalta myös geososiaalisena verkostopalveluna, sillä sen käyttäjien on mahdollista halutessaan jakaa sijaintinsa kartalla.

Sekä geososiaalisissa verkostopalveluissa, että mobiileissa sosiaalisissa verkostopalveluissa voidaan Taulukon 1 palikoista nähdä painottuvan erityisesti läsnäolo, sillä kuten aiemmin todettiin, on palveluille ominaista, että ne ovat käyttäjilleen jatkuvasti läsnä. Palvelusta riippuen palikat painottuvat hieman eri tavoin. Esimerkiksi Twitterissä keskeinen toiminnallisuus on käyttäjien välillä käydyt keskustelut, kun taas Facebookissa olennaisinta on käyttäjien väliset suhteet. Molemmat palvelut voidaan kuitenkin nähdä mobiileina sosiaalisina verkostopalveluina ja toisaalta paikkatietoa hyödynnettäessä myös geososiaalisina verkostopalveluina. Taulukon 1 rakennuspalikat on tarkoitettu kuvaamaan erityisesti tavallisen sosiaalisen median toimintoja, eivätkä ne näin ollen täysin sovellu mobiilien tai paikkatietoa hyödyntävien palveluiden jaotteluun. Kietzmannin ym. (2011) rakennuspalikat eivät esimerkiksi suoraan viittaa paikkatiedon hyödyntämiseen.

3 YKSITYISYYS

Tässä luvussa tarkastellaan ensin yksityisyyden eri määritelmiä, sen käsittämistä eri aikoina ja sen saralla tehtyä tutkimusta eri tieteenalojen piirissä. Myöhemmin tutkielman teeman mukaisesti tarkastelun keskiössä ovat erityisesti informaation yksityisyys online-ympäristöissä, yksityisyys tietojärjestelmätieteessä ja yksityisyys geososiaalisissa verkostopalveluissa.

3.1 Käsitykset yksityisyydestä ja aiempi tutkimus

Yksityisyyden määritteleminen ei ole yksioikoista. Warren ja Brandeis (1890) määrittelivät sen aikanaan oikeudeksi tulla jätetyksi rauhaan. Sittemmin käsitteelle on esitetty lukuisia erilaisia määritelmiä. Yhdistyneiden kansakuntien ihmisoikeuksien yleismaailmallisen julistuksen 12. Artiklassa viitataan yksityisyyteen seuraavasti: ”Älköön mielivaltaisesti puututtako kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon älköönkä loukattako kenenkään kunniaa ja mainetta. Jokaisella on oikeus lain suojaan sellaista puuttumista tai loukkausta vastaan” (Yhdistyneet kansakunnat, 1948). Yhdistyneiden kansakuntien mukaan yksityisyys voidaan siis nähdä *puuttumattomuutena,* eli ihmisillä tulisi olla oikeus siihen, ettei heidän elämäänsä puututa. Näin ollen Warrenin ja Brandeisin (1890), sekä Yhdistyneiden kansakuntien (1948) näkemykset yksityisyydestä voidaan nähdä melko samankaltaisina.

Eri aikoina yksityisyyden määrittelyssä on korostettu erilaisia teemoja. Warrenin ja Brandeisin (1890) mukaan yksityisyys oli nähty pitkään eritoten omaisuuden yksityisyytenä ja he halusivat korostaa yksityisyyttä median ja yksilön suhteessa; huolta aiheuttivat esimerkiksi yksittäisistä henkilöistä lehdistössä julkaistut valokuvat. Myöhemmin määritelmissä on korostettu esimerkiksi valtioiden ja yksityisten yritysten osuutta ja erityisesti niiden valtuuksia kerätä tietoja yksittäisistä henkilöistä (Emerson, 1979). Yksityisyys aiheena on herättänyt kiinnostusta laajemminkin eri tieteenalojen keskuudessa ja sitä on tarkasteltu muiden muassa oikeustieteen (esim. Gavisont, 1980) lääketieteen (esim. Gellman, 1984) ja markkinoinnin (esim. Wang ym., 1998) näkökulmista.

Oikeustieteen alalla yksityisyyttä on tutkittu erityisesti lainopillisesta näkökulmasta. Gavisont (1980) ei tarjoa yksityisyydelle tarkkaa määritelmää, vaan pyrkii kuvaamaan sille ominaisia piirteitä, joina hän näkee muun muassa yksilöstä kerätyn informaation, yksilöön kiinnitetyn huomion ja fyysisen koskemattomuuden. Parent (1983) puolestaan ymmärtää yksityisyyden tilana, jossa yksilön henkilökohtaisia ja arkaluontoisia tietoja ei ole muiden hallussa. Näin ollen hän näkeekin yksityisyyden piiriin kuuluvan tiedon aikaan sidottuna, eli aikaisemmin henkilökohtaisena ja arkaluontoisena koettua tietoa saatetaan myöhemmin jakaa huolettomasti. Esimerkiksi parisuhdestatus saatetaan suhteen alussa pyrkiä pitämään yksityisenä, mutta myöhemmin asiaa ei välttämättä ole enää tarpeen salata.

Lääketieteen saralla yksityisyyttä on tutkittu potilaiden informaation yksityisyyden näkökulmasta. Keskiössä on erityisesti lääkäreiden vaitiolovelvollisuus, joka Gellmanin (1984) mukaan on jo aikojen alusta nähty eräänä tärkeimpänä luottamusta ylläpitävänä elementtinä potilaiden ja lääkäreiden välisessä suhteessa. Gellman (1984) toteaa myös yksityisyyden merkityksen korostuvan tulevaisuudessa entisestään, sillä potilaista kerätään yhä enemmän ja yksityiskohtaisempaa tietoa. Yksityisyyteen on kiinnitetty huomiota myös lääketieteellisen tutkimuksen parissa. Tutkimuksissa käytetyn potilasdatan tulee olla sellaista, että sen perusteella ei voida tunnistaa yksittäisiä henkilöitä. Datan saattaminen täysin anonyymiin muotoon on kuitenkin hankalaa (Ohno-Machado, Silveira, & Vinterbo, 2004).

Tämän tutkielman kannalta ehkä kiinnostavampaa on kuitenkin markkinoinnin saralla tehty yksityisyydentutkimus, jossa oleellista on erityisesti kuluttajien yksityisyys. Kuluttajien huoli yksityisyydestään alkoi herätä sitä mukaa, kun yritykset ryhtyivät kasvavissa määrin keräämään tietoa asiakkaistaan. Tämän voidaan nähdä tapahtuneen Internetin yleistymisen myötä (Cambell, 1997; Culnan & Bies, 2003; Wang ym., 1998). Siitä lähtien aiheeseen onkin kiinnitetty paljon huomiota niin julkisessa, kuin tieteellisessä keskustelussa. Keskustelun näkökulmat voidaan Culnanin ja Biesin (2003) mukaan jakaa karkeasti kolmeen ryhmään: yritys-, aktivisti- ja keskustanäkökulmaan. Yritysnäkökulman mukaan yritysten pääsyä kuluttajien tietoihin ei tule rajoittaa, sillä rajoittaminen hankaloittaisi niiden liiketoimintaa ja näin vaarantaisi niiden perimmäisen tarkoituksen, eli yhteiskunnan kehittämisen ja talouskasvun luomisen. Aktivistinäkökulmasta tietojen esteetön kerääminen aiheuttaa uhkia kuluttajien yksityisyydelle, sillä kerätty tieto olisi tällöin kaikkien saatavilla. Keskustanäkökulma puolestaan pyrkii asettumaan edellä mainittujen väliin, eli vaikka siinä tiedostetaankin yritysten tarve kerätä tietoa, tulee keräystä kuitenkin säädellä esimerkiksi lainsäädännön keinoin. (Culnan & Bies, 2003.)

Yksityisyys on siis herättänyt kiinnostusta eri tieteenalojen piirissä ja se on myös koettu eri tavoin eri aikoina. Siinä missä Warren ja Brandeis vuonna 1890 korostivat erityisesti oikeutta tulla jätetyksi rauhaan fyysisessä maailmassa, oli Emersonin (1979) mukaan mielekkäämpää tarkastella ihmisistä kerättävän informaation yksityisyyttä. Gavisontin (1980) näkemys pitää sisällään Warrenilta ja Brandeisilta, sekä Emersonilta tuttuja ajatuksia; yksityisyyttä voidaan tarkastella niin fyysisen maailman koskemattomuutena, kuin kerätyn tiedon yksityisyytenä. Edellä mainittuihin verrattuna esimerkiksi Gellman (1984) puolestaan

tarkastelee yksityisyyttä tiukemmin oman alansa kontekstissa; siinä missä Warren ja Brandeis aiemmin, sekä Emerson myöhemmin tarkastelevat yksityisyyttä yleisellä tasolla, keskittyy Gellman erityisesti siihen, miten käsite näyttäytyy lääketieteessä. Kirjallisuuskatsauksen perusteella vaikuttaa siltä, että eri tieteenaloilla kiinnostuttiin yksityisyyden käsitteestä laajemmin vasta 1900-luvun puolen välin jälkeen; sitä ennen käsitettä tarkasteltiin lähinnä yhteiskuntatieteellisestä ja filosofisesta näkökulmasta. Myöhemmin eri alat lääketieteestä markkinointiin kiinnostuivat siitä, millaisena käsite kunkin alan näkökulmasta näyttäytyy. Vaikka eri näkökulmat korostavat yksityisyyden eri osa-alueita, voidaan Warrenin ja Brandeisin (1890) toteamuksen oikeudesta tulla jätetyksi rauhaan nähdä kiteyttävän yksityisyyden merkityksen; oli kyse sitten informaatiosta yleensä, potilaskertomuksista, asiakastiedoista tai fyysisestä maailmasta, on yksityisyydessä pohjimmiltaan kyse siitä, ettei ihmisen yksityiselämään tämän tahtomatta puututa.

Tämän tutkielman kannalta relevanteinta tutkimusta on kuitenkin tietojärjestelmätieteen parissa tehty tutkimus. Seuraavaksi tarkastellaan, kuinka yksityisyyttä on käsitelty tietojärjestelmätieteen piirissä. Tietojärjestelmätieteessä keskeinen käsite on informaation yksityisyys. Käsite on tietojärjestelmätieteelle ominainen, vaikka käytännössä samasta asiasta puhutaan eri aloilla eri termeillä. Esimerkiksi Gellman (1980) tarkasteli yksityisyyttä lääkärin vaitiolovelvollisuuden näkökulmasta, mutta tarkasteluun liittyivät olennaisesti potilaskertomusten, eli potilaista kerätyn informaation yksityisyys. Näin ollen myös Gellmanin voidaan nähdä puhuneen informaation yksityisyydestä.

3.2 Yksityisyys tietojärjestelmätieteessä

Tietojärjestelmätieteessä yksityisyyttä tarkastellaan tyypillisesti informaation yksityisyytenä. Käsitteenä informaation yksityisyys on tunnettu jo kauan ennen informaatioteknologian kehittymistä (Bélanger & Crossler, 2011). Internetin yleistymisen myötä keskiöön nousi myös informaation yksityisyys online-ympäristöissä (O'Neil, 2001). Tieteelliselle keskustelulle ominaisesti myös informaation yksityisyydelle on vuosien saatossa esitetty monia määritelmiä. Bélangerin, Hillerin ja Smithin (2002) mukaan se voidaan nähdä yksilön kontrollina itseään koskevan informaation toissijaiseen käyttöön. Toissijaisella käytöllä Bélanger, ym. (2002) viittaavat informaation hyödyntämiseen johonkin muuhun kuin alkuperäiseen tarkoitukseen. Esimerkiksi Web-sivustoille rekisteröidyttäessä käyttäjien tulee usein luovuttaa henkilökohtaisia tietoja itsestään. Mikäli palveluntarjoaja myy tai muuten jakaa nämä tiedot kolmansille osapuolille, puhutaan informaation toissijaisesta käytöstä.

Clarke (1999) puolestaan määrittelee informaation yksityisyyden kiinnostuksena, joka yksilöllä on kontrolloida tai ainakin merkittävästi vaikuttaa itseään koskevan datan käsittelyyn. Tätä kiinnostusta on tietojärjestelmätieteen parissa tutkittu laajemminkin; Bélangerin ja Crosslerin (2011) mukaan suurin osa alalla tehdystä yksityisyyteen liittyvästä tutkimuksesta tarkastelee erilaisia in-

formaation yksityisyyteen liittyviä huolenaiheita (information privacy concerns), yksityisyyteen liittyviä asenteita ja yksityisyyden vaikutuksia sähköiseen liiketoimintaan.

Huolenaiheita on useiden tutkimusten avulla tunnistettu monia. Smith, Milberg ja Burke (1996) esittelivät CFIP-mallin (Concern For Information Privacy), jonka mukaan he jakavat informaation yksityisyyteen liittyvät huolenaiheet neljään ulottuvuuteen: datan keräämiseen, sen luvattomaan toissijaiseen käyttöön, sopimattomaan pääsyyn ja virheisiin:

- Datan keräämisen liittyvä huoli viittaa ajatukseen, että henkilökohtaisia tietoja kerätään ja tallennetaan liikaa.
- Huoli luvattomasta toissijaisesta käytöstä tarkoittaa ajatusta siitä, että kerättyjä henkilökohtaisia tietoja hyödynnetään luvatta johonkin muuhun kuin alkuperäiseen tarkoitukseen.
- Sopimaton pääsy puolestaan viittaa huoleen informaation liian helposta saatavuudesta myös niille, jotka eivät ole sen hyödyntämiseen valtuutettuja.
- Huoli virheistä syntyy ajatuksesta, että kerättyä dataa ei suojella tarpeeksi mahdollisilta tahallisilta ja tahattomilta yksityisyyden vaarantavilta virheiltä.

Myöhemmin informaation yksityisyyteen liittyviä huolenaiheita on tarkasteltu esimerkiksi IUIPC –mallin (Internet Users' Information Privacy Concerns) mukaisesti (Malhotra, Kim, & Agarwal, 2004). Mallissa huolenaiheita jäsennetään kolmen ulottuvuuden mukaan, joita ovat keruu, kontrolli ja tietoisuus.

- Keruu (Collection) viittaa yksilön huoleen hänestä kerätyn tiedon määrästä.
- Kontrolli (Control) puolestaan viittaa yksilölle mahdollisuuteen vaikuttaa tietojen keruuseen.
- Tietoisuus (Awareness) käsittää yksilön ymmärryksen siitä, että henkilökohtaisia tietoja ylipäänsä kerätään.

Vaikka Smithin ym. (1996) ja Malhotran ym. (2004) mallit ovat keskenään melko samankaltaisia, on myös eroja havaittavissa. Smithin ym. malli lähestyy yksityisyyttä erityisesti organisatorisesta näkökulmasta, kun taas Malhotran ym. mallissa yksilöt ovat tarkastelun keskiössä. Lisäksi Malhotran ym. mallin ollessa Smithin ym. mallia monta vuotta tuoreempi, ottaa se Internetin yleistymisen myötä myös enemmän kantaa yksityisyyshuoliin online-ympäristössä.

Informaation yksityisyyteen liittyviä asenteita kartoittavat tutkimukset tarkastelevat tyypillisesti ihmisten suhtautumista informaation yksityisyyskäytänteisiin (Bélanger & Crossler, 2011). Tutkimuksessa asenteita on tarkasteltu monesta eri näkökulmasta, kuten käyttäjien asenteena Facebookin tietosuojaa kohtaan (Debatin ym., 2009), kulttuurin vaikutuksena asenteisiin (Lowry, Cao, & Everard, 2011) ja kuluttajien suhtautumisena RFID-teknologiaan (Razzouk, Seitz, & Nicolaou, 2008). Tutkimuksessa pyritään tyypillisesti etsimään tietyn-

laisiin asenteisiin ja käytökseen johtavia tekijöitä, joita voivat olla esimerkiksi kulttuuri, aiemmat kokemukset, muiden mielipiteet, tietämättömyys tai välinpitämättömyys.

Kuluttajien yksityisyysnäkemysten vaikutus heidän valmiuteensa ostaa tuotteita verkosta on eräs tyypillisimmistä tutkimuskohteista tutkittaessa yksityisyyden vaikutuksia elektroniseen liiketoimintaan. Lisäksi tutkimus keskittyy usein kuluttajien halukkuuteen jakaa tietojaan yritysten kanssa ja siihen liittyviin eroihin valtioiden välillä. Suurin osa tutkimuksista viittaa siihen, että mikäli käyttäjät ovat huolissaan yksityisyydestään, heidän mielenkiintonsa ostaa tuotteita Internetistä laskee. Toisaalta osa tutkimuksista kuitenkin viittaa siihen, että yksityisyyshuolilla ei ole juurikaan vaikutusta kuluttajien käyttäytymiseen. (Bélanger & Crossler, 2011.)

3.3 Informaation yksityisyys online-ympäristöissä

Kuten aiemmissa kappaleissa on havaittu, yksityisyys on käsitteenä laaja ja eri tieteenaloilla on tehty paljon tutkimusta sen parissa. Käsitteen määritelmät vaihtelevat sekä aikakauden, tieteenalan, että tutkijan myötä ja sitä on käsitelty monesta eri näkökulmasta. Tämän tutkielman kannalta oleellinen näkökulma informaation yksityisyyden lisäksi on yksityisyys online-ympäristöissä, johon eri julkaisuissa viitataan tyypillisesti käsitteillä online-yksityisyys (esim. Nissenbaum, 2011), Web-yksityisyys (esim. Gritzalis, 2004) ja Internet-yksityisyys (esim. Cranor, 1999; Miyazaki & Fernandez, 2000). Tässä tutkielmassa edellä mainittuihin viitataan käsitteellä 'yksityisyys online-ympäristöissä'. Informaation yksityisyys on viime vuosikymmeninä kiinnostanut tutkijoita laajalti. Se on ollut eräitä online-palveluiden käyttäjien suurimmista huolenaiheista (Wang, Lee, & Wang, 1998; O'Neil, 2001; Sheehan, 2002; Yao, Rice, & Wallis, 2007).

Cranorin (1999) mukaan yksityisyys on pitkään ollut arkaluontoinen aihe, mutta internetin yleistymisen myötä siitä on tullut aiempaankin tärkeämpi, sillä internet on mahdollistanut uudenlaisen tavan kerätä dataa nopeasti ja suuria määriä. Internetin myötä myös käyttäjiin liittyvän informaation määrä on kasvanut ja Nissenbaumin (2011) mukaan internetin käytöstä kertyykin käyttäjäkohtaista informaatiota muiden muassa evästeiden (cookies), latenssien, klikkausten, ip-osoitteiden, sosiaalisiin suhteisiin liittyvän grafiikan ja selaushistorian muodossa. Ennen internetiä kyseistä informaatiota ei ollut edes olemassa, eikä se näin ollen voinut olla uhka yksityisyydelle.

Yaon ym. (2007) mukaan lähes kaikkia yksityisyyttä online-ympäristöissä tarkastelevia tutkimuksia yhdistää ajatus käyttäjiin liittyvän informaation kontrolloitavuudesta, eli käyttäjillä itsellään tulisi olla mahdollisuus päättää siitä, miten heihin liittyvää tietoa käsitellään. Tässä mielessä yksityisyyteen online-ympäristöissä pätevät samat määritelmät, kuin informaation yksityisyyteen yleensä. Rezgui, Bouguettaya ja Eltoweissy (2003) näkevätkin yksityisyyden online-ympäristöissä käyttäjien oikeutena salata heitä koskeva henkilökohtainen informaatio ja lisäksi mahdollisuutena jonkinasteiseen kontrolliin muille

tahoille jakamansa informaation käyttöön. Lisäksi Rezgui ym. jakavat yksityisyyden online-ympäristöissä kahdeksaan ulottuvuuteen, joiden yhteydessä he esittävät yksityisyyteen liittyviä vaatimuksia ja ehdotuksia ulottuvuuksien suhteen. Ulottuvuuksia ovat: informaation keruu, käyttö, varastointi, ilmitulo, turvallisuus, pääsyn kontrolli, valvonta ja käytäntöjen muutokset.

- Informaation keruu viittaa tapoihin kerätä informaatiota käyttäjistä. Sitä ei tule tehdä käyttäjien tietämättä tai ilman heidän suostumustaan.
- Informaation käyttö viittaa niihin tapoihin, jolla kerättyä informaatiota käytetään. Keräävä taho voi esimerkiksi ilmoittaa, mitä kerätyllä tiedolla tehdään.
- Informaation varastointi viittaa siihen, että käyttäjien tulisi tietää varastoidaanko kerättyä tietoa ja mikäli varastoidaan, kuinka kauan sitä säilytetään.
- Informaation ilmitulo viittaa siihen, voiko informaatiota keräävä taho jakaa kerättyä informaatiota muille ja mikäli voi, niin kenelle.
- Informaation turvallisuus puolestaan viittaa kykyyn ja tapoihin suojella kerättyä informaatiota.
- Pääsyn kontrolli tarkoittaa niitä käytänteitä, joilla pääsyä kerättyyn informaatioon rajoitetaan. Tietosuojakäytänteissä tulee määritellä, kenellä on pääsy mihinkin tietoon.
- Valvonta viittaa tapoihin valvoa kerätyn informaation käyttöä; informaatiota keräävän tahon tulee tietää, mitä informaatiolla tehdään.
- Käytäntöjen muutokset puolestaan viittaavat siihen, että tietosuojakäytäntöjen muutokset eivät saa vaikuttaa jo aiemmin kerätyn informaation käyttöön.

Rezguin ym. (2003) ulottuvuudet ja Malhotran ym. (2004) IUIPC-malli sisältävät osittain samoja ajatuksia, kuin Smithin ym. (1996) CFIP-malli, vaikka CFIP-malli käsitteleekin informaation yksityisyyteen liittyviä huolenaiheita, IUIPC informaation yksityisyyden huolenaiheita internetissä ja Rezgui ym. yksityisyyttä online-ympäristöissä käsitteenä. Kaikkien ajatusten keskiössä on informaation keruu ja tavat käyttää sitä, vaikka Rezgui ym. ja Malhotra ym. käsittelevät erityisesti online-ympäristöjä ja Smith ym. informaatiota yleensä.

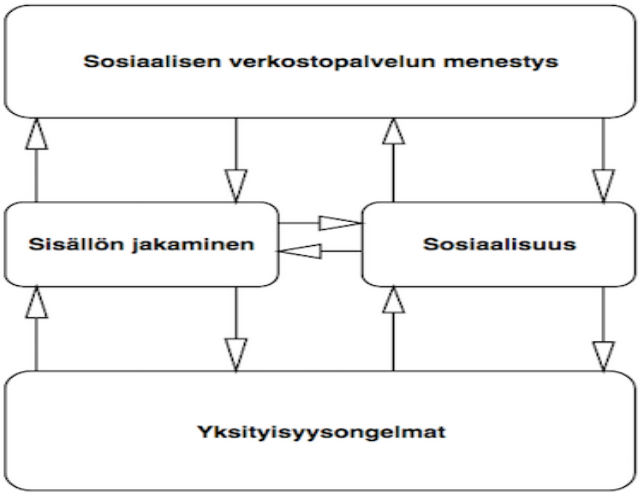
Vaikka Rezguin ym. (2003), Malhotran ym. (2004) ja Smithin ym. (1996) ajatukset ovat saman tyyppisiä, ovat ne selkeästi aikansa tuotteita. Kaikissa julkaisuissa esitetään esimerkiksi viittauksia datan ja informaation keräyksen, käyttöön ja tallennukseen, mutta vain Rezgui ym ja Malhotra ym. mainitsevat selkeästi online-ympäristöt. Tässä mielessä voidaan havaita, että Smithin ym. julkaisun ilmestyessä internet oli vasta yleistymässä, kun taas Rezguin ym. ja Malhotran ym. julkaisujen aikaan se oli isolle osalle varsinkin länsimaalaisista jo arkipäivää.

Rezqui ym. (2003) ja Smith ym. (1996) tarkastelevat yksityisyyttä erityisesti informaatiota keräävän ja varastoivan tahon näkökulmasta. Vähemmälle huomiolle jää käyttäjien oman toiminnan, kuten vapaaehtoisen tietojen luovuttami-

sen vaikutus. Malhotra ym. (2004) toteavat myös käyttäjän tietoisuuden merkittävänä tekijänä. Käyttäjien luodessa profiileja ja paljastaessaan tietojaan sosiaaliseen mediaan, on yksityisyysongelmien uhka läsnä (Rosenblum, 2007). Ongelmaa pahentaa se, että suurin osa käyttäjistä ei ole kiinnostunut yksityisyydestään (Madden, 2012).

Yksityisyysongelmat voidaan Rosenblumin (2007) mukaan karkeasti jakaa kahteen osaan; sisäisiin ja ulkoisiin ongelmiin. Sisäisillä ongelmilla Rosenblum (2007) viittaa käyttäjästä itsestään johtuviin ongelmiin, joita ovat esimerkiksi liiallinen arkaluontoisen tiedon paljastaminen. Lisäksi sisäisiin ongelmiin liittyy käyttäjien heikko ymmärrys julkistetun informaation pysyvyydestä; siinä missä kasvotusten käydystä keskustelusta ei jää mitään jälkiä, ellei sitä erikseen tallenneta, jää sosiaaliseen mediaan jaettu informaatio muiden saataville ja tallennettavaksi. Ulkoisilla ongelmilla Rosenblum (2007) puolestaan viittaa ulkoisten toimijoiden, kuten muiden käyttäjien tai yritysten toimintaan. Sosiaalinen media mahdollistaa esimerkiksi muiden käyttäjien, kuten tulevien työnantajien, tarkastella yksittäisen käyttäjän henkilökohtaisia tietoja ja aiempaa käyttäytymistä verkossa. Lisäksi sosiaalisen median palveluita ylläpitävien yritysten on mahdollista myydä tietoja käyttäjistään eteenpäin.

Luvussa 2.1 todettiin sosiaalisessa mediassa tyypillisesti olevan kyse osallistumisesta, vuorovaikutuksesta ja jakamisesta. Lisäksi onnistuneiden sosiaalisten medioiden mainittiin olevan helppokäyttöisiä, luotettavia ja helposti ymmärrettäviä. Samojen periaatteiden voidaan nähdä koskevan myös sosiaalisia verkostopalveluja. Brandtzægin, Lüdersin, ja Skjetnen (2010) mukaan menestyneet sosiaaliset verkostopalvelut lisäksi rohkaisevat käyttäjiään julkaisemaan itsestään mahdollisimman paljon tietoa, mikä puolestaan aiheuttaa kuviossa 1 havainnollistettavan yksityisyysdilemman; ihmisiä rohkaistaan julkaisemaan itsestään mahdollisimman paljon tietoa, mutta samalla yhä kasvavan määrän tietoa on mahdollista joutua vääriin käsiin.



KUVIO 1 Sosiaalisten verkostopalveluiden yksityisyysdilemma (Brandzæg ym., 2010, 1010)

3.4 Yksityisyys geososiaalisissa verkostopalveluissa

Edellisessä luvussa käsiteltiin informaation yksityisyyttä erityisesti online-ympäristöissä. Keskeisenä ajatuksena on, että ihmisillä tulisi siis olla mahdollisuus kontrolloida itseään koskevaa informaatiota (Yao. ym., 2007). Aiemmin osoitetun mukaisesti geososiaaliset verkostopalvelut ovat osa sosiaalista mediaa, joka puolestaan Kietzmannin ym. (2011) sekä Kaplanin & Haenlainin (2010) mukaan pohjautuu WEB 2.0 teknologioihin. Näin ollen voidaan siis todeta, että geososiaaliset verkostopalvelut ovat online-ympäristöjä ja siten niiden yksityisyyteen pätee myös aiemmin esitelty online-ympäristöjen informaation yksityisyyden määritelmä.

Paikkatiedon hyödyntämisen ollessa geososiaalisten verkostopalvelujen keskiössä (Roick & Heuser, 2013), on tämän tutkielman kannalta kiinnostavinta tarkastella yksityisyyttä erityisesti paikkatiedon yksityisyyden näkökulmasta. Paikkatieto voidaan Wun Ja Schulzrinnen (2005) mukaan jakaa kahteen alakategoriaan, sijaintitietoon ja attribuuttitietoon. Sijaintitieto viittaa tietoon siitä, missä jokin sijaitsee. Esimerkiksi Jyväskylän sijaintitiedoksi voidaan todeta Keski-Suomi. Attribuuttitieto puolestaan viittaa tietoon siitä, mitä jossakin on. Jyväskylä, monien muiden kaupunkien tavoin, on osa Keski-Suomen attribuuttitietoa.

Paikkatiedon yksityisyyttä voidaan kuvata jakamalla se kahteen alakäsitteeseen: paikallaolon yksityisyyteen (location privacy) ja poissaolon yksityisyyteen (absence privacy) (Freni, Ruiz Vicente, Mascetti, Bettini, & Jensen, 2010). Ensin mainittu viittaa Frenin ym., (2010) mukaan tietoon siitä, että henkilö X on paikassa Y tiettynä aikana ja jälkimmäinen taas tietoon siitä, että henkilö X ei ole paikassa Y. Toisin sanoen, mikäli vihamielinen taho tietää, että geososiaalisen verkostopalvelun käyttäjä on sairaalassa, on hänen paikallaolon yksityisyytensä uhattuna. Samalla voidaan myös päätellä, ettei hän ole kotona, jolloin hänen poissaolonsa yksityisyys puolestaan vaarantuu. Myöhemmin kuvausta on tarkennettu lisäämällä myös yhteisen paikkatiedon (co-location) yksityisyyden ja identiteetin (identity) yksityisyyden käsitteet. Yhteisen paikkatiedon yksityisyydellä tarkoitetaan tietoa siitä, että henkilöt X ja Y ovat paikassa P samaan aikaan. Identiteetin yksityisyys puolestaan viittaa tietoon siitä, että henkilö X on jonkin tietyn geososiaalisen verkostopalvelun käyttäjä (Ruiz Vicente, Freni, Bettini, & Jensen, 2011).

Seuraavassa kappaleessa tarkastellaan ensin geososiaalisten verkostopalvelujen toimintaa kolmen eri tyyppiesimerkin avulla ja myöhemmin palveluihin liittyviä yksityisyysongelmia ja ongelmien syitä. Kappaleessa pyritään saamaan vastaus tutkimusongelmaan: *minkälaisia yksityisyysongelmia geososiaalisten verkostopalveluiden käyttöön liittyy?*

4 YKSITYISYYSONGELMAT GEOSOSIAALISISSA VERKOSTOPALVELUISSA

Geososiaalisten verkostopalvelujen kasvattaessa suosiotaan jatkuvasti, lisääntyy myös niiden potentiaalisesti kerättävissä olevan informaation määrä. Kuten aiemmin Najaflouta ym. (2013) mukaillen todettiin, poikkeavat mobiilin sosiaalisen median sovellukset perinteisestä sosiaalisesta mediasta siten, että ne ovat käyttäjilleen jatkuvasti läsnä. Jatkuvan läsnäolon myötä käyttäjäkohtaista informaatiota syntyy paitsi enemmän, on se myös tarkempaa. Paikkatiedon keräämisen mahdollistumisen myötä on palveluntarjoajille avautunut uusi ikkuna käyttäjien yksityiselämään. Siinä missä kerätty tieto vielä sosiaalisen median alkuvuosina oli staattista, sisältäen useimmiten esimerkiksi käyttäjän nimen ja kansalaisuuden, on se paikkatiedon keräämisen myötä muuttunut dynaamiseksi; nimen lisäksi tietoa voidaan kerätä myös käyttäjien liikkeistä.

Paikkatiedon kerääminen on monille tervetullut ominaisuus, mistä kielii geososiaalisten verkostopalvelujen yhä kasvava suosio. Yhä tarkemman käyttäjäkohtaisen informaation keruu kuitenkin mahdollistaa myös uudenlaiset uhat käyttäjien yksityisyydelle. Käyttäjät eivät kuitenkaan erinäisistä syistä ole välttämättä tietoisia näistä ongelmista. Tässä kappaleessa tarkastellaan ensin tyyppiesimerkkejä geososiaalisista verkostopalveluista ja myöhemmin niihin liittyviä yksityisyysongelmia käyttäjien näkökulmasta. Lisäksi selvitetään ongelmien tyypillisimpiä syitä.

4.1 Tyyppiesimerkit

Kuten johdantokappaleessa mainittiin, ovat Facebook ja Twitter suosituimpia länsimaissa käytettyjä sosiaalisia verkostopalveluja. Valtaosa palveluiden käyttäjistä käyttää niitä jonkin mobiililaitteen avulla ja suurin osa mobiililaitteista sisältää jonkinlaista paikkatiedon keräämisen mahdollistavaa teknologiaa. Näin ollen ei ole lainkaan yllättävää, että käyttäjien on mahdollista jakaa tietoja sijainnistaan niin Facebookiin kuin Twitteriinkin. Facebook ja Twitter eivät kuitenkaan alun perin pohjautuneet paikkatiedon jakamiseen, vaan omaksuivat

toiminnallisuuden hieman myöhemmin. Alun perin paikkatiedon hyödyntämisen ympärille syntyneistä sovelluksista tunnetuin lienee Foursquare, joka nykyisin tunnetaan nimellä Swarm. Tyyppiesimerkeiksi on valittu neljä paikkatietoa hyödyntävää palvelua joista kolme, eli Facebook, Twitter ja Foursquare/Swarm ovat maailmanlaajuisesti tunnettuja. Neljäs esimerkki, Jodel, puolestaan ei ole maailmalla kovinkaan tunnettu, mutta sen tarkastelu nähtiin mielekkäänä, sillä ainakin Jyväskylässä sillä on vankka käyttäjäkunta.

Aiemmin viitattiin Wun ja Schulzrinnen (2005) ajatukseen paikkatiedon sisällöstä; se koostuu sijainti- ja attribuuttitiedosta. Tyyppiesimerkeistä Foursquare ja Facebookin Paikat –toiminto hyödyntävät niin sijaintietoa, kuin attribuuttitietoa. Molempien avulla on mahdollista tarkastella erilaisten paikkojen sijainteja ja toisaalta käyttäjät voivat ilmoittautua läsnä olevaksi kyseisiin paikkoihin. Jodel ja Twitterin Paikat –toiminto puolestaan hyödyntävät ainoastaan sijaintitietoa; niiden avulla käyttäjän on mahdollista ilmoittaa sijaintinsa, mutta sijaintiin liittyvä attribuuttitieto, eli mitä kyseisessä sijainnissa on, ei käy suoraan ilmi. Paikallistuntemuksen avulla sekin tosin on muiden käyttäjien pääteltävissä.

4.1.1 Foursquare & Swarm

Ehkä kaikista tunnetuin paikkatiedon jakamisen ympärille syntynyt geososiaalinen verkostopalvelu on Foursquare. Se oli mobiilisovellus, jonka avulla käyttäjät voivat olla yhteydessä toisiinsa, jakaa tietoa sijainnistaan ja saada tietoa muiden käyttäjien sijainnista. Sijaintitiedon jakaminen tapahtui siten, että käyttäjät ilmoittautuivat läsnä oleviksi (Check-in) haluamiinsa ennalta määriteltyihin todellisen maailman paikkoihin (venues), kuten museoihin, ravintoloihin tai kahviloihin. He voivat esimerkiksi tietyssä kahvilassa ollessaan ilmoittaa muille käyttäjille, että olivat kyseisessä paikassa juuri tietyllä hetkellä ja toisaalta seurata, missä muut käyttäjät sijaitsivat. Paikkatiedon jakamiseen oli lisätty myös kilpailullinen elementti; mikäli käyttäjä ilmoittautui läsnä olevaksi tiettyyn paikkaan useammin kuin kukaan muu, hän sai kyseiseen sijaintiin liittyvän pormestari (mayor) -statuksen. (Lindqvist, Cranshaw, Wiese, Hong, & Zimmerman, 2011).

Käyttäjien paikannus tapahtui tukiasemien, lähellä olevien Wifi-verkkojen ja GPS:n avulla. Hiljalleen Foursquaren toiminta laajeni kattamaan myös erilaisten kohteiden, kuten ravintoloiden arviointeja. Vuonna 2014 yhtiö päätti jatkaa paikkojen arvioihin keskittyvää sovellusta nimellä Foursquare ja jatkaa sovelluksen alkuperäistä ideaa uudessa Swarm-nimisessä sovelluksessa. (Popper & Hamburger, 2014).

Foursquaren ollessa geososiaalisista verkostopalveluista tunnetuin, on sen parissa tehty myös tyyppiesimerkeistä eniten paikkatiedon ympärille keskittyvää tutkimusta. Tutkimusaiheina ovat olleet muiden muassa paikkatiedon väärentäminen (esim. Carbunar & Potharaju, 2012; He, Liu, & Ren, 2011), palvelun käytön syyt (esim. Lindqvist ym., 2011) ja käyttäjien paikkatiedon ennustaminen Foursquaren avulla (esim. Pontes, Vasconcelos, Almeida, Kumaraguru, & Almeida, 2012).

4.1.2 Facebook & Twitter

Facebook ja Twitter eivät kumpikaan alun alkaen perustuneet paikkatiedon hyödyntämiseen, vaan omaksuivat toiminnallisuuden vasta hieman myöhemmin. Edelleenkään paikkatiedon hyödyntäminen ei ole niiden käytön keskiössä, vaan se voidaan nähdä yhtenä niihin kuuluvista ominaisuuksista.

Facebook esitteli Paikat –toimintonsa vuonna 2010. Toiminnon avulla käyttäjät voivat Foursquaren tavoin ilmoittautua läsnä oleviksi haluamiinsa, ennalta määriteltyihin paikkoihin (Gross & Hanna, 2010). Twitter puolestaan mahdollisti oman sijainnin koordinaattien jakamisen muille käyttäjille vuonna 2009 (Stone, 2009) ja esitteli seuraavana vuonna Facebookin Paikat –toimintoa vastaavan Twitter Places –toiminnon (Laraki, 2010). Facebookin ja Twitterin Paikat –toiminnot olivat alun perin melko samankaltaisia, mutta sittemmin Facebook on lisännyt Paikat –toimintoonsa erilaisia toiminnallisuuksia. Molempien ajatuksena oli antaa käyttäjille mahdollisuus ilmoittautua läsnä oleviksi tiettyihin paikkoihin, mutta Facebook on myöhemmin lisännyt mahdollisuuden esimerkiksi arvostella ja kommentoida paikkoja, etsiä uusia paikkoja ja tarkastaa niiden aukiolo. Vuonna 2014 Facebook toi mobiilisovellukseensa Lähellä olevat kaverit –toiminnon. Toiminnon avulla käyttäjien on mahdollista nähdä toistensa fyysinen sijainti reaaliajassa, sen sijaan että he erikseen ilmoittautuisivat läsnä oleviksi tiettyihin paikkoihin (Kelly, 2014).

Facebookin ja Twitterin yksityisyyteen liittyen on tehty melko paljon tutkimusta, mutta niissä hyödynnettävän paikkatiedon käsittely on jäänyt vähemmälle. Facebookin paikkatietoon liittyvä tutkimus käsittelee esimerkiksi erilaisia paikkatietoon liittyviä hyökkäyksiä (esim. Wernke, Skvortsov, Dürr, & Rothermel, 2012) ja käyttäjien mahdollisuuksia rajoittaa muiden pääsyä omaan paikkatietoonsa (esim. Jin, Long, Joshi, & Anwar, 2012). Tyypillisesti Facebookia käsittelevät julkaisut eivät kuitenkaan keskity yksinomaan Facebookiin, vaan käyttävät sitä yhtenä esimerkeistä.

Twitterin suhteen paikkatiedon tutkimus on melko vastaavaa, kuin Facebookin; se toimii yleensä yhtenä esimerkeistä. Twitterin kohdalla on tutkittu esimerkiksi, kuinka jonkin käyttäjän kodin sijainti voidaan saada selville (Gu, Yao, Liu, & Song, 2016) ja kuinka suurin vaikutusvalta yksittäisellä henkilöllä on tietyllä alueella (Rao & Nagpal, 2011).

4.1.3 Jodel

Jodel eroaa aiemmista esimerkeistä siinä mielessä, että sen käyttäjät kommunikoivat keskenään anonyymisti. Kommunikaatio perustuu käyttäjien tekemiin keskustelunavauksiin, ns. jodlauksiin, joita muut käyttäjät voivat kommentoida ja äänestää. Jodlausten näkyvyys muille käyttäjille pohjautuu paikallisuuteen, eli paikkatietoa hyödyntäen se näyttää käydyt keskustelut ainoastaan lähialueilla oleville käyttäjille (Heikkilä, 2016). Lisäksi sovellus kertoo käyttäjilleen muiden käyttäjien suurpiirteisen sijainnin asteikolla ”lähellä” tai ”erittäin lähellä”.

Jodel ei anonyymiytensä vuoksi välttämättä sovi tyypillisen geososiaalisen verkostopalvelun määritelmään. Toisaalta se kuitenkin täyttää suurimman osan Roickin ja Houserin (2013) ehdoista: sen verkostot koostuvat ihmisistä, sen

käyttäjät kommunikoivat mobiililaitteiden välityksellä ja heidän on mahdollista liikkua fyysisessä maailmassa kommunikoinnin aikana. Lisäksi sosiaalisten verkostopalveluiden tapaan käyttäjien on mahdollista jakaa keskenään itse tuottamaansa sisältöä.

Jodel julkaistiin lokakuussa 2014 (Scherkamp, 2015). Se on aiempiin esimerkkeihin nähden uusi, joten sen suhteen ei vielä olla tehty juurikaan tutkimusta. Kirjallisuuskatsauksen aikana löydettiin ainoastaan yksi Jodelia käsittelevä julkaisu, jossa selvitettiin, voidaanko yksittäisten jodlausten perusteella selvittää anonyymien käyttäjien sijainti. Böhm, Taubmann, ja Reiser (2016) havaitsivat, että yksittäisen käyttäjän sijainti on mahdollista selvittää 10 metrin tarkkuudella.

4.2 Yksityisyysongelmat

Geososiaaliset verkostopalvelut voidaan nähdä perinteisen sosiaalisen median jatkeena (Sun, Wang, Shen, & Zhang, 2015), mikä tarkoittaa, että niissä ilmenevät samat yksityisyyden ongelmat, kuin sosiaalisessa mediassa yleensä (Fusco & Michael, 2010). Paikkatiedon hyödyntämisen vuoksi geososiaalisten verkostopalveluiden potentiaaliset yksityisyysongelmat ovat kuitenkin sosiaalista mediaa vakavampia (Puttaswamy ym., 2014), sillä paikkatieto on muuta sosiaaliseen mediaan tyypillisesti jaettavaa tietoa arkaluontoisempaa (Zhao, Lu, & Gupta, 2012).

Geososiaalisten verkostopalveluiden yksityisyysongelmat voivat johtua monesta eri tekijästä. Syinä voi olla esimerkiksi käyttäjät itse, sovellusten toiminta tai ulkoiset uhat, kuten kyberrikollisuus. Seuraavaksi tarkastellaan käyttäjien näkökulmasta tyypillisimpiä yksityisyysongelmia ja niiden syitä.

4.2.1 Käyttäjien toiminta

Käyttäjien oma toiminta vaikuttaa geososiaalisissa verkostopalveluissa esiintyviin yksityisyysongelmiin, vaikka tyypillinen uskomus Tamminsen, Lehmuskallion ja Johnsonin (2011) mukaan onkin, että yksityisyysongelmat aiheutuvat eritoten palveluntarjoajista. Ongelmia aiheuttaa jo pelkästään se, että käyttäjät eivät välttämättä ole huolissaan tietojensa jakamisesta (Christofides, Muise, & Desmarais, 2009), eikä heitä usein edes kiinnosta paikkatietojensa yksityisyys (Krumm, 2009). Huolettomuuteen ja kiinnostuksen puutteeseen puolestaan vaikuttanee tietämättömyys siitä, mitä kerätyllä informaatiolla tehdään. Milnen ja Culnanin (2004) mukaan suurin osa erilaisten online-palveluiden käyttäjistä ei lue palvelujen tietosuojasopimuksia. Esimerkiksi Facebookin tietosuojasopimusta ei lukenut 89 % ja käyttöehtoja 91 % käyttäjistä (Jones & Soltren, 2005). Näin ollen käyttäjät eivät siis voi tietää, minkälaiseen tietojen keruuseen antavat suostumuksensa palvelua käyttäessään. Toisaalta välinpitämättömyys tietojen keruun suhteen voi olla myös tietoinen valinta. Culnanin ja Biesin (2003) mukaan ihmiset ovat usein valmiita tinkimään yksityisyydestään, mikäli siten saavutetaan jotakin haittoja suurempaa hyötyä.

Hyöty voi tarkoittaa esimerkiksi mahdollisuutta käyttää geososiaalisia verkostopalveluita.

Vastakkaistakin näyttöä on olemassa: osa käyttäjistä ei tahdo käyttää paikkatietoa hyödyntäviä sovelluksia, sillä he ovat huolissaan paikkatietonsa yksityisyydestä (Barkhuus ym., 2008; Tang, Lin, & Hong, 2010). Vaikka näyttöä aiheesta on puolesta ja vastaan, on kuitenkin hyvä tiedostaa Maddenin (2012) huomio siitä, että käyttäjät usein antavat ymmärtää olevansa huolissaan yksityisyydestään, vaikka näin ei oikeasti olisikaan.

Kuten aiemmin todettiin, voidaan geososiaaliset verkostopalvelut nähdä perinteisen sosiaalisen median jatkeena ja näin ollen käyttäjät jakavat niihin samankaltaista informaatiota kuin sosiaaliseen mediaan yleensä, kohdaten myös samankaltaisia yksityisyyden ongelmia. Sosiaaliseen mediaan tyypillisesti jaettavaa informaatiota ovat Boydin ja Ellisonin (2008) mukaan esimerkiksi sukupuoli, ikä, asuinpaikka, kiinnostuksen kohteet ja profiiliin liitettävä valokuva. Edellä mainittujen lisäksi geososiaalisissa verkostopalveluissa myös paikkatiedon jakaminen korostuu. Valitettavaa on, että mikäli käyttäjä esimerkiksi hyväksyy kaveripyynnön tuntemattomalta henkilöltä, on vaarana, että tiedot päätyvät käyttäjän kannalta vihamielisen tahon käsiin. Brandtzægin, Lüdersin ja Skjetnen (2010) mukaan ei ole kovinkaan harvinaista, että käyttäjät hyväksyvät kaveripyyntöjä henkilöiltä, joita eivät tunne.

Jakaessaan henkilötietojensa lisäksi myös paikkatietonsa, käyttäjät siis jakavat geososiaalisiin verkostopalveluihin enemmän arkaluontoista tietoa, kuin perinteiseen sosiaaliseen mediaan. Näin ollen voidaan todeta, että käyttäjät itse ovat merkittävä yksityisyysongelmien aiheuttaja. Syitä tiedon jakamiseen voi olla monia ja ne myös riippuvat käyttäjistä ja palveluista. Pohjimmiltaan niin geososiaaliset verkostopalvelut kuin muutkin sosiaalisen median palvelut kuitenkin perustuvat tiedon jakamiseen ja näin ollen palveluiden toimintalogiikka rohkaisee käyttäjiä jakamaan mahdollisimman paljon tietoa (Brandtzæg ym., 2010).

Kuten aiemmin todettiin, paikkatiedon jakamisen myötä käyttäjien liikkeitä on mahdollista seurata ja ennustaa. Tämä puolestaan antaa rikollisille mahdollisuuksia toimia (Puttaswamy ym., 2014). Esimerkiksi murtovarkaiden toiminta helpottuu, mikäli käyttäjän poissaolon yksityisyys on vaarantunut ja varkaat voivat käyttäjän jakaman paikkatiedon perusteella päätellä, että tämä ei ole paikalla asunnossaan. Samoin vainoajien on helpompaa seurata vainottaviaan, mikäli he paikkatiedon jakamisen myötä tietävät näiden liikkeistä.

Toisaalta paikkatiedon jakaminen voi saattaa käyttäjän kiusalliseen tilanteeseen. Käyttäjät voivat esimerkiksi jäädä kiinni valheesta, mikäli ovat kertoneet olevansa tietyssä paikassa, mutta jaettu paikkatieto väittää muuta. Lisäksi ikäviä tilanteita saattaa aiheuttaa vaikkapa vääriin käsiin päätynyt paikkatieto erotiikkaklubin, sairaalan tai muun mahdollisesti arkaluontoisen paikan lähettyviltä.

Paikkatiedon jakaminen voi jopa saattaa käyttäjät hengenvaaraan. Eräänlaisena ääriesimerkkinä voidaan pitää tapausta, jossa terroristijärjestö ISIS:in sotilaat jakoivat Twitteriin paikkatietonsa GPS-koordinaatteina. Paikkatiedon perusteella Yhdysvaltain armeijan oli mahdollista kohdistaa ilmaisku ISIS – taistelijoiden asemiin. (Castillo, 2015).

4.2.2 Sovellusten toiminta

Yksityisyysongelmat geososiaalisissa verkostopalveluissa eivät johdu pelkästään käyttäjistä. Jo aiemmin esitetty Brandtzægin ym. (2010) yksityisyysdilemma viittaa sovellusten osuuteen, eli vaikka pääpiirteittäin käyttäjät jakavat tietojaan itse, rohkaisevat sovellukset kuitenkin tekemään niin. Lisäksi tietojen jako ei välttämättä ole käyttäjän kannalta aktiivista toimintaa; voi riittää, että siihen on kerran annettu lupa. Tällöin puhutaan paikkatiedon jakamisen automatisoinnista. Vihavaisen, Oulasvirran, ja Sarvaksen (2009) mukaan automaattinen paikkatiedon jakaminen on käyttäjien mielestä houkutteleva vaihtoehto, sillä heidän ei itse tarvitse nähdä tiedon jakamisen vaivaa. Esimerkiksi Facebookin Lähellä olevat kaverit –toiminto, ollessaan kertaalleen otettu käyttöön, jakaa käyttäjän fyysisen sijainnin muille tämän sosiaaliseen verkostoon kuuluville jatkuvasti (Kelly, 2014). Vastaavia toimintoja on valitettavan helppoa käyttää esimerkiksi vainoamiseen (C. Ma & Chen, 2014), sillä vainoja voi aktiivisesti seurata kohteensa liikkeitä reaaliajassa.

Paikkatieto pitää Zhengin (2012) mukaan sisällään käyttäjän reaaliaikaisen sijainnin lisäksi myös tiedon aikaisemmista sijainneista. Kyseiset tiedot vihamielisten tahojen käsissä voivat olla käyttäjän kannalta vaarallisia, sillä niiden perusteella on Pontesin, Vasconcelosin, Almeidan, Kumaragurun ja Almeidan (2012) mukaan mahdollista ennustaa käyttäjän tulevia liikkeitä ja sijainteja. On hyvä muistaa myös Frenin ym. (2010) huomio poissaolon yksityisyydestä; siinä missä paikkatieto kertoo käyttäjän sijainnin, kertoo se myös ne paikat, joissa käyttäjä ei ole.

Myös Swarmin kohdalla on nähtävissä sovelluksen toimintalogiikasta johtuvia yksityisyysongelmia. Luvussa 4.1.1 mainittiin pormestari –status, joka aktiivisten käyttäjien on mahdollista saavuttaa. Status voi aiheuttaa ongelmia käyttäjän yksityisyydelle, sillä sovelluksen muidenkin käyttäjien on mahdollista nähdä, kuka on tietyn sijainnin pormestari. Esimerkiksi tieto siitä, että käyttäjä vierailee hampurilaisravintolassa neljästi päivässä saattaa aiheuttaa kiusallisia tilanteita. Tietenkään käyttäjien ei ole pakko pyrkiä saavuttamaan pormestarin arvoa, mutta kuten kuviosta 1 havaittiin, sovellusten toimintalogiikka tyypillisesti ajaa käyttäjiä kyseiseen toimintaan. Teoriassa käyttäjien tulisi olla tietoisia siitä, että pormestari –status on näkyvissä muille käyttäjille; ovathan he palveluun liittyessään hyväksyneet sen yksityisyyskäytänteet. On kuitenkin hyvä muistaa Culnanin (2004) havainto: suurin osa käyttäjistä ei lue tietosuojasopimuksia.

Yksityisyysongelmia voi ilmetä myös silloin, kun geososiaalinen verkostopalvelu toimii huonosti. Ajoittain voi käydä niin, että paikkatieto ei päivity palveluun oikein ja käyttäjä saattaa vaikuttaa sen perusteella olevan väärässä sijainnissa (Jin & Takabi, 2014). Palveluun päivittyvä väärä sijainti saattaa aiheuttaa sosiaalisesti kiusallisia tilanteita esimerkiksi Facebookin Lähellä olevat kaverit –toiminnon kohdalla, jolloin käyttäjän sosiaaliseen verkostoon kuuluvat ihmiset näkevät käyttäjän olevan sijainnissa, jossa hän ei oikeasti ole.

Geososiaalisiin verkostopalveluihin liittyvät yksityisyysongelmat eivät kuitenkaan aina liity sovellusten aktiiviseen toimintaan. Ajoittain kyse on toimimattomuudesta; esimerkiksi tietoturva-aukoista ja yritysten hitaasta rea-

goinnista niihin. Tyypillinen ongelma Bilgen, Strufen, Balzarottin, Kirdan ja Antipolisin (2009) mukaan on käyttäjien heikko identifikaatio; palveluihin on helppo liittyä keksityllä nimellä ja väärillä tiedoilla. Heikko identifikaatio avaa oven tekaistujen käyttäjien tehtailuun, mikä puolestaan on kohtuullisen helppo tapa urkkia tietoja oikeilta käyttäjiltä, sillä kuten Brandtzægiin ym. (2010) viitaten aiemmin todettiin, ei ole harvinaista, että ihmiset hyväksyvät kaveripyyntöjä käyttäjiltä, joita eivät tunne.

Heikko identifikaatio voi tekaistujen käyttäjien lisäksi johtaa tekaistujen paikkojen luomiseen. Esimerkiksi Foursquaren ja Swarmin kohdalla käyttäjät itse luovat palvelussa olevat paikat. Paikkoja luovat käyttäjät pyritään identifioimaan puhelinnumeron avulla ennen uuden paikan luomista, mutta puhelinnumeroon perustuva identifikaatio on kuitenkin helppo kiertää. Tekaistujen paikkojen vuoksi rehellisten käyttäjien paikkatiedon yksityisyys voi joutua vaaraan: mikäli vihamielinen käyttäjä esimerkiksi perustaa paikan jonkin kiusallisen sijainnin, kuten erotiikkaliikkeen kohdalle, näkee hän kaikkien niiden käyttäjien tiedot, jotka paikkaan ilmoittautuvat läsnä oleviksi. Kiusallinen tieto väärissä käsissä voi aiheuttaa käyttäjille erilaisia ongelmia. (Jin & Takabi, 2014.)

4.2.3 Ulkoiset tekijät

Käyttäjien oman toiminnan ja sovellusten toiminnan lisäksi geososiaalisten verkostopalveluiden yksityisyysongelmat voivat johtua myös ulkoisista tekijöistä. Ulkoisilla tekijöillä tarkoitetaan tässä yhteydessä käyttäjistä riippumattomia tahoja, kuten heidän sosiaalisiin verkostoihinsa kuuluvia henkilöitä tai esimerkiksi kyberrikollisia. Ulkoisista tekijöistä aiheutuvat yksityisyysongelmat liittyvät usein sovellusten toimintaan: sovellukset saattavat rohkaista käyttäjän sosiaaliseen verkostoon kuuluvia henkilöitä julkaisemaan tietoa, joka on käyttäjän kannalta haitallista. Toisaalta kyberrikollisten on mahdollista hyödyntää sovellusten yksityisyyden suojaan liittyviä puutteita. Ruiz Vicenten ym. (2011) mukaan geososiaalisten verkostopalveluiden yksityisyyden suoja ei pysty vastaamaan sitä kohtaaviin yksityisyyden haasteisiin.

Käyttäjien sosiaalisiin verkostoihin kuuluvat jäsenet saattavat tahattomasti tulla loukanneiksi näiden paikallaolon, poissaolon, yhteisen paikkatiedon ja identiteetin yksityisyyttä (Ruiz Vicente ym., 2011). Taulukossa 2 esitetään kuvitteellisten henkilöiden tekemiä fiktiivisiä geososiaalisten verkostopalveluiden statuspäivityksiä ja myöhemmin käydään läpi, minkälaisia yksityisyysongelmia päivitykset voivat aiheuttaa.

TAULUKKO 2 Kuvitteellinen esimerkki käyttäjien päivityksistä

Käyttäjä	Päivitys
A	Klo: 12:00: ”Oluella!”
B	Klo: 12:00: ”Paikassa X!”
C	Klo: 12:00: ”A:n ja B:n seurassa!”

Mikäli jollakin taholla on pääsy taulukossa 2 esiteltyjen A:n, B:n ja C:n statuspäivityksiin, on niiden perusteella mahdollista tehdä käyttäjien yksityisyyden kannalta ongelmallisia johtopäätöksiä, vaikka yksittäin päivitykset paljastavat melko vähän tietoa: käyttäjä A kertoo ainoastaan mitä tekee, käyttäjä B sijaintinsa ja käyttäjä C kenen seurassa on.

Kolmen päivityksen tietoja yhdistelemällä voidaan kuitenkin havaita, että käyttäjien paikallaolon, poissaolon ja yhteisen paikkatiedon yksityisyys on uhattuna: B:n kertoessa sijaintinsa ja C:n seuransa, voidaan päivitysten perusteella päätellä, missä henkilöt ovat ja samalla missä he eivät ole. Lisäksi tiedetään, kenen seurassa he ovat ja tapahtumien tarkka kellonaika. A:n kertoessa tekemisistään, voidaan myös tehdä oletuksia siitä, mitä muutkin käyttäjät ovat tekemässä. Näin ollen voidaan todeta, että käyttäjästä riippumattomat tekijät voivat tahattomasti aiheuttaa yksityisyysuhkia.

Ulkoisista tekijöistä johtuvat yksityisyysuhat eivät kuitenkaan välttämättä ole tahattomia. Vihamieliset tahot saattavat käyttää sovellusten toimintaan liittyviä haavoittuvuuksia hyväkseen ja näin aiheuttaa uhkia käyttäjien yksityisyydelle (Gambs, Cedex, Killijian, & Núñez, 2010; Ruiz Vicente ym., 2011). Tämän kaltaiset tahot voivat esimerkiksi ujuttaa haittaohjelmia geososiaalisiin verkostopalveluihin tai rakentaa vakoilutyökaluja, jotka hyödyntävät sovellusten tietoturvassa ilmeneviä puutteita.

Tutkielman teon aikana havaittiin, että esimerkiksi Jodel -sovellukselle on kehitetty työkalu, jonka avulla vihamielisen tahon on mahdollista nähdä kunkin viestin lähettäjän tarkka sijainti kartalla. Tarkan sijainnin vakoilu on siinä mielessä erityisen ongelmallista, että sovellusta markkinoidaan täysin anonyyminä palveluna ja näin ollen käyttäjät saattavat paljastaa hyvinkin arkaluontoista tietoa itsestään. Man, Hancockin ja Naamanin (2016) mukaan ihmiset paljastavat itsestään anonymiteetin turvin enemmän ja intiimimpää tietoa, kuin tilanteessa, jossa heidän henkilöllisyytensä on tiedossa. Anonyymina markkinoidun sovelluksen kohdalla erityisesti käyttäjien identiteetin yksityisyys on uhattuna.

Sovellusten lisäksi, kuten luvussa 4.2.1 havaittiin, myös käyttäjien toiminnassa on usein virheitä, jotka mahdollistavat vihamielisten tahojen toiminnan.

Esimerkiksi käyttäjän manipulointi (social engineering) on tavallinen vihamielisten tahojen käyttämä tekniikka, joka hyödyntää sovellusten ohella myös käyttäjiin liittyviä heikkouksia, kuten hyväuskoisuutta ja auttamisen halua (Flores, 2013). Manipuloinnin avulla käyttäjiä pyritään harhauttamaan siten, että he luovuttaisivat henkilökohtaisia tietoja itsestään tai muista (Thornburgh, 2004). Geososiaalisten verkostopalveluiden kontekstissa esimerkiksi aiemmin mainittu keksittyjen paikkojen luominen edustaa kyseistä tekniikkaa. Näin ollen voidaankin todeta, että vaikka tutkielmassa erilaisten yksityisyyteen liittyvät ongelmat ja niiden syyt esitetään erillään, ovat ne kuitenkin todellisuudessa sidoksissa toisiinsa.

5 YHTEENVETO

Geososiaalisten verkostopalveluiden suosio on ollut kasvussa viime vuosina ja onkin odotettavissa, että kasvu jatkuu edelleen. Kasvavan suosion myötä myös käyttäjistä kerättävän informaation määrä oletettavasti kasvaa. Siinä missä perinteisten sosiaalisten median palveluiden havaittiin keräävän käyttäjistään lähinnä staattisia henkilötietoja, keräävät geososiaaliset verkostopalvelut tietoa myös käyttäjiensä sijainnista. Sijaintitiedon puolestaan havaittiin olevan muita tyypillisesti jaettavia henkilötietoja arkaluontoisempaa. Tässä tutkielmassa selvitettiin, minkälaisia yksityisyysongelmia geososiaalisiin verkostopalveluihin liittyy. Ongelmia tarkasteltiin ainoastaan käyttäjin näkökulmasta, sillä niiden tarkastelu myös yritysten kannalta olisi tehnyt tutkimusaiheesta liian laajan. Havaittuja ongelmia jäsenneltiin sen mukaan, mistä niiden voidaan nähdä aiheutuvan. Tutkielman mukaan tärkeimpiä syitä yksityisyysongelmille ovat käyttäjien toiminta, sovellusten toiminta ja kolmansien osapuolten toiminta.

Monet yksityisyysongelmat vaikuttavat aiheutuvan käyttäjien toiminnasta. Käyttäjät esimerkiksi vapaaehtoisesti jakavat verkkopalveluihin tietoa, joka saattaa vaarantaa heidän yksityisyytensä. Tiedon huoleton jakaminen näyttää johtuvan sekä tietämättömyydestä, että välinpitämättömyydestä; suuri osa ihmisistä ei lue tietosuojaselosteita tai palveluiden käyttöehtoja lainkaan. Lisäksi käyttäjät hyväksyvät helposti kaveripyyntöjä käyttäjiltä, joita eivät tunne.

Sovellusten toiminnasta aiheutuvat yksityisongelmat näyttävät liittyvän sovellusten toimintalogiikkaan ja niiden heikkoon tietoturvaan. Sovelluksille on tyypillistä, että ne ohjaavat käyttäjiään paljastamaan mahdollisimman paljon tietoa itsestään, mutta toisaalta eivät identifioi käyttäjiä kovinkaan tarkasti. Tämä puolestaan mahdollistaa esimerkiksi valekäyttäjien luomisen ja sitä kautta rehellisten käyttäjien manipuloimisen.

Kolmansista osapuolista johtuvat yksityisyysongelmat ovat tyypillisesti joko vahinkoja tai tarkoituksella aiheutettuja. Esimerkiksi käyttäjän ystävät saattavat epähuomiossa paljastaa tähän liittyviä tietoja ja näin saattaa käyttäjän yksityisyyden vaaraan. Toisaalta vihamieliset tahot voivat erilaisia työkaluja ja manipulointia hyödyntäen pyrkiä urkkimaan käyttäjään liittyviä tietoja.

Tutkielmassa pyrittiin ottamaan eri yksityisyysongelmia aiheuttavat tekijät mahdollisimman hyvin huomioon. Aiemmissa geososiaalisia verkostopalve-

luja käsittelevissä tutkimuksissa keskitytään yleensä tiettyjen tekijöiden aiheuttamiin yksityisyysongelmiin ja varsinkin tapoihin suojautua niiltä.

Vaikka eri yksityisyysongelmien syyt jaoteltiin aiemmin mainittujen kolmen tekijän mukaan, on hyvä muistaa, että syyt usein liittyvät toisiinsa. Esimerkiksi kolmansien osapuolten olisi vaikeaa urkkia käyttäjästä tietoja, mikäli käyttäjä ei olisi liittynyt mihinkään palveluun. Samoin sovellusten haavoittuvuuksia olisi vaikeaa käyttää hyväkseen, mikäli haavoittuvuuksia ei olisi.

Yksityisyysongelmia voi olla tutkielmassa esitettyjen lisäksi muitakin. Tutkielmassa pyrittiin tuomaan esiin sellaisia ongelmia, joita on käsitelty tieteellisessä keskustelussa. Muut tieteellisen keskustelun ulkopuolelta havaitut ongelmat luvun 4.2.3 Jodeliin liittyvää esimerkkiä lukuun ottamatta jätettiin tutkielman ulkopuolelle. Tavoitteena oli antaa tiivis katsaus tutkimukseen, jota on tehty geososiaalisten verkkopalveluiden yksityisyysongelmien parissa.

Lisäksi tulee tiedostaa tutkielman lähdeaineistoon liittyvät rajoitteet. Suurin osa lähdeaineistosta on joko Yhdysvaltain tai eri Aasian maiden perspektiivistä kirjoitettuja. Vaikka tässä tutkielmassa ei otettu kantaa maantieteellisiin eroihin yksityisyysongelmissa tai niiden käsittämisessä, on hyvä pitää mielessä, että jo pelkästään lainsäädännöllisistä syistä eri maissa saatetaan kohdata erilaisia yksityisyysongelmia kuin Suomessa.

Lähdeaineiston läpikäynnin perusteella vaikuttaa siltä, että aikaisempi tutkimus keskittyy lähinnä yksityisyysongelmiin perinteisessä sosiaalisessa mediassa. Geososiaalisten verkostopalveluiden kontekstissa enemmän huomiota ovat ongelmien sijaan saaneet esimerkiksi käyttäjien asenteiden kartoittaminen. Näin ollen aiheesta tarvitaan lisää tutkimusta.

Lisäksi paikkatietoa hyödyntävien anonyymien sovellusten yksityisyyttä ja tietoturvaa olisi hyvä kartoittaa. Monet anonyymit paikkatietoa hyödyntävät sovellukset, kuten Jodel, Yik Yak ja Whisper ovat muihin sosiaalisen median palveluihin verrattuna uusia, joten niihin liittyen ei ole vielä ehditty tehdä juurikaan tutkimusta. Niiden suosio on kuitenkin kasvussa. Kiinnostava tutkimusaihe voisi olla esimerkiksi paikkatiedon yksityisyys anonyymeissa paikkatietoa hyödyntävissä palveluissa.

Kaiken kaikkiaan vaikuttaa siltä, että geososiaalisiin verkostopalveluihin liittyy useita yksityisyysongelmia. Ongelma on siinä, että useimmiten käyttäjät eivät todellisuudessa ole kovin kiinnostuneita yksityisyydestään, vaikka kyselyissä väittäisivät toista. Tutkielma on täyttänyt tavoitteensa, mikäli lukija sen luettuaan tiedostaa tyypillisimmät yksityisyysongelmat, ymmärtää niiden syyt ja osaa jatkossa kiinnittää omaan yksityisyyteensä enemmän huomiota.

LÄHTEET

Acquisti, A., & Gross, R. (2006). Imagined Communities : Awareness , Information Sharing , and Privacy on the Facebook, 1–22.

Barkhuus, L., Brown, B., Bell, M., Hall, M., Sherwood, S., & Chalmers, M. (2008). From awareness to repartee: Sharing Location within Social Groups. *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08*, 497.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in Electronic Commerce : The Role of Privacy, Security, and Site Attributes, *11*(July 2016), 245–270.

Bilge, L., Strufe, T., Balzarotti, D., Kirda, E., & Antipolis, S. (2009). All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks. *Www 2009*, 551–560.

Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites : Definition , History , and Scholarship. *Journal of Computer-Mediated Communication*, *13*, 210–230.

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction*, *26*(March), 1006–1030.

Böhm, A., Taubmann, B., & Reiser, H. P. (2016). Geographic Localization of an Anonymous Social Network Message DataSet. *The 1st International Work shop on Social collaboration in trusted, user-driven software development*, (March), 844–850.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Interactive Marketing*, *11*(3), 25–31.

Carbunar, B., & Potharaju, R. (2012). You unlocked the Mt. Everest badge on foursquare! Countering location fraud in GeoSocial networks. *MASS 2012 - 9th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, 182–190.

Castillo, W. (2015). U.S. bombs ISIS using social media intel - CNNPolitics.com. Noudettu 5. joulukuuta 2016, osoitteesta http://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society*, *12*(3), 341–345.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67.

Cranor, L. F. (1999). Internet Privacy. *Communications of the ACM*, *42*(2), 29–31.

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, *59*(2), 323–342.

Debatin, B., Ann-Kathrin Horn, M. ., & Hughes, B. N. (2009). Facebook and Online Privacy : Attitudes , Behaviors , and Unintended Consequences. *Journal of Computer-Mediated Communication*, *15*, 83–108.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Americas The*, *123*(4), 339–350.

Emerson, T. I. (1979). The Right of Privacy and Freedom of the Press. *Harvard Civil Rights-Civil Liberties Law Review*, *14*(2).

Flores, D. A. (2013). A Social Engineering Discussion about Privacy Attacks and Defences Considering Web Browsers and Social Networks. *8th Congress of Science and Technology-ESPE*, 1–6.

Freni, D., Ruiz Vicente, C., Mascetti, S., Bettini, C., & Jensen, C. S. (2010). Preserving Location and Absence Privacy in Geo-social Networks. *Cikm'10*, 309.

Fusco, S. J., & Michael, K. (2010). Using a social informatics framework to study the effects of location-based social networking on relationships between people : A review of literature. *International Conference on Mobile Business*, 157–171.

Gambs, S., Cedex, R., Killijian, M., & Núñez, M. (2010). Show Me How You Move and I Will Tell You Who You Are. *Public Policy*, *4*, 34–41.

Gao, H., & Liu, H. (2014). Data analysis on location--based social networks. *Mobile social networking*, 165–194.

Gavisont, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421–471.

Gellman, R. M. (1984). Prescribing Privacy : The Uncertain Role of the Physician in the Protection of Patient Privacy, *62*(2).

Gritzalis, S. (2004). *Enhancing Web privacy and anonymity in the digital era*. *Information Management & Computer Security* (Vsk. 12).

Gross, D., & Hanna, J. (2010). Facebook introduces check-in feature - CNN.com. Noudettu 28. marraskuuta 2016, osoitteesta http://edition.cnn.com/2010/TECH/social.media/08/18/facebook.location/

Gu, Y., Yao, Y., Liu, W., & Song, J. (2016). We know where you are: Home location identification in location-based social networks. *25th International Conference on Computer Communications and Networks, ICCCN 2016*.

He, W., Liu, X., & Ren, M. (2011). Location cheating: A security challenge to location-based social network services. *Proceedings - International Conference on Distributed Computing Systems*, 740–749.

Heikkilä, T. (2016). Jodel on virtuaalinen vessanseinä, jolla kysytään sitä, mitä ei muuten kehdata. Noudettu 28. marraskuuta 2016, osoitteesta http://www.aviisi.fi/2016/11/jodel-virtuaalinen-vessanseina-kysytaan-sita-mita-muuten-kehdata/

Heinonen, S. (2009). SOSIAALINEN MEDIA Avauksia nettiyhteisöjen maailmaan ja vuorovaikutuksen uusiin muotoihin. *TUTU-ejulkaisuja*, 1–23.

Huang, Q., & Liu, Y. (2009). On Geo-social Network Services. *17th International Conference on Geoinformatics, IEEE*, 1–6.

Jin, L., Long, X., Joshi, J. B. D., & Anwar, M. (2012). Analysis of access control mechanisms for users' check-ins in Location-Based Social Network Systems. *Information Reuse and Integration (IRI), 2012 IEEE 13th International Conference on*, 712–717.

Jin, L., & Takabi, H. (2014). Venue Attacks in Location-Based Social Networks. *Proceedings of the 1st ACM SIGSPATIAL International Workshop on Privacy in Geographic Information Collection and Analysis*, 0–7.

Jones, H., & Soltren, H. (2005). Facebook : Threats to Privacy. *Social Science Research*, *December 1*, 1–76. https://doi.org/10.1371/journal.pone.0068524

Kantola, S. (2013). *Paikkatiedon käyttö tietojohtamisessa ja päätöksenteossa*. *Pro-gradu tutkielma*.

Kaplan, A. M. (2012). If you love something , let it go mobile : Mobile marketing and mobile social media 4x4. *Business Horizons*, *55*(2), 129–139.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68.

Kelly, H. (2014). Facebook launches friend-tracking feature - CNN.com. Noudettu 28. marraskuuta 2016, osoitteesta http://edition.cnn.com/2014/04/17/tech/mobile/facebook-nearby-friends/

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241–251.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, *13*(6), 391–399. https://doi.org/10.1007/s00779-008-0212-5

Laraki, O. (2010). Twitter Places: More Context For Your Tweets | Twitter Blogs. Noudettu 28. marraskuuta 2016, osoitteesta https://blog.twitter.com/2010/twitter-places-more-context-for-your-tweets

Lietsala, K., & Sirkkunen, E. (2008). *Social media*. *Social Media - Introduction to the tools and processes of participatory economy* (Vsk. 2010).

Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., & Zimmerman, J. (2011). I'm the Mayor of My House: Examining Why People Use foursquare - a Social-Driven Location Sharing Application. *CHI '11 Proceedings of the 2011 annual conference on Human factors in computing systems*, *54*(6), 2409–2418.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems*, *27*(4), 163–200.

Ma, C., & Chen, C. W. (2014). Nearby friend discovery with Geo-indistinguishability to stalkers. *Procedia Computer Science*, *34*, 352–359.

Ma, X., Hancock, J., & Naaman, M. (2016). Anonymity, Intimacy and Self-Disclosure in Social Media. *Proceedings of the 2016 CHI Conference on Human*

Factors in Computing Systems, 3857–3869.

Madden, M. (2012). Privacy management on social media sites. *Pew Internet & American Life Project*, 20.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users ' The Information the Scale , and a Causal (IUIPC): *Information Systems Research*, *15*(4), 336–355.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29.

Miyazaki, A. D., & Fernandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Source Journal of Public Policy & Marketing*, *19*(1), 54–61.

Najaflou, Y., Jedari, B., Xia, F., Yang, L. T., & Obaidat, M. S. (2013). Safety Challenges and Solutions in Mobile Social Networks. *IEEE Systems Journal*, *9*(3), 1–21.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, the Journal of the American Academy of Arts & Sciences*, *140*(4), 32–48.

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review*, *19*(1), 17–31.

Ohno-Machado, L., Silveira, P. S. P., & Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. *International Journal of Medical Informatics*, *73*(7–8), 599–606.

Parent, W. . (1983). Privacy, Morality and the Law. *Philosophy & Public Affairs*, *12*(4), 269–288.

Pontes, T., Vasconcelos, M., Almeida, J., Kumaraguru, P., & Almeida, V. (2012). We know where you live. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, 898.

Popper, B., & Hamburger, E. (2014). Meet Swarm: Foursquare's ambitious plan to split its app in two | The Verge. Noudettu 28. marraskuuta 2016, osoitteesta http://www.theverge.com/2014/5/1/5666062/foursquare-swarm-new-app

Puttaswamy, K. P. N., Wang, S., Steinbauer, T., Agrawal, D., Abbadi, A. El, Kruegel, C., & Zhao, B. Y. (2014). Preserving Location Privacy in Geosocial Applications, *13*(1), 159–173.

Rao, T., & Nagpal, S. (2011). Real-time geo influence in social networks. *ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology*, *1*, 246–250.

Razzouk, N. Y., Seitz, V., & Nicolaou, M. (2008). Consumer Concerns Regarding Rfid Privacy : an Empirical Study. *Journal of Global Business and Technology*, *4*(1), 69–79.

Rezgui, A., Bouguettaya, A., & Eltoweissy, M. Y. (2003). Privacy on the web: Facts, challenges, and solutions. *IEEE Security and Privacy*, *1*(6), 40–49.

Roick, O., & Heuser, S. (2013). Location Based Social Networks–Definition, Current State of the Art and Research Agenda. *Transactions in GIS*, *17*(5), 763–784.

Rosenblum, D. (2007). What Anyone Can Know. *IEEE Security and Privacy*, *5*(3), 40–49.

Ruiz Vicente, C., Freni, D., Bettini, C., & Jensen, C. S. (2011). Location-Related Privacy in Geo-Social Networks. *IEEE Internet Computing*, *15*(3), 20–27.

Scherkamp, H. (2015). Warum Studenten die App Jodel lieben – und Promi-Investoren auch | Gründerszene. Noudettu 24. tammikuuta 2017, osoitteesta http://www.gruenderszene.de/allgemein/jodel-app-erfolg

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21–32.

Smith, J. ., Milberg, S. ., & Burke, S. . (1996). Information privacy: measuring individuals concerns about organizational practices. *MIS quaterly*, (June), 167–196.

Smith, P., Syed, N., Thaw, D., & Wong, A. (2011). When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches. *The Yale Law Journal*, *177*, 177–202.

Souza, A. D. S., & Frith, J. (2010). Locative Mobile Social Networks : Mapping Communication and Location in Urban Spaces. *Mobilities 5.4*, *5*(4), 485–505.

Stone, B. (2009). Location, Location, Location | Twitter Blogs. Noudettu 28. marraskuuta 2016, osoitteesta https://blog.twitter.com/2009/location-location-location

Stone, E., Gueutal, H., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, *68*(3), 459–468.

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292.

Tamminen, S., Lehmuskallio, A., & Johnson, M. (2011). *Yksityisyyden haasteet sosiaalisessa mediassa*. *Silmät auki sosiaaliseen mediaan* (Vsk. 3/2011).

Tang, K., Lin, J., & Hong, J. (2010). Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. *Proceedings of the 12th …*, *12*(4–5), 85–94.

Thornburgh, T. (2004). Social Engineering : The " Dark Art ". *Proceedings of the 1st annual conference on Information security curriculum development*, 133–135.

Vihavainen, S., Oulasvirta, A., & Sarvas, R. (2009). "I can't lie anymore!": The implications of location automation for mobile social applications. *Mobile and Ubiquitous Systems: Networking & Services*, 1–10.

Wagner, D., Lopez, M., Doria, A., Pavlyshak, I., Kostakos, V., Oakley, I., & Spiliotopoulos, T. (2010). Hide and seek. *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services - MobileHCI '10*, *40*, 55. h

Wang, H., Lee, M. K. ., & Wang, C. (1998). Consumer PRIVACY CONCERNS about Internet Marketing. *Communications of the ACM*, *41*(3), 63–70.

Warren, S. D., & Brandeis, L. D. (1890). The Right To Privacy. *The Harvard Law Review Association*, *4*(5), 193–220.

Wernke, M., Skvortsov, P., Dürr, F., & Rothermel, K. (2012). A classification of location privacy attacks and approaches. *Personal and Ubiquitous Computing*, *18*(1), 163–175.

Wu, X., & Schulzrinne, H. (2005). *Location-based Services in Internet Telephony*.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting User Concerns About Online Privacy Mike. *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY*, *58*(5), 710–722.

Yhdistyneet Kansakunnat. (1948). Ihmisoikeuksien yleismaailmallinen julistus.

Zhao, L., Lu, Y., & Gupta, S. (2012). *Disclosure Intention of Location-Related Information in Location-Based Social Network Services. International Journal of Electronic Commerce* (Vsk. 16).

Zheng, Y. (2012). Tutorial on location-based social networks. *Proceedings of the 21st international conference on World wide web, WWW*, *12*(5).