TECHNOLOGY • RESEARCH HIGHLIGHTS • VISIONS • SCIENCE
256

Yksityisyyden suoja ja luottamus liikkumisen sähköisissä palveluissa

Immo Heino

VTT

VTT TECHNOLOGY 256

Yksityisyyden suoja ja luottamus liikkumisen sähköisissä palveluissa

Immo Heino

ISBN 978-951-38-8409-3 (URL: http://www.vtt.fi/julkaisut)

VTT Technology 256

ISSN-L 2242-1211
ISSN 2242-122X (Verkkojulkaisu)
http://urn.fi/URN:ISBN:978-951-38-8409-3

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Alkusanat

Tämä yksityisyyden suojaa ja luottamusta käsittelevä raportti on tuotettu osana Liikenteen sähköiset palvelut -tutkimushanketta 2014–2015. Kyseistä työtä ovat rahoittaneet Liikenne- ja viestintäministeriö (LVM), Liikenteen turvallisuusvirasto Trafi, Liikennevirasto (LiVi) ja Tekes. Toteutuksesta on vastannut Teknologian tutkimuskeskus VTT Oy. Raportissa esitetyt käsitykset ovat tutkijan omia eivätkä välttämättä edusta rahoittajien tai VTT:n näkemyksiä.

Hankkeen ohjausryhmän jäseniä olivat Juuso Kummala Liikennevirastosta, Anders Granfelt Trafista, Seppo Öörni LVM:stä, Sampo Hietanen ITS Finlandista ja Karri Rantasila VTT:ltä.

Sisällysluettelo

“The erosion of privacy, unlike war, economic bad times, or domestic unrest, does not jump to the citizen’s attention and cry out for action. But by the time privacy is seriously compromised it is too late to clamour for reform.”

– Samuel Alito, Report of the Chairman, in The Boundaries of Privacy in American Society, 1972

1. Johdanto

Suomessa on julkaistu Lakimiesliiton Kustannuksen kustantamana Riku Neuvosen teos ”Yksityisyyden suoja Suomessa” (Neuvonen 2014), joka tarkastelee yksityisyyden suojaa erityisesti lainopillisesta näkökulmasta useilla elämän osa-alueilla. Teoksen laajuuden huomioiden ei siinä luonnollisestikaan ole voitu ulottaa syvempää tarkastelua kaikkiin mahdollisiin teemoihin. Tämän raportin tarkoituksena onkin tarkastella yksityisyyden suojaan liittyviä kysymyksiä erityisesti liikkumiseen liittyvien palveluiden kannalta lainopillista tulkintaa täydentäen. Liikkumisen palvelut perustuvat pitkälti paikkatiedon hyväksikäyttöön, joten tarkastelussa painotetaan paikkatiedon yksityisyyden suojaan liittyviä teemoja.

Yleisellä tasolla yksityisyyteen liittyvät tutkimuskysymykset ovat tässä tarkastelussa seuraavat:

- Mitä yksityisyydellä tarkoitetaan yleisesti ja liikkumisen palveluissa erityisesti?
- Mitkä on yksityisyyden arvo, ja kuinka se vaikuttaa liikennepalveluiden käyttämiseen, tuottamiseen ja innovaatioihin?
- Millaisia ovat käyttäjien asenteet yksityisyyden suojaan yleisesti ja älyliikennepalveluihin (ITS, Intelligent Traffic Services) erityisesti?

Palveluiden personointi helppokäyttöisiksi ja kuluttajien tavoitteita tukeviksi riippuu pitkälti yritysten ja yhteisöjen mahdollisuudesta käyttää kuluttajiin yhdistettyä tietoa (personal data). Jos tällaista henkilöön sidottua tietoa on käytettävissä, erilaisilla tietoteknisillä menetelmillä voidaan kerätystä aineistosta ennustaa käyttäjien käyttäytymistä ja mieltymyksiä, mikä puolestaan helpottaa palveluiden asiakaskohtaista räätälöintiä asiakaskokemuksen parantamiseksi.

Kun liikkumisen palveluiden hyödyntämiseen käytetään henkilökohtaista paikkatietoa, kysymyksiksi nousevat seuraavat:

- Muodostaako yksityisyyden suoja esteen personoiduille ja kontekstitietoisille liikkumisen palveluille?
- Mitkä ovat mahdolliset paikkatietoisiin palveluihin liittyvät uhat – käyttäjien itse kokemat tai sellaiset, joista käyttäjät eivät ole mahdollisesti edes tietoisia?

- Miten uhkia voidaan vähentää lainsäädännöllisin ja teknisin keinoin?
- Miten voidaan kasvattaa käyttäjien luottamusta henkilökohtaisen tiedon käyttämiseen osana palveluiden tehokasta kohdentamista?
- Jos liikenteeseen liittyvää sääntelyä puretaan, millaisia mekanismeja on taata käyttäjien luottamus palveluihin muuttuneessa tilanteessa?

Tutkimuksessa on käytetty seuraavia menetelmiä:

- laajaa kirjallisuustutkimusta nykytilan kartoittamiseksi ja kokonaiskuvan muodostamiseksi
- kohderyhmähaastatteluja suomalaisen liikennepalveluekosysteemin sidosryhmien (yksityiset palveluntarjoajat, viranomaiset ja kansalaisjärjestöjen edustajat) keskuudessa
- käyttötapaustarkasteluja olemassa olevista palveluista.

Tarkastelu on poikkitieteellinen, ja siinä on tarkastelunäkökulmina käytetty sosiologista, taloudellista ja teknistä lähestymistapaa sekä teoreettisista että käytännön lähtökohdista. Raportissa keskitytään erityisesti taloudellisiin ja teknisiin tarkasteluihin. Lähteinä on käytetty pääasiallisesti länsimaista aineistoa, lähinnä siis eurooppalaisia ja yhdysvaltalaisia lähteitä. Yhdysvaltalaisten lähteiden runsasta käyttöä voidaan perustella mm. seuraavilla seikoilla:

- Yksityisyyteen liittyvien kysymysten tutkimus on USA:ssa niin teoreettisella kuin käytännön tasolla maailman huippuluokkaa. Monet yksityisyyden suojaan liittyvät ongelmat ja käyttötapaukset ovat hyvin dokumentoituja julkisissa lähteissä.
- Yhdysvallat on johtava kaupallisten, liikkumiseen liittyvien kuluttajapalveluiden tuottaja, ja ”liberaalit” yksityisyyden suojan käytännöt ovat mahdollistaneet valtavan palvelutarjonnan ja innovointimahdollisuudet.
- Lähes kaikki nykyiset johtavat kuluttajapalvelut ovat USA:sta lähtöisin, ja täten niiden lainsäädännöllinen pohja perustuu Yhdysvaltojen käytäntöihin ja eurooppalaiset määräykset ovat vaikuttaneet niihin hyvin löyhästi (ns. Safe Harbour -menettely).
- Käynnissä olevat vapaakauppaneuvottelut EU:n ja Yhdysvaltojen välillä saattavat myös vaikuttaa jossain määrin EU:n lainsäädännölliseen tulkintaan yksityisyyden suojasta pitemmällä aikajänteellä.

Raportin tarkoituksena on antaa perustietoa yksityisyyden suojaan ja luottamukseen liittyvistä tekijöistä ja joitakin käytännön suuntaviivoja niiden huomioimiseen, kun palvelukehityksessä muodostetaan suomalaista liikennepalveluiden ekosysteemiä. Lukijalta ei edellytetä esitietoja yksityisyyden suojasta. Älyliikennepalveluiden olemusta ja liikennettä koskevan sääntelyn lähtökohtia ja sen purkamista on kuvattu liitteissä A (Älyliikenne [ITS] ja siihen liittyvät palvelut) ja B
(Julkisen liikenteen sääntely ja sen purkaminen).

Koska raportti sisältää alun perin englannin kielestä peräisin olevia käsitteitä, joilla ei suomen kielessä välttämättä ole yhtä hienovaraista vastinetta, alkuperäinen englanninkielinen termi saatetaan esittää suluissa suomenkielisessä yhteydessä. Tässä selvityksessä on jouduttu karsimaan joidenkin tieteellisesti merkittävien yksityiskohtien tarkastelua yleisesti kiinnostavien teemojen ja havaintojen esille tuomiseksi sekä ymmärrettävyyden lisäämiseksi laajaa lukijakuntaa silmällä pitäen.

2. Yksityisyys käsitteenä

Yksityisyyden käsitettä on yritetty määritellä vaihtelevalla menestyksellä sitä koskevassa kirjallisuudessa. Esimerkiksi pelkästään Amazon-verkkokaupan kirjahaku termillä ”yksityisyys” (privacy) antaa yli 12 000 ja Google Scholar -verkkopalveluhaku yli 4 miljoonaa osumaa. Yksikäsitteinen ja perusteltu yksityisyyden käsitteen määrittely on hankalaa ja loputtoman väittelyn lähde, koska (Westin 2003):

> “yksityisyys on sidottu sosiaalisiin normeihin siitä, mikä katsotaan hyödylliseksi, neutraaliksi tai vahingolliseksi yhteisen hyvän kannalta”.

Muita luonnehdintoja yksityisyyden käsitteen määrittelemisen vaikeudesta ovat mm. seuraavat:

> ”Yksityisyys on liikkuva kohde, joka muuttuu ajan kuluessa. Ihmiset määrittävät ja arvottavat sen eri tavoin. Lisäksi yksityisyyttä punnitaan muita arvoja vastaan, kuten yhteiskunnan turvallisuuteen nähden.” (Prescient 2011)

> ”Yksityisyys on konseptina kaaos, kukaan ei voi pukea sitä sanoiksi. Yksityisyys on liian epämääräinen käsite lainsäädännön luomiseen ja tuomiovallan ohjaamiseen.” (Solove 2006)

Yksityisyyden monimuotoisuudesta huolimatta on tarpeen yrittää muodostaa intuitiota selkeämpi käsitteen määrittely.

2.1 Yksityisyyden elementtejä

Yksityisyyskäsitteen luonnehdinnan hankaluuksista huolimatta siihen näyttää kuitenkin liittyvän selvästi tiettyjä keskeisiä elementtejä: ”Yksityisyys sisältää hallinnan/määräysvallan itseä koskevaan kommunikaatioon ja vuorovaikutukseen,

joka puolestaan vähentää haavoittuvuutta ja lisää henkilökohtaiseen päätöksentekoon ja käyttäytymiseen liittyviä mahdollisuuksia" (Margulis 2003).

Yksityisyyden ja turvallisuuden (security) suhde on monimutkainen. Yksityisyyttä ei voi olla ilman turvallisuutta, ts. ilman tietosuojan tuomaa varmuutta henkilökohtaisen tiedon yhtenäisyyttä, saatavuutta ja luottamuksellisuutta ei voida taata. Yksityisyyden loukkaamista perustellaan toisaalta turvallisuudella. Esimerkiksi viimeaikaisia NSA:n (National Security Agency) yksityisyyden suojaan liittyviä rikkomuksia on perusteltu Yhdysvaltojen kansallisella turvallisuudella. Onkin esitetty (Omtzigt & Schirmer 2015), että moderneissa yhteiskunnissa kaikkialle ulottuvan tarkkailun ja sitä kautta tapahtuvan yksityisyyden suojan rikkomisen hyväksyminen lisääntyy, koska yleinen yhteiskuntaa koskevien riskien toteutumisen sieto on jatkuvasti vähenemässä.

Länsimaisen yksityisyyskäsityksen historia on pitkä. Artikkelissa "Yksityisyyden historia" (History of privacy) Holvast (2009) on pyrkinyt kuvaamaan sitä informaation käsittelyn näkökulmasta. Yksityisyys käsitteenä on lähtöisin antiikin Kreikasta, jossa tehtiin selvä ero eristyneisyyden (solitude) ja yhteisön (society) sekä julkisen (public) ja yksityisen (private) välillä. Yksityisyyttä käsiteltiin esim. Euroopassa lakitapauksissa jo 1400-luvulla, jolloin se liitettiin kotiin, perhe-elämään sekä kirjesalaisuuteen (Langheirich 2009). Holvastin mukaan eurooppalaisten suorittama Yhdysvaltain kolonisaatio vahvisti edelleen yksityisyyttä maanomistuksen muodossa – kodista tuli paikka yksityisyydelle.

Vuosisadan alussa yksityisyyden suojan ajatukseen vaikutti erityisesti Harvard Law Review'ssa joulukuussa 1890 julkaistu Warrenin ja Brandeisin artikkeli "The Right of Privacy", jossa keskitytään lähinnä "oikeuteen olla yksin" ja viitataan sen ajan keltaisen lehdistöön ja kuvien julkaisemiseen – teemoihin jotka ovat edelleenkin ajankohtaisia. Vaikutteita ko. artikkeliin antoi Ranskan vuoden 1891 lehdistölaki (Neuvonen 2014).

Nykymuotoisen länsimaisen yksityisyyskäsitteen voidaan katsoa syntyneen 1960-luvun jälkeen ensiksi lähinnä Yhdysvalloissa, jossa perusteet luotiin Alan Westinin artikkelisarjassa Columbia Law Review -julkaisussa ja kirjassa Privacy and Freedom (1967). Tämän jälkeen lähes kaikissa yksityisyyttä käsittelevissä julkaisuissa on viitattu Westinin tuotoksiin. Westinin määrittelyn mukaan yksityisyys koostuu seuraavista seikoista:

- Yksinäisyydestä (solitude), joka on eristyneisyyden (seclusion, isolation) ja yksin olemisen tila (ihmiskontaktien poissaolo). Toisaalta se merkitsee myös vapautta olla olematta muiden havainnoinnin kohteena.
- Intimiteetistä (intimacy), jolla tarkoitetaan yleisesti tunnetilaa, jossa ollaan läheisessä henkilökohtaisessa yhteydessä (henkilökohtainen suhde).
- Anonymiteetistä (anonymity), vapaudesta olla julkisesti tunnettu.
- Varaumasta (reserve), halusta rajoittaa toisten ihmisten lähestymistä ja kanssakäymistä sekä olettamuksesta, että muut huomaavat ja kunnioittavat tätä pyrkimystä.

Westinin hahmotelman jälkeen erilaisia määrityksiä on luonnollisesti lukemattomia, mutta tämän raportin tarkastelun kannalta voidaan käyttää yksityisyyden käsitteeseen liittyvää yksinkertaistusta (Westin 2003):

> ”Yksityisyys on yksilöiden, ryhmien tai instituutioiden oikeutettu vaatimus määritellä itse milloin, miten ja missä laajuudessa heitä koskevaa tietoa voidaan jakaa muille.”

Ottaen huomioon tarkastelun konteksti – liikkumiseen liittyvät palvelut ja niihin hyvin usein keskeisesti liittyvä paikkatieto – voidaan käyttää Duckhamin ja Kulikin (2006) esittämää laajennettua määritelmää:

> ”Paikkatiedon yksityisyys on informaation yksityisyyden erityistapaus, joka määrittää yksilöiden, ryhmien tai instituutioiden oikeutetun vaatimuksen määritellä itse milloin, miten ja missä laajuudessa heitä koskevaa paikkatietoa voidaan jakaa muille”.

Yksityisyyteen liittyy voimakkaasti siis yksityiseksi koetun tiedon hallinta, jota on pyritty selittämään mm. Communication Privacy Management -teorian avulla (Petronio & Reierson 2009). Tämän teorian mukaan keskeiset piirteet yksityisen tiedon jakamiselle ovat seuraavat:

- Yksilöillä on vahva uskomus, että he omistavat yksityisyyteensä liittyvän tiedon ja että heillä on oikeus hallita sitä.
- Tämän tiedon hallintaa varten he kehittävät säännöstön (privacy rules) omien arvotustensa mukaan.
- Kun yksityisyyttä koskevaa tietoa jaetaan, tiedon luonne muuttuu – siitä tulee yhdessä omistettua niiden luetettujen osapuolten kanssa, joille tieto uskotaan.
- Ideaalitapauksessa henkilö ja luotetut osapuolet neuvottelevat ne säännöt, joilla tietoa välitetään edelleen kolmansille osapuolille. Koska tätä ”säännöstöä” ei säännöllisesti ja aktiivisesti päivitetä, syntyy ”rajankäynnin turbulenssia” (boundary turbulence), josta taas on seurauksena epäluottamusta, epäluuloa ja epävarmuutta koskien ko. yksityisen tiedon jakamista edelleen.

Ennen kuin lähdetään tarkastelemaan yksityisyyttä yksityiskohtaisemmin, on syytä tutkia, mitä eroa on henkilöön liitetyllä (personal information) ja yksityisellä tiedolla (private information). Jälleen joudutaan toteamaan, että rajanveto on varsin haastavaa. Pikaisesti ajateltuna henkilöön liitetty tieto voi olla esimerkiksi (WEF 2011)

- identiteettiin (digitaalinen) liittyvää, kuten nimi, sähköpostiosoite, kotiosoite, puhelinnumero, sukupuoli, ikä jne.
- yhteystietoja toisiin ihmisiin ja instituutioihin (työpaikka, valtion hallinnollinen tieto jne.)

- taloudellista tietoa, esim. pankkitransaktiot
- erilaisia kommunikaatiolokeja: sähköpostit, tekstiviestit, sosiaalisen verkon päivitykset jne.
- terveystietoja.

Kyseinen tieto voidaan joko luovuttaa vapaaehtoisesti tai se voidaan tuottaa yhdistelemällä sitä eri lähteistä. Yhdysvalloissa käytetään henkilöön liitettävästä tiedosta käsitettä PII (Personal Identifiable Information) ja Euroopassa käsitettä ”personal data”. Molemmat käsitteet ovat kuitenkin melko epämääräisesti määriteltyjä. Esimerkiksi EU:n direktiivi 95/46/EC kuvailee, mitä ko. henkilöön liitettävä data voisi olla, mutta jättää kuitenkin sen tarkemman määrittelyn auki (EU 1995).

Suomen lainsäädännön (Henkilötietolaki 22.4.1999/523) mukaan henkilötiedolla tarkoitetaan ”kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi”. Tässä raportissa käytetään lainsäädännön henkilötiedosta käsitettä ”henkilöön liitettävä tieto” samassa merkityksessä kuin termiä ”henkilötieto”.

McCullagh (2008) on pyrkinyt määrittelemään eron henkilöön liitetyn tiedon ja yksityisen tiedon välillä seuraavasti: yksityinen tieto on henkilöön liitettävän tiedon osajoukko, jonka yksilö haluaa pitää ehdottomasti salaisena ja jonka käyttöön hän haluaa pidättää hallintaoikeuden.

2.2 Yksityisyyden merkitys

Nyky-yhteiskunnassa yksilöä koskeva tieto ei enää näytä olevan pelkästään hänen omassa hallinnassa, vaan siitä on tullut uuden liiketoiminnan väline. Ne, jotka eniten näyttäisivät hyötyvän siitä kaupallisesti, ovat julistamassa yksityisyyttä kuolleeksi. Esim. entinen Sun Microsystemin toimitusjohtaja Scott McNealy sanoi jo 1999 kuuluisaksi nousseen toteamansa (Sprenger 1999):

> ”You have zero privacy anyway – Get over it” eli vapaasti suomennettuna ”sinulla ei kuitenkaan ole mitään yksityisyyttä – yritä päästä sen yli”.

Vastaavan kaltaisia yksityisyyttä vähätteleviä lausuntoja ovat antaneet sittemmin mm. Googlen toimitusjohtaja Eric Schmidt ja Facebookin perustaja Mark Zuckenberg. Ironista sinänsä, että esim. Schmidt loukkaantui syvästi, kun CNET News on-linen toimittaja julkisti tietoja, jotka oli kerätty puolessa tunnissa julkisista lähteistä Googlen omalla hakukoneella; tiedot koskivat Schmidtin kotiosoitetta, palkkaa, naapurustoa, harrastuksia ja poliittisia lahjoituksia.

Tämän tyyppiset mielipiteet herättävät kysymyksen siitä, mihin yksityisyyttä ylipäätänsä tarvitaan. B. Moore on havainnut (Moore 1984), että ”yksityisyys on sosiaalisesti syntynyt tarve – ilman yhteiskuntaa ei olisi yksityisyyden tarvetta”. Solove

(2006) puolestaan näkee yksityisyyden helpottavan ”sosiaalista kitkaa”, sillä se mahdollistaa toiminnan, joka olisi muuten hankalaa tai mahdotonta toteuttaa.

Sosiologisten ja psykologisten tutkimusten mukaan yksityisyys on henkilökohtaisen autonomian (yksilöllisyyden) kannalta keskeistä. Se tukee normaalia henkistä toimintaa, tasapainoisia henkilösuhteita ja persoonan kehittymistä. Jopa ”liberaalisen yksityisyysteorian” arvostelijat (Cohen 2013) myöntävät, että yksityisyys on keskeinen rakennusosa yksilöllisyydessä.

Yksityisyyttä tarvitaan myös tunteiden purkamiseen. Se tarjoaa mahdollisuuden rentoutumiseen (olla oma itsensä), pakoa stressaavasta ympäristöstä ja kiukun, turhautumisen, ahneuden sekä muiden negatiivisten tai vahvojen tuntemusten purkamisen joutumatta naurunalaiseksi tai häpeään. Kolmantena yksityisyyden tehtävänä on itsetarkastelu ja päätöksenteko – yksityisyys avaa mahdollisuuden luovuuteen. Yksilöt tarvitsevat tilaa ja aikaa tiedon käsittelyyn, ja oma rauha mahdollistaa vaihtoehtojen punninnan ja seurausten pohdinnan.

Toinen tämän tutkimuksen kannalta tärkeä tarkastelun lähtökohta on yksityisyyden merkitys taloudessa ja innovaatioissa. Ensimmäistä kertaa ihmiskunnan historiassa yrityksillä ja yhteisöillä on kyky tarkkailla ja rekisteröidä yksilöiden käyttäytymistä hyvin yksityiskohtaisesti. Tilanne mahdollistaa massoille personoitujen tuotteiden ja palveluiden tarjoamisen siten, että molemmat osapuolet hyötyvät tilanteesta. Yritykset voivat synnyttää taloudellista toimeliaisuutta uusien palveluiden ja tuotteiden muodossa, saada uusia tulolähteitä ja voittoa. Julkiset organisaatiot voivat puolestaan kohdentaa resurssit aiempaa tehokkaammin.

Henkilöön liittyvän tiedon hyödyntäminen onkin luonut kokonaisen uuden talouden. Henkilökohtaisten tietojen keräämisen ja käsittelyn kustannukset ovat laskeneet siten, että kuka tahansa voi olla riittävän kiinnostava kohde seurattavaksi:

> ”If you’re not paying for something, you’re not the customer; you’re the product being sold”[1] eli ”jos et maksa jostain, et ole asiakas vaan myytävä tuote”.

Näin sanotaan internetmeemissä. Tämä kuvaa tilannetta, jossa ”ilmaiset” onlinepalvelut tuottavat rahaa keräämällä henkilökohtaisia tietoja, kun niiden tarjoajat myyvät keräämänsä tiedot (kuluttajaprofiilit) markkinoijille viestinnän kohdentamiseksi tehokkaammin.

Henkilöön liittyvä tieto on ns. ei-vähenevä hyödyke taloudessa, eli sen käyttö ei vähennä ”varastosaldoa”. Sama tieto voidaan myydä useamman kerran useille eri asiakkaille. Nämä uuden henkilöön liitetyn tiedon markkinat ovat valtavat ja tuotot suuria, esimerkiksi kotiosoitteen hinta USA:ssa on arvion mukaan n. 0,50 dollaria, ajokortin numeron 3 dollaria ja sosiaaliturvatunnuksen 8 dollaria. Facebookin arvioidaan saavan tuottoa 1–12 dollaria vuodessa käyttäjää kohti häneen liitetyn tiedon edelleen markkinoinnista. Tämä on kuitenkin vaatimatonta Googleen verrat-

[1] Meemin tarkka alkuperä on tuntematon, ks. http://www.metafilter.com/95152/Userdriven-discontent#3256046

tuna: esim. erään arvion mukaan Google teki hakukoneellaan pelkästään vuonna 2011 liikevaihtoa 14,7 dollaria 1000:ta hakua kohden myymällä hauista saatavaa tietoa mainostajille (Kelly 2012, Mullin 2012).

Klassisen taloustieteen näkökulmasta – erityisesti ns. Chicagon koulukunnan edustajien Posnerin, Stiglerin jne. mukaan – yksityisyys on häiriö markkinoiden tehokkuudelle, koska se piilottaa mahdollisesti relevanttia tietoa muilta taloudellisilta toimijoilta (tiedon asymmetrisyys) ja pienentää siten kilpailua ja hyvinvointia. Goldfarb ja Tucker (2011a) ovat alustavissa tutkimuksissaan todenneet, että henkilöihin liitetyn käytöllä on positiivisia vaikutuksia talouteen:

- Suosittelujärjestelmät, jotka perustuvat käyttäjien ostohistorioihin, voivat lisätä liikevaihtoa 0,3 % ja ohjaavat ostoksia korkeamman tuoton tuoteryhmiin.
- Kuluttajien tarkkailu voi parantaa yritysten toiminnallista tehokkuutta ja lisää asiakastuntemusta.
- Hakukoneiden antamia tietoja voidaan käyttää kysynnän ennustamiseen ja siten toimitusketjujen tehokkaampaan hallintaan.

Yksityisyys vähentää markkinainformaatiota ja siten pienentää kuluttajille tulevaa etua ja toisaalta yritysten voittoja. Esimerkkinä on käytetty mm. Euroopan tietosuoja-asetusta, joka rajoittaa yritysten yksilöä koskevan tiedon keruuta, ja tutkimusten mukaan se pienentää online-mainosten tehokkuutta jopa 65 %. Goldfarbin ja Tuckerin toisen tutkimuksen mukaan yksityisyys ja innovaatiopolitiikka linkittyvät toisiinsa. Yksityiseksi laskettavan tiedon hyödyntämisellä on merkittävä vaikutus sitä käyttävään teollisuuteen ja sen kykyyn innovoida uusia tuotteita ja palveluita. (Goldfarb & Tucker 2011b.)

Taloudellisten vaikutusten positiiviseen tulkintaan on esitetty myös poikkeavia näkemyksiä. Esimerkiksi Varianin (1996) mukaan uusklassinen taloustiede ei tee eroa henkilöön liitetyn tiedon ja liikesalaisuuksien välillä. Lisäksi ko. uusklassinen tulkinta korostaa rationaalista päätöksentekoa yksityisyyteen liittyvien tietojen vaihdannassa – mikä harvoin kuitenkaan pitää paikkansa. Kolmansille osapuolille luovutettava, henkilöön liitetty tieto on ongelmallista, koska yksilö voi rationaalisella päätöksenteolla luovuttaa tietojaan palvelutarjoajalle oman nettohyödyn tavoittelemiseksi, mutta toisaalta hän ei saa hyötyä tietojensa edelleen myynnistä. Nettohyöty voi jäädä jopa negatiiviseksi esim. roskapostituksien ja identiteettivarkauksien takia. Näitä negatiivisia vaikutuksia ei käytännössä sisällytetä (internalisoida) yritysten tuloksiin.

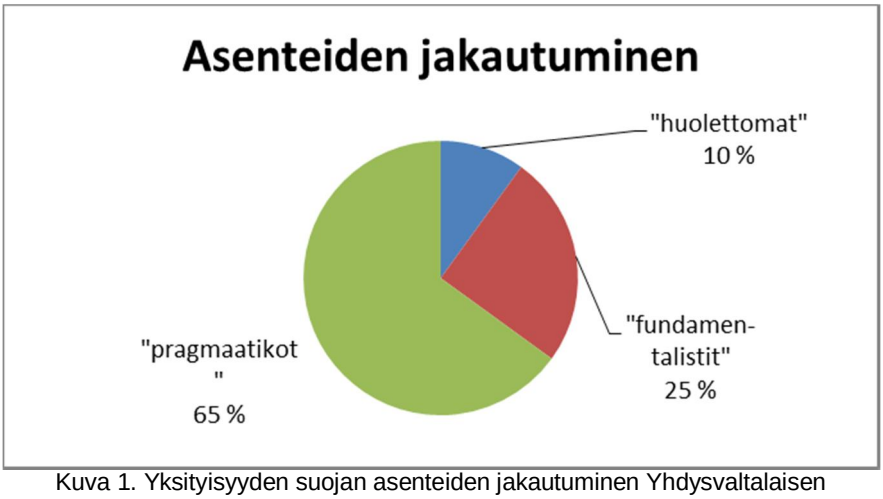
Toistaiseksi yritykset ovat perustaneet toimintansa siihen, että käyttäjät ovat huolettomia heihin liitetyn tiedon kaupallistamisessa, mutta suunta voi muuttua tulevaisuudessa. Yksityisyydellä on tunnistetusti taloudellinen arvo, jota käsitellään seuraavassa luvussa. Sellaiset henkilöt, jotka ovat valmiita maksamaan yksityisyydestään, ovat kuitenkin vähemmistö niihin nähden, jotka puolestaan ovat valmiita luopumaan yksityisyydestä käypää arvoa vastaan. Nykyisin esim. kuluttajat ovat valmiita suosimaan sellaisia toimijoilta, joiden tuotteet tai palvelut ovat halvempia, vaikka kauppiaiden toimintaperiaatteet rikkoisivatkin yksityisyyttä.

Erityisesti henkilökohtaisen paikkatiedon jakeluun näyttää kuitenkin jo muodostuneen käyttäjien varaumia. Amerikkalainen PEW-tutkimuslaitos havaitsi, että ns. paikkatiedon jakopalveluiden (location sharing) kasvu on ollut vähäistä vuosina 2011–2013 (Zickuhr 2013). Käyttäjäpenetraatio oli kasvanut vain 5 %:sta 8 %:iin, kun muiden vastaavien palveluiden yleistyminen on ollut merkittävästi suurempaa. McKinsey-markkinatutkimuslaitos on myös arvioinut, että yksityisyyteen liittyvät tekijät tulevat muodostamaan suurimman esteen henkilökohtaisen paikkatiedon hyödyntämiselle (Brown ym. 2014). Tällä on ennustettavasti seurannaisvaikutuksia esim. paikkatietoa hyödyntävien liikennepalveluiden käytön yleistymiseen.

2.3 Yksityisyyteen liittyvät asenteet ja paikkatiedon arvottaminen

Yhdysvaltalainen Harris Interactive on 90-luvun alusta tehnyt säännöllisesti vertailukelpoisia markkinatutkimuksia ihmisen yksityisyyteen liittyvistä asenteista n. 2000 henkilön otannalla. Tutkimukset on tehty siten (Kumaraguru & Cranor 2005), että haastateltavien jakauma vastaa USA:n väestön koostumusta. Näiden tutkimusten mukaan voidaan erottaa kolme asenneryhmää (kuva 1):

- Noin 10 % vastanneista kuuluu ns. luottavaiseen ryhmään (privacy unconserned), joita ei erityisesti huoleta, kuinka muut ihmiset ja organisaatiot käyttävät heidän tietojaan. Tähän ryhmään kuuluvat eivät myöskään halua uusia asetuksia tai lakeja yksityisyyttä suojaamaan.
- Noin 25 % vastanneista kuuluu ns. fundamentalisteihin, joilla on hyvin tiukka asenne yksityisyyden heikkenemiseen. Tämä ryhmittymä suhtautuu hyvin epäluuloisesti heistä tietoja kerääviin organisaatioihin, ja he ovat huolissaan tietojen hyödyntämisestä. He kannattavat uusia lakeja ja asetuksia yksityisyyden suojaan. Valintatilanteissa tämä ryhmittymä suosii yksityisyyden säilyttämistä palveluiden käytön sijaan, jos nämä seikat ovat tavoitteiltaan vastakkaisia.
- Noin 65 % vastaajista on ns. pragmaatikkoja, joilla on vahva tunne yksityisyydestä ja jonkinasteinen huoli tietojensa edelleen käytöstä, mutta valintatilanteessa he suosivat palveluita, jos he katsovat niistä olevan heille riittävästi hyötyä. Pragmaatikot ajattelevat, että tietoja keräävien organisaatioiden täytyy itse ansaita luottamus pikemminkin kuin että niillä automaattisesti olisi se.



Kuva 1. Yksityisyyden suojan asenteiden jakautuminen Yhdysvaltalaisen tutkimuksen mukaan (Kumaraguru & Cranor 2005).

Paikkatiedon luottamuksellisuutta on myös tutkittu useissa haastatteluissa USA:ssa, esimerkiksi PewReseachCenterin toimesta 2013 (Zickuhr 2013). Tähän otokseen osallistui 2250 yli 18-vuotiasta Yhdysvaltain kansalaista suurimmista kieliryhmistä (englanti, espanja). Tutkimuksen mukaan:

- N. 45 % aikuisista käytti paikkatietopohjaisia palveluita, jotka tarjosivat mm. reittiohjeistusta tai muuta informaatiota käyttäjän nykyisen sijainnin mukaan. 75 % älypuhelimen haltijoista käytti näitä palveluita, ja kyllästymispiste käytössä lienee jo saavutettu, koska vuoden 2012 vastaavan tutkimuksen jälkeen käyttäjämäärä ei enää ollut kasvanut (vuonna 2011 palveluita käytti vain 55 % älypuhelimen omistajista).
- N. 7 % haastatelluista käytti geo-sosiaalisia palveluita (”check-in”-palvelut), joissa paikkatietoja jaetaan ystävien kesken. Suosituimmat näistä palveluista olivat Facebook n. 40 % markkinaosuudella, Foursquare 18 % ja GooglePlus 12 %. Käyttäjämäärässä ei ollut tapahtunut merkittävää kasvua sitten vuoden 2011 vastaavan otannan.

On huomioitava, että näiden kahden edellä kuvatun palveluryhmän välinen raja on nopeasti hämärtymässä ja sosiaaliset paikkatietopalvelut ovat tarjoamassa myös muuta paikkatietoon perustuvaa sisältöä. Merkille pantavaa on se, että 35 % PEWin haastatteluun osallistuneista ilmoitti sulkeneensa paikkaseurannan joissain tapauksissa yksityisyyden suojaan liittyvistä syistä.

Toisaalta on syytä huomata, että löytyy myös ihmisjoukko, joka ei pidä käyttäytymisensä seuraamista millään tavalla tungettelevana. Yhdysvalloissa on markkinatutkimuslaitoksia, esim. Luth Research ja Datacoup, jotka molemmat tarjoavat rahaa käyttäytymisen seurannasta – esim. Luth sata dollaria kuukautta kohden

täydellisestä käyttäjän laiteseurannasta PC:n, tablettilaitteen tai älypuhelimen kautta. Tarjoukseen on jo tarttunut 20 000 PC- ja 6000 älypuhelinkäyttäjää. Myös markkinatutkimuslaitoksia isommat toimijat ovat liikkeellä: Verizon-operaattori (yli sata miljoonaa asiakasta) on käynnistänyt ”Smart Reward” -kanta-asiakasohjelman, jossa käyttäjän paikkatietoa ja nettiselailuinformaatiota kerätään markkinointitiedon myyntiä varten.

Liikennepalveluihin liittyvän paikkatiedon käytön asenneilmastoa on kartoitettu Euroopassa useissa eri hankkeissa. Näistä voidaan mainita Euroopan unionin CVIS (Cooperative vehicle-infrastructure systems) -ohjelma vuodelta 2007 (CVIS 2007), Tšekeissä Bilerin ryhmän toimesta tehty tutkimus (Biler ym. 2013) sekä Suomessa Tekesin rahoittama ja Aula Researchin toteuttama asennetutkimus vuodelta 2014 (Aula 2014). Eräänä osa-alueena kaikissa näissä tutkimuksissa on tarkasteltu käyttäjien suostumusta paikkatiedon luovuttamiseen. Tutkimusten tulokset tältä osin on koottu taulukkoon 1.

Taulukko 1. Paikkatiedon seurannan hyväksyminen eräiden eurooppalaisten tutkimusten mukaan.

Tutkimus (vuosi)	Otannan koko	Hyväksyntä %	Kieltäytyminen %	Ei mielipidettä %
CVIS, koko Eurooppa (2007)	7687	~54	~15	~20
Biler, Tšekki (2013)	502	~8	~67	~25
Tekes, Suomi (2014)	1087	~50	~34	~16

Esitetyt tutkimukset eivät ole täysin yhteismitallisia, ja riippuen hieman kysymyksenasettelusta tulokset voivat olla hyvinkin erilaisia. Jos esimerkiksi GPS (Global Position Systems) -perustainen seuranta mainitaan erityisesti, varauksellisuus paikkatiedon käyttöön kasvaa huomattavasti. Myös kansallisuuksien välillä on selviä eroja: erityisesti entisen itäblokin maissa ollaan yleisesti varautuneempia paikkatiedon hyödyntämiseen osana palveluita kuin läntisissä Euroopan maissa.

Pellin ryhmä (Pell ym. 2012) havaitsi tutkimuksessaan, että useimmat heidän haastattelemansa ihmiset eivät vastusta yrityksen omistuksessa olevan ajoneuvon seurantaa (58 % hyväksyisi tämän), kun taas yksityisen ajoneuvon seuraamisen hyväksyminen oli selvästi vähäisempää (45 % hyväksyisi). Vastaavan kaltainen pienempi asennetutkimus (otos 62 haastateltavaa) on tehty myös Suomessa liittyen ajoneuvoperustaisen verotuksen asenteisiin (Rohunen ym. 2014).

Rohusen ym. (2014) tutkimus vahvistaa jo aiemmin esitettyä asenneryhmien jakoa. Sen mukaan otannasta n. 14,5 % oli paikkatiedon käytön suhteen fundamentalisteja, 24 % huolettomia ja 60 % pragmaatikkoja, jotka hyväksyisivät ajoneuvon seurannan joitain hyödylliseksi koettuja palveluita, kuten reittiopastusta, ajotyylipalautetta tai automaattista ajopäiväkirjaa, vastaan. Rohusen ym. tutkimuksesta on

kuitenkin merkille pantavaa, ettei haastelluilla ollut aina selvää käsitystä, mitä tietoja ja mitä varten niitä kerätään ja mitkä ovat mahdolliset yksityisyyden suojan uhat. Tällöin huolettomien suuri määrä (24 %) voi olla todellisuuteen nähden suhteettoman iso.

Ihmisten yksityisyyteen liittyvä päätöksenteko perustuu prosessiin, jossa tietoja luovutetaan jotain hyödylliseksi koettua vastaan. Acquisti ja Grossklags (2007) havainnoivat tätä päätöksentekoa seuraavasti:

> ”Pidämme oikeutena suojata informaatiota itsestämme, mutta olemme valmiita luovuttamaan saman tiedon kuitenkin hyvin pientä korvausta vastaan. Olemme huolissamme merkityksettömistä yksityisyyden loukkauksista ja toisaalta ylenkatsomme sellaisia, jotka voivat aiheuttaa meille merkittäviä vahinkoja.”

Acquistin ja Grossklagsin (2007) mukaan yksilöt siis yleensä yliarvioivat yksityisyyden merkityksen ja helposti luopuvat siitä ilmaisia palveluita vastaan. Sama ilmiö on ollut toistettavissa useissa tutkimuksissa (Chin ym. 2012, Fisher ym. 2012, Pell ym. 2012). Esimerkiksi Krumm (2008) havaitsi, että tutkimuksessa, jossa 250:tä kuljettajaa seurattiin GPS:llä kahden viikon ajan, vain 20 % kieltäytyi tietojen edelleen luovuttamisesta muuhun kuin tutkimuskäyttöön, kun mahdollisuutena oli 1 %:n todennäköisyydellä voittaa n. 200 dollarin arvoinen Mp3-soitin.

Vaikeuksista huolimatta erityisesti paikkatiedon yksityisyyden arvoa on pyritty mittaamaan rahallisesti muutamissa merkittävissä tutkimuksissa, joissa koeasetelma on ollut samankaltainen (Danezis ym. 2005, Cvrcek ym. 2006, Brush ym. 2010). Näissä tutkimuksissa on käytetty paikkatiedon huutokauppamekanismia koeryhmän (otos 111 Danazisella, Cvrcekillä 1200, Bruschilla 32) keskuudessa siten, että jokainen osallistuja on voinut asettaa oman alimman hinnan, jolla luovuttaa itseään koskevan paikkatiedon joko tutkimuksen tai yleiseen käyttöön. Suhteellisen monimutkaisen koejärjestelyn yksityiskohdat joudutaan tässä sivuuttamaan, mutta johtopäätöksinä voidaan mainita seuraavat:

- Vain pieni osa tutkimuksesta kiinnostuneista kieltäytyy osallistumasta kokeeseen seurannan ehdot kuultuaan.
- Paikkatietoa luovutetaan melko edullisesti: noin kuukauden (28 päivän) seurantatiedon keskihinnaksi tutkimuskäyttöön muodostui 43 euroa Cvrcekin tutkimuksessa (tutkimuksen kohderyhmänä oli tietojenkäsittelyn opiskelijoita useissa Euroopan maissa) ja Danezisin tutkimuksessa 10–20 puntaa (tehtiin brittiläisten opiskelijoiden keskuudessa). Muuhun kuin tutkimuskäyttöön tieto luovutettaisiin kaksinkertaisella hinnalla.
- Naiset ovat varautuneempi tiedon jatkokäyttöön kuin miehet.
- Brushin tutkimuksen mukaan pitempiaikainen seuranta moninkertaistaa vaaditun korvauksen (kuukausi 100 dollaria, koko vuosi 500 dollaria keskimäärin).

Näihin alustaviin tuloksiin on kuitenkin syytä suhtautua varauksella – kohderyhminä ovat olleet lähinnä opiskelijat, joilla saattaa valtaväestöstä poiketen olla huomattavasti väljemmät asenteet yksityisyyttä kohtaan pienempien vastuiden ja sallivamman opiskelijaympäristön myötä. Täten näistä tuloksista ei voida johtaa yleispäteviä sääntöjä siitä, miten suuremmat käyttäjäryhmät arvottaisivat paikkatietonsa hyväksikäytön rahallisesti.

3. Digitaalinen jalanjälki ja yksityisyyteen liittyvät uhkatekijät

Ihmiset eivät usein ymmärrä, kuinka paljon paikkatietoa heidän päivittäisestä käyttäytymisestään jää ”digitaalisena jalanjälkenä” tietojärjestelmiin. Taulukkoon 2 on kerätty joukko paikantamiseen soveltuvia teknologioita, niiden paikannustarkkuuksia ja tietoja siitä, mihin käyttöympäristöön teknologia pääasiassa soveltuu tai on erikseen tarkoitettu.

Taulukko 2. Paikkatiedon erilaisia lähteitä, niiden paikannustarkkuuksia ja ensisijaisia sovellusympäristöjä.

Paikkatiedon lähde	**Paikannuksen tarkkuus**	**Ulkotilat**	**Sisätilat**
Soluverkkopaikannus	100–300 m, pikosoluilla jopa 20 m	x	(rajoitetusti)
Kiinteät IP-osoitteet	50 m		x
Maksukorttijärjestelmät	0,1 m		x
RFID	0,01–10 m	x	x
Bluetooth beacons	10–50 m	x	x
Matkapuhelinsovellukset (GPS)	5–10 m	x	
Kamerajärjestelmät	1–10 m (GPS)	x	x

Kansainvälinen puhelinjärjestö ITU (International Telecommunication Union) arvioi keväällä 2014, että maailmassa on yli seitsemän miljardia matkapuhelinliittymää, joista jokaisen sijainti voidaan paikantaa tukiaseman tarkkuudella jatkuvasti, mikä johtuu soluverkon toimintaperiaatteesta. Paikannustarkkuus vaihtelee solukoon mukaan 20 metristä (pikosolu kaupungissa) 20 kilometriin (makrosolut maaseudulla). Operaattorit voivat tarvittaessa paikantaa matkapuhelimen sijainnin signaalitunnisteiden avulla kolmiomittauksen avulla (AOA, TOA, TDOA -menetelmät).

Käyttäjän päätelaitteita voidaan paikantaa myös lähiverkkojen (WiFi) tukiasemien SSID (Service Set Identifiers) ja MAC (Media Access Control) -tietojen avulla. Kaupalliset toimijat, kuten Apple, Google ja Microsoft, ovat jopa osin käyttäjien tietämättä keränneet käyttäjien sijaintitietoja tukiasematiedon avulla. Kiinteiden päätelaitteiden sijainti voidaan likimain selvittää IP (Internet Protocol) -osoitteiden avulla käyttämällä esim. ARIN Whois, Geobytes tai Dnsstuff -palveluita, joskin paikannus ei ole aina erityisen tarkkaa. Sen sijaan matkapuhelinten paikantaminen IP-osoitteen perusteella on lähes mahdotonta, koska maantieteellisesti hyvinkin laajan alueen (satoja neliökilometrejä) matkapuhelimet voivat jakaa saman osoiteavaruuden (Balakhrisnan ym. 2009).

Toinen merkittävä paikkatiedon lähde ovat erilaiset korttijärjestelmät, kuten luottokortit, kanta-asiakaskortit, matkustuskortit jne. Jokaisella kerralla, kun käyttäjä suorittaa maksutapahtuman, taustajärjestelmään välittyy sen suorituspaikka. Erityisesti Yhdysvalloissa näitä tietoja käytetään tehokkaasti hyödyksi ostokäyttäytymisen seurantaan ja ennakointiin, luottokorttipetosten ehkäisyyn jne. Googlen maksujärjestelmä (Google Wallet) pystyy jo hyödyntämään käyttäjien paikkatietoa kohdentamalla käyttäjäkohtaisesti tarjouksia maantieteellisellä alueella. On ilmeistä, että korttijärjestelmistä kerättyä paikkatietoa tullaan jatkossa käyttämään entistä enemmän markkinoinnin apuna.

RDIF (Radio Frequency Identification) -perustaiset liikkumiskorttijärjestelmät voivat antaa hyvin yksityiskohtaista käyttäytymistietoa. Esim. Singaporen matkakorttijärjestelmä kerää tietoja matkan alku ja loppupisteestä, kestosta, matkustajatyypistä jne. Vastaavia järjestelmiä on useissa maissa (Suomessakin, kehitteillä on kansallinen liikkumiskortti Waltti) sillä erolla, ettei kaikkialla matkan päätepistettä voida vielä varmuudella tunnistaa. Kerättyä liikkumistietoa käytetään toistaiseksi lähinnä reittilinjaston suunnittelun perusteena, mutta kerättävissä olevalla tiedolla on runsaasti muitakin ajateltavissa olevia sovelluskohteita. Vastaavasti erilaiset RFID-perustaiset tietullijärjestelmät keräävät tietoa liikkumisesta, vaikkei tietoa suoranaisesti ole liitetty henkilöön vaan ajoneuvoon.

Uutena likimääräisen (n. 50 metriä tai tarkempi) paikkatiedon lähteenä toimivat Bluetooth-teknologiaan perustuvat Bluetooth-majakat (beacons). Nämä helposti asennettavat paristokäyttöiset laitteet (pariston elinikä 3–5 vuotta) soveltuvat erityisesti sisätilapaikannukseen. Nyt noin 10–50 dollaria (tulevaisuudessa 5–10 dollaria) maksavat Bluetooth-majakat lähettävät omaa tunnustaan, jonka älypuhelin vastaanottaa ja lähettää edelleen taustajärjestelmään, joka tunnistaa majakan sijainnin ja lähettää takaisin älypuhelimeen paikkaan liittyvän vasteen, esimerkiksi alennuskupongin kauppaan, tietoja lentoaseman portista jne. Bluetooth-majakoita arvellaan olevan viiden vuoden päästä käytössä 60–400 miljoonaa, ja vuonna

2018 n. 90 % älypuhelimista kykenee hyödyntämään niihin liittyviä palveluita käyttäjien niin halutessa. (Bluetooth 2015.)

Lisäksi erilaiset navigointijärjestelmät tuottavat runsaasti käyttäjälähtöistä paikkatietoa. Reitinsuunnittelupalvelut antavat usein mahdollisuuden anonyymiin reitinsuunnitteluun, mutta asiakkaat kirjautuvat järjestelmiin kasvavassa määrin palveluiden käytön helpottamiseksi ja personoimiseksi. Esimerkiksi matkapuhelinpohjaiset reititysjärjestelmät ovat jatkuvasti tietoisia käyttäjän sijainnista ja välittävät sitä ajoittain taustajärjestelmiin. Esimerkiksi Google Now – henkilökohtainen avustuspalvelu (personal assistant) pyrkii sekä aiemman käyttäytymishistorian että nykyisen sijainnin, hakujen ja kalenteritietojen perusteella ennakoimaan tulevia toimia ja siten opastamaan käyttäjää tarpeen mukaan.

Paikkatietoa kertyy kasvavassa määrin myös digitaalisen kuvaustekniikan kehityksen ansiosta. Kamerat pystyvät tallettamaan kuvauspaikan GPS-koordinaatit osana EXIF (Exchangeable Image File) -tiedostoa, ja kuvia ladataan Flickr- ja Picasa-tyyppisiin kuvapalveluihin, joissa jossakin tapauksissa EXIF-tiedot säilyvät. Viimeaikaiset kasvontunnistusalgoritmien kehitysaskeleet (ns. deep learning) mahdollistavat jo henkilön tunnistuksen samalla tarkkuudella katselukulmasta riippumatta kuin mihin ihminen kykenee (97 %:n tarkkuus) (Simonite 2014). Kun esim. pelkästään Britanniassa on yksi valvontakamera 32:ta ihmistä kohti (Suomessa tuskin tullaan kovin paljoa perässä), anonymiteetti joukossa ei enää jatkossa toteudu. Lisäksi jos hiljattain haudatun Google Glass -hankkeen tyyppiset datalasit yleistyisivät matkapuhelinten tapaan, kaikkialta olisi saatavilla henkilöön liitettävissä olevaa paikkatietoa. Sen mahdollistaisivat kameroiden määrän kasvu entisestään ja siihen liittyvä kasvontunnistus.

Epäsuoran paikkatiedon syntymisen lisäksi ihmiset jättävät digitaalista jälkeä tietoisesti. Erilaiset älypuhelinsovellukset, joilla reitit voidaan tallettaa GPS-paikannuksen tarkkuudella, ovat kasvattaneet suosiotaan. Näitä ovat mm. MyTrack, aktiviteettipäiväkirjat kuten Moves, Endomondo, Sports Tracker ja Strava sekä seurantasovellukset kuten Glympse jne. Niiden lisäksi paikkatietoa tallennetaan sosiaalisen median sovellusten kautta (osittain myös käyttäjien tietämättä), esimerkkeinä Facebook, Twitter ja Foursquare. Liikennepuolelta voidaan mainita Waze ja Automatic, jotka mahdollistavat käyttäjien paikkatiedon jakamisen ja hyödyntämisen.

Edellä esitettyjä paikkatiedon lähteitä tarkastelemalla voidaan havaita, että useimmat käyttäjille tarkoitetut ”ilmaiset” paikkatietoa keräävät palvelut ovat Yhdysvalloista lähtöisin muutamaa poikkeusta lukuun ottamatta. Raportissa ”Big Data: the next frontier for innovation, competition and productivity” (Maniyka ym. 2011) McKinsey-markkinatutkimuslaitos on arvioinut, että paikkatiedon määrä tulee näissä järjestelmissä lisääntymään vuosittain 20 % kasvuvauhdilla.

3.1 Käyttäjien mieltämät uhkakuvat

Raportissa ”On Location Privacy, and How to Avoid Losing It Forever” Blumberg ja Eckersley (2009) esittävät eräitä liikkumisen seurantaan liittyviä uhkakuvia:

- Kävitkö abortti- tai aids-klinikalla?
- Osallistuitko mielenosoitukseen tai muuhun kansalaisaktivismiin viime viikolla?
- Kävitkö ruokatunnilla hotellihuoneessa – sihteerin kanssa?
- Tapasitko riskirahoittajaa tai vierailitko yrityksessä X viime viikolla?

Aiemmin edellisen kaltaisen tiedon kerääminen oli työlästä ja kallista sekä edellytti valitun kohteen varjostamista. Nyt se on mahdollista helposti ja kustannustehokkaasti kaikkialla mukana kulkevien mobiililaitteiden antamien tietojen perusteella.

Haastattelututkimuksen (Tsai ym. 2009) mukaan tavalliset käyttäjät näkevät seuraavia uhkakuvia heitä koskevan paikkatiedon jakamiselle:

- kotiosoitteen paljastuminen henkilöille, joiden he eivät tahdo sitä tietävän
- ihmisten tunkeutuminen yksityisenä pidettävään tilaan, pahimmillaan ”stalking” eli ”vaaniminen”, ahdistelu ja häiriökäyttäytyminen, joka onneksi Suomessa on vielä suhteellisen vähäistä (Björklund 2010)
- sellaisten ihmisten kohtaaminen, joita ei haluta tavata
- hallituksen suorittama tarkkailu
- paikkatietoinen kohdemarkkinointi (”spamming”).

Kyseiset pelot eivät ole tuulesta temmattuja, sillä esim. 2012 Foursquare esti ”Girls Around Me” -sovelluksen käytön juuri häiriökäyttäytymiseen uhkaan vedoten. Sovelluksella pystyi seuraamaan käyttäjää lähellä olevien nuorten naisten sijaintipäivityksiä. Yhdysvaltain oikeusministeriön vuoden 2009 tutkimuksen mukaan enemmän kuin 3,4 miljoonaa yli 18-vuotiasta amerikkalaista on ollut häiriökäyttäytymisen kohteena. Näistä tapauksista n. 25 %:ssa on käytössä ollut jonkinlainen sähköinen väline ja n. 25 000 tapauksessa on käytetty GPS-perustaista teknologiaa (Baum ym. 2009, Catalano 2012).

Käyttäjien tietoisuutta paikkatiedon jakamisen haitoista on pyritty herättämään esim. PleaseRobme.com-verkkopalvelulla, joka on kerännyt paikkatietoja Twitter-lyhytviestipalvelusta ja tehnyt ne kaikille näkyviksi. Brittiläisen tutkimuksen mukaan (Dickinson 2011, Kelsey 2011) rikolliset ovat ajatelleet hyödyntävänsä sosiaalista mediaa mm. murtovarauksien suunnittelussa. 50 tuomitun murtovarkaan haastattelussa ilmeni, että 78 % heistä arveli Facebookin, Foursquaren ja Twitterin olevan hyödyllisiä rikosten suunnittelussa ja 74 % ilmoitti, että Google Street View on käyttökelpoinen tietolähde kotimurtojen kohteiden valinnassa.

Älyliikennepalveluihin, joissa käytetään runsaasti paikkatietoa, liittyviä uhkakuvia on selvitetty esim. Yhdysvaltain Government Accountability Officen (GAO) ja Privacy, Technology and the Law Committee of the Judiciaryn toimesta. Tämän tutkimuksen (GAO 2013) mukaan selkeinä uhkakuvina koettiin

- paikkatiedon myynti kolmansille osapuolille markkinointia varten
- identiteettivarkaudet, vaaniminen ja käyttäjien seuranta heidän siitä tietämättään
- sensitiivisen tiedon, kuten poliittisen tai uskonnollisen vakaumuksen, päättely käyttäjien jättämän jäljen perusteella.

Jo aiemmin esitellyssä Pellin ym. tutkimuksessa (2012) selvitettiin vastaavia uhkakuvia myös Euroopassa. Haastattelujen perusteella nämä uhat olivat samankaltaisia kuin jo edellä esitetyt, kuten

- henkilökohtaisen käyttäytymisen seuranta
- tietojen anonymisointiin liittyvät ongelmat (mm. niiden epäonnistuminen) ja niiden päätyminen internetiin ilman käyttäjien suostumusta
- ylinopeussakotus liikkumistiedon perusteella.

Viimeinen pelko ei ole mitenkään aiheeton. Esimerkiksi hollantilainen autonavigaattorivalmistaja TomTom myi Hollannin poliisille navigaattoreista käyttäjien pilvipalveluun lataamien tietojen perusteella ne paikat, joissa ylinopeudet olivat yleisiä. Tämän tiedon perusteella poliisi saattoi järjestää liikennevalvonnan ja kamerat ko. tieosuuksille. Älyliikennepalveluiden osalta on tehty myös palvelukohtaista uhkakartoitusta Algoe Consultant ja RappTrans -konsulttiyhtiöiden toimesta, mihin palataan myöhemmin älyliikennepalveluiden tarkastelun yhteydessä.

Henkilötietoihin perustuvat identiteettivarkaudet ovat muodostumassa todelliseksi ongelmaksi länsimaissa. US Bureau of Justice Statistics arvioi 2015 (Harrell 2015), että n. 17,6 miljoonaa kansalaista (n. 7 % yli 16-vuotiaasta väestöstä) on joutunut identiteettivarkauden kohteeksi. Niistä on aiheutunut käsittämättömän suuret 24,7 miljardin dollarin menetykset. Ne ovat kymmenen miljardia dollaria suuremmat kuin muut omaisuuteen kohdistuvat vahingot Yhdysvalloissa. Konsultointiyhtiö Deloitte on arvioinut, että vastaava luku Euroopassa olisi niinkin suuri kuin 0,4 % koko EU:n bruttokansantuotteesta. Vaikka suuri osa tästä liittyykin luottokorttitietojen väärinkäyttöön, henkilöön kohdistuvan tiedon välinpitämätön hallinta pahentaa tätä ongelmaa entisestään.

3.2 Käyttäjään liitetyn paikkatiedon perusongelmat

Paikkatiedon yksityisyyteen liittyy teoreettisesti muutama väistämätön perusongelma (Duckham 2010):

- Maantiede asettaa aina tiettyjä rajoitteita liikkumiseen: käyttäjät seuraavat polkuja ja teitä, jotka asettavat ehtoja yksityisyyden suojaamisen lähtökohtiin.

- Ihmisten liikkuminen ei ole satunnaista, vaan käyttäjät seuraavat aina joitakin toistettavia ja ennustettavia käyttäytymismalleja, jotka puolestaan lisäävät säännönmukaisuutta, joka mahdollistaa heidän tunnistamisensa ja siihen liittyvän tiedon väärinkäytön.

Erityisesti käyttäytymisen ennustettavuutta on tutkittu runsaasti (Gonzales ym. 2008, Eagle & Pentland 2009, Rhee ym. 2011, Scafetta 2011, Song 2010. Näiden tutkimusten perusteella voidaan todeta, että

- ihmisten käyttäytyminen muistuttaa tilastollisesti suuressa määrin satunnaista ns. Levy-kävelyä (Levy-walk), jonka mukaan suurin osa liikkumisesta muodostuu lyhyistä siirtymistä ja pitemmät ovat harvinaisempia
- ihmisten liikkumisessa on kuitenkin hyvin suurta ajallista ja tilallista (maantieteellistä) säännöllisyyttä. Liikkumisen ennustetarkkuus eri tutkimuksissa vaihteli 79–93 % välillä, ja ne voidaan jakaa kolmeen luokkaan: 1–10 km, 10–300 km ja 300–1000+ km, mikä noudattaa ns. käänteistä Pareto-jakaumaa. Pitkien siirtymien ennustettavuus on heikompi kuin lyhyiden, ja toisaalta ne ovat mm. kustannussyistä harvinaisempia.

Kyseiset tutkimukset siis vahvistavat selvän intuitiivisen käsityksen siitä, että ihmiset noudattavat tiettyjä päivittäisiä liikkumisrutiineja maantieteellisesti rajatulla alueella ja toisaalta tekevät ajoittain pitkiäkin matkoja, joiden ennustettavuus on huonompi. Yksityisyyden suojan kannalta tästä säännöllisyydestä muodostuu selvä ongelma, jota voidaan eritellä esim. seuraavan esimerkin avulla.

Montjoyen tutkimusryhmä (Montjoye ym. 2013) analysoi eurooppalaiselta operaattorilta saadun, tunneittain kerätyn 1,5 miljoonan käyttäjän soluverkon tukiaseman perusteella määritetyn paikkatiedon. Vaikka tieto oli anonymisoitu, vain neljän spatio-temporaalisen pisteen (ts. tukiasema-alueeseen liittyvän sijaintitiedon) avulla oli mahdollista identifioida 95 %:n tarkkuudella kyseisten sijaintien liittyvän samaan yksilöön ns. sormenjäljen avulla. Tämä ei tietenkään tarkoita sitä, että tiedettäisiin varmuudella kyseinen henkilön identiteetti suoraan, mutta liittämällä ns. ulkopuolista tietoa, kuten henkilön tunnistus ja hänen liikkeensä, voidaan jäljittää siis hyvin suurella todennäköisyydellä.

Esimerkiksi Apple ja Google ovat keränneet vastaava tietoa käyttäjien vierailemista WiFi-tukiasemista (jotka ovat sijanneiltaan siis suhteellisen staattisia), ja Apple on jakanut ko. tietoa ”partnerien ja lisenssikumppaniensa” kanssa väittäen tiedon olevan anonymisoitua ja siten mahdotonta yhdistää johonkin tiettyyn henkilöön (Apple 2011). Montjoyen ym. (2013) tutkimuksen valossa kyseistä väittämää voidaan pitää vähintäänkin epäuskottavana.

Vastaavaa liikkumistietoa kertyy erityisesti erilaisista liikennepalveluista. Esimerkiksi maailmalla suositut ilmaiset Waze-navigaatiosovellus ja Ubertaksisovellus keräävät valtavan paikkatietoaineiston paljon suuremmalla tarkkuudella (GPS:n paikannustarkkuudella) kuin soluverkko-operaattorit kykenevät, joten tunnistustarkkuus ja sitä myöten myös yksityisyyden suojaan liittyvät haasteet ovat sitäkin suuremmat.

3.3 Yksityisyyden loukkauksista aiheutuvat vahingot

Yksityiseksi katsottujen tietojen vuotamisesta aiheutuvia vahinkoja on ollut hyvin vaikea arvioida (Acquisti ym. 2008). On esitetty kuitenkin (Cavoukian 2009), että yksityisyyden suojan ennakoivat (proaktiiviset) käytännöt olisivat pitkällä aikajänteellä edullisempia kuin ns. reaktiiviset toimenpiteet yksityisyyden loukkaamisen jälkeen. Yksityisyyden loukkauksista aiheutuu mahdollisesti seuraavia haittoja:

- Suorat viranomaisten antamat sakot. Esim. Yhdysvalloissa Federal Trade Commission voi antaa yritykselle 15 miljoonan dollarin sakon yksityisyyden suojan loukkaamisesta. Euroopassa on vastaavasti ehdotettu esim. maksimissaan 100 miljoonan euron sakkoa tai vuotuiseen liikevaihtoon sidottua 5 % sakkoa yksityisyyden suojaan liittyvästä leväperäisyydestä.
- Joukkokanteet USA:ssa. Esim. TD Amertrade tuomittiin nimien, kotiosoitteiden ja puhelinnumeroiden vuotamisesta 2,5–6,5 miljoonan dollarin korvauksiin 2011. Euroopassa ollaan kulkemassa samaan suuntaan, jolloin esim. kuluttajaorganisaatiot voivat nostaa joukkokanteen tyyppisiä vaateita yrityksiä kohtaan.
- Käyttäjien luottamuksen menettäminen. Brändejä pidetään yritysten keskeisinä voimavaroina, joita on kallista rakentaa ja ylläpitää. Tahrat yksityisyyden suojassa saattavat johtaa brändiarvon laskemiseen, asiakkaiden menetykseen, uusien asiakkaiden saannin hankaloitumiseen ja tuottojen vähenemiseen.
- Kriisinhallinta voi käydä kalliiksi. Sony PSN:n (PlayStation Network) tietovuodon (jossa vain pieneltä osata 77 miljoonasta käyttäjästä varsinaiset luottokorttitiedot vuosivat muiden henkilötietojen mukana) jälkihoito maksoi 171 miljoonaa dollaria ja aiheutti 15 miljoonan dollarin menetyksen joukkokanteena ja 425 000 dollarin sakon Yhdysvalloissa (Wikipedia 2015).

Tutkimusten mukaan kaikki nämä haittavaikutukset eivät välttämättä kuitenkaan realisoidu käytännössä. Esimerkiksi luottamuksen menetyksestä ei ole varsinaista näyttöä. Asiaa on tutkittu (Acquisti ym. 2008, Gatzlaff & McCullough 2010, Gangewere 2013) seuraavan hypoteesin avulla: Yrityksen pörssiarvon tulisi kärsiä yksityisten tietojen vuotamisen paljastuttua. Näiden tutkimusten mukaan yrityksen pörssiarvo kyllä laskee lyhytaikaisesti yksityisyyttä koskevan tietovuodon jälkeen, mutta palautuu jälleen ennalleen pitemmällä tarkastelujaksolla. Tietointensiiviset yritykset näyttävät kärsivän kurssin laskusta hieman lyhytaikaisemmin kuin muilla toimialoilla vaikuttavat pörssiyritykset.

Toinen käyttäjien luottamuksen menettämistä koskeva havainto perustuu Afrozin ym. (2013) tutkimukseen koskien Apple IOSin yksityisyyden suojan murtoa ja edellä kuvattua Sony PSN:n tietovuotoa sekä Facebookin yksityisyyssuoja-

asetuksia koskevien muutosten tarkasteluun. Tutkimusten mukaan käyttäjien luottamus ko. yritykseen ei ollut vähentynyt välittömästi tapauksien julkistuksen jälkeen eikä vuotta myöhemmin. Osa käyttäjistä tosin menetti luottamuksen heti tapahtuman jälkeen, mutta vuoden kuluttua tästä luottamuspulasta ei enää ollut näyttöä – itse asiassa päinvastoin: Facebookin kohdalla luottamus oli jopa vahvistunut yritystä kohtaan vuoden kuluttua. Tutkijat selittivät ilmiötä ”väsymyksellä” (privacy fatique) ja sillä, että kuluttajat yleensä luottavat niihin yrityksiin, joiden tuotteita he käyttävät. Ainoastaan todella vakavat tietovuodot, kuten taloudellisesti merkittävien tietojen (esim. luottokorttitiedot) paljastuminen, lopettaisivat haastattelun mukaan (otos 600 haastateltavaa) yritysten palveluiden käytön. (Afroz ym. 2013.)

Luottamus on kuitenkin yritysten toiminnan kannalta keskeistä, ja erityisesti digitaalisten palveluiden kyberluotettavuus (”cyber trust”) on keskeinen osa nykyistä internetperustaista palvelutoimintaa (Dutton 2006), joten yksityisyyden loukkausten merkitystä ei pidä missään tapauksessa vähätellä. Päinvastoin mm. World Economic Forum (WEF) on esittänyt huolensa siitä, että henkilöön sidotun tiedon nopea kaupallistaminen heikentää käyttäjien luottamusta ja lisää heidän epäilyjään tietojen väärinkäytöstä (WEF 2011).

4. Yksityisyyden uhilta suojautuminen

Yksinkertaisin tapa suojautua edellä kuvatuilta yksityisyyden uhilta olisi luonnollisesti olla käyttämättä sellaisia palveluita, jotka mahdollistavat yksilön seurannan. Tämä tuskin on mahdollista nyky-yhteiskunnassa, sillä jo aivan yleisesti käytetyt peruspalvelut, mm. rahaliikenteen käyttö (maksukortit), liikkuminen (matkakortit) ja puhelimet, jättävät käyttäjästään digitaalisen jalanjäljen kuten jo aiemmin todettiin.

Käytännössä uhkakuviin liittyvien ongelmien ratkaisemiseen voidaan käyttää kahta periaatteellista lähestymistapaa:

- sääntelyä
- teknologista suojautumista.

Molemmat ovat jo käytössä, ja niillä on omat vahvuutensa ja ongelmansa. Sääntely lainsäädännön muodossa on voimakas väline, mutta koska teknologia edistyy nopeasti, sääntely tulee aina laahaamaan teknistä kehitystä jäljessä. Täten lainsäädäntö ei voi olla erityisen spesifistä tai teknologiasidonnaista, koska silloin se helposti muuttuu vanhanaikaiseksi ja merkityksettömäksi. Lainsäädäntö myös vaatii aina toimeenpanemista ja valvontaa; rikkomukset ovat aina mahdollisia joko tahattomasti tai tahallisesti, kuten paljon julkisuutta saanut NSA-tapaus osoittaa: se rikkoi selkeästi mm. Yhdysvaltain vuoden 1974 tietosuojalakia.

Teknologian käyttö yksityisyyden suojaamiseen kuulostaa houkuttelevalta, koska suojaus voitaisiin rakentaa sisään järjestelmiin ja siten ulkoiseen lainsäädännön valvontaan ei tarvitsisi kiinnittää niin paljon huomiota ja resursseja. Teknologiseen lähestymistapaan, esim. yksityisyydensuoja-arkkitehtuureihin, taas liittyy ongelmana se, että niitä pidetään liian rajoittavina kaupallisesta näkökulmasta ja toisaalta kalliina toteuttaa, sillä selkeät systemaattiset lähestymistavat ja työkalut ovat vielä puutteellisia.

4.1 Sääntely

Sääntelyyn on olemassa nykyisin kaksi lähestymistapaa:

- Kansainvälinen, EU:n ja kansallinen lainsäädäntö, joka painottaa oikeusopillista lähestymistapaa ja julkisen vallan roolia yksityisen tiedon käsittelyn ohjaamisessa ja valvonnassa.
- Toimijoiden (teollisuuden) itsesäätely, jossa vastuu yksityisyyden suojasta on niillä, jotka keräävät, prosessoivat ja jakavat yksilöön liittyvää tietoa. Osapuolet voivat yhdessä pyrkiä rakentamaan säännöstöä ja luottamusta kolmannen osapuolen, esim. TruSTe-tyyppisten yritysten, kanssa.

Ensimmäinen lähestymistapa on otettu käyttöön Euroopan unionissa ja jälkimmäinen taas Yhdysvalloissa, jossa tietoteollisuus on luonut omat säännöstönsä ns. reilujen informaatiokäytäntöjen (FIPS, Fair Information Practises) muodossa. Yksityinen sektori luonnostaan suosii jälkimmäistä, koska se antaa enemmän toimintavapauksia.

EU:n ja Yhdysvaltain lainsäädännön lähestymistavat poikkeavat siis huomattavasti toisistaan. EU:ssa yksityisyys on perusoikeus, joka ajaa kaiken muun ohi, kun taas Yhdysvalloissa yksityisyyden suojan lainsäädännön merkitys on huomattavasti vähäisempi. Näiden lähestymistapojen ero on niin perimmäinen, että sillä on suuri merkitys tietojen välittämisessä kansainvälisesti. Tulevaisuudessa eron otaksutaan vain syvenevän EU:n yksityisyydensuojalainsäädännön uudistuksen myötä ja EU:n tuomioistuimen lokakuussa 2015 Facebookin tietojen siirrosta antaman ennakkopäätöksen seurauksena.

4.1.1 EU:n yksityisyyden suoja

EU:n yksityisyyden suoja, joka koskee erityisesti liikkumiseen liittyvää tietoa, koostuu lähinnä seuraavista määrityksistä:

- ihmisoikeusjulistus, European Convention on Human Rights and Freedom 1950 (EU 1950)
- tietosuojadirektiivi, Data Protection Directive (95/46/EC) and Data Protection Regulation (EU 1995)
- sähköisen viestinnän tietosuojalaki Suomessa, Euroopassa yleisemmin E-Privacy Directive (2002/58/EC) (EU 2002)
- älyliikennedirektiivi, ITS Directive (2010/40/EU) (EU 2010)
- valmisteilla oleva yleinen tietosuoja-asetus, General Data Protection Regulation (EU 2012).

Lainsäädännön yksityiskohtiin ei tässä yhteydessä voida paneutua kovin syvälle, mutta eräitä keskeisiä piirteitä voidaan kuitenkin nostaa esille.

Ihmisoikeusjulistuksen mukaan jokaisella yksilöllä on pääpiirteittäin oikeus yksityisen ja perhe-elämän kunnioittamiseen, ja toisaalta sitä voidaan rikkoa ainoastaan pakottavissa tarpeissa (lainmukaisesti), kuten kansallisen turvallisuuden, yleisen turvallisuuden tai kansallisen hyvinvoinnin tähden. Lisäksi poikkeuksena on rikosten estäminen, terveyden ja moraalin turvaaminen ja muiden ihmisten

oikeuksien ja vapauksien takaaminen. Kyseistä julistusta on käytetty mm. ihmisten yksityisyyden suojaamiseen median sensaatiohakuisuutta vastaan.

EU:n tietosuojadirektiivi määrittää henkilötiedon (personal data) käsittelyn periaatteet EU:n alueella, ja se pohjautuu OECD:n suositukseen vuodelta 1980 (”Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data”). Asetuksen mukaan vaaditaan mm.:

- Läpinäkyvyyttä, ts. datan käsittelijän (controller) täytyy tehdä selväksi mm., mihin tarkoitukseen ja kuka vastaanottaa yksityiseksi katsottavaa tietoa. Luovuttajalla (data subject) tulisi olla oikeus kieltää datan käsittely.
- Laillista tarkoitusta (legimate purpose), ts. yksityinen tieto voidaan kerätä vain määrättyä tarkoitusta varten kohteen antaessa siihen selvästi luvan.
- Tiedon laatua, ts. kerätyn yksityisen tiedon tulee olla tarkkaa ja ajantasaista. Pääsääntöisesti on kiellettyä kerätä tietoa, joka paljastaa etnisen taustan, poliittisen kannan, uskonnollisen tai filosofisen katsomuksen, ammattiliittojen jäsenyyden, terveyden tai seksielämän.

On huomattava, että suositus sinänsä ei sellaisenaan ole EU:ssa yhtenäinen, vaan se vaatii kansallista lainsäädäntöä toteuttamiseen. Suomessa direktiivi toteutuu henkilötietolain muodossa (Henkilötietolaki 523/1999).

Vuoden 2002 Privacy and Electronic Communications- eli E-Privacy-direktiivi, Suomessa sähköisen viestinnän tietosuojalaki 16.6.2004/516, säätää henkilökohtaisen tiedon käsittelyn sähköisessä liikenteessä ja palveluissa. Suosituksen tarkoituksena on määrittää tiedon luottamuksellisuus, käsittelyn turvallisuus, tiedon säilyttäminen (hävittämiseen) ja roskapostin sekä verkkopalveluiden tunnisteiden (cookies) käyttöön liittyvät asiat. Vuoden 2004 ja 2005 Madridin ja Lontoon terroriiskujen jälkeen suositusta on täydennetty (Directive 2006/24/EC of The European Parliament and of the Council) koskien teletunnistetietojen säilytystä, mutta Euroopan korkein oikeus totesi vuonna 2014 sen rikkovan EU:n ihmisoikeuksia.

Sähköisen viestinnän tietosuojalain 2 §:n 1 momentin 9 kohdan mukaan paikkatiedolla tarkoitetaan tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin verkkopalvelun tai viestintäpalvelun toteuttamiseen. Teleyritys, lisäarvopalvelun tarjoaja ja yhteisötilaaja sekä niiden lukuun toimivat henkilöt saavat käsitellä paikkatietoja laissa säädetyin edellytyksin lisäarvopalvelun tarjoamiseksi ja hyödyntämiseksi.

E-privacy-direktiivi eli suomalainen sähköisen viestinnän tietosuojalaki korvautui 1.1.2015 Tietoyhteiskuntakaarella 7.11.2014/917, joka määrittää sijaintitiedoksi ”viestintäverkosta tai päätelaitteesta saatavaa tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun kuin viestin välittämiseen”. Lain mukaan ”sijaintitietoja, jotka voidaan yhdistää luonnolliseen henkilöön saa käsitellä lisäarvopalvelun tarjoamiseksi ja hyödyntämiseksi jos tilaaja tai käyttäjä, jota tiedot koskevat, on antanut siihen suostumuksensa, taikka suostumus yksiselitteisesti ilmenee asiayhteydestä tai jos laissa niin säädetään”.

Älyliikenteen palveluita säännellään EU:ssa ITS-direktiivillä (Directive 2010/40/EU). ITS-järjestelmät ovat määrittelyn mukaan ”kehittyneitä sovelluksia, joihin ei varsinaisesti sisälly älyä, mutta jotka pyrkivät tarjoamaan eri liikennemuotoja ja liikenteen hallintaa koskevia innovatiivisia palveluja ja jotka mahdollistavat sen, että eri käyttäjät saavat paremmin tietoa ja voivat hyödyntää liikenneverkkoja turvallisemmin, koordinoidummin ja ’älykkäämmin’”. Sovellusten ja palvelujen käyttöönotto ja käyttö edellyttävät henkilötietojen käsittelyä, ja niiden osalta noudatetaan tietosuojadirektiivin ja sähköisen viestinnän tietosuojalain yksityisyyden suojaa koskevia määräyksiä.

EU on uudistamassa koko henkilötietolainsäädäntöä ns. General Data Protection Regulation -mietinnöllä ja myöhemmin sen mukaisella asetuksella. Tämän tarkoituksena olisi paremmin vastata nykyisiin ja tulevaisuuden tietosuojahaasteisiin sekä yksinkertaistaa lainsäädäntöä. Yksi keskeisistä tavoitteista on yhdenmukaistaa EU:n lainsäädäntö, koska tietosuojadirektiivillä ei ole saatu aikaan toivottua yhdenmukaisuutta eri jäsenvaltioiden soveltaessa direktiivin säännöksiä eri tavoin.

Tavoitteena on yksilön oikeuksien lujittaminen edelleen ja niiden ulottaminen koskemaan kaikkia globaaleja toimijoita, jotka omassa liiketoiminnassaan keräävät eurooppalaisten henkilötietoja. Toteutuessaan tietosuoja-asetus saattaa kasvattaa yritysten ja yhteisöjen henkilöstö- ja hallintokuluja, koska se mm. edellyttää tietosuojavastaavan tehtävän perustamista kaikkiin julkisyhteisöihin sekä yrityksiin, jotka käsittelevät vuosittain yli 5000 henkilön tietoja. Oletettava lainsäädännön toteutumisaikataulu on vuonna 2016, ja sen arvioidaan olevan voimassa päivitettynä vuonna 2018.

4.1.2 Yksityisyydensuoja Yhdysvalloissa

Yhdysvaltojen yksityisyyttä koskeva lainsäädäntö on huomattavasti eurooppalaista väljempää. Liittovaltion laki The Privacy Act of 1974 (US DoJ 1974) määrittää yksityisyyden suojan yleiset periaatteet ns. Fair Information Practise -käytännöin, joilla lähinnä suojataan yksilöä liittovaltion viranomaisten mahdollisia salaisia rekistereitä vastaan mukaan lukien jopa salaiseksi luokiteltu tieto (classified information). Kyseistä lainsäädäntöä pidetään sisällöltään vaikeasti tulkittavana ja vanhentuneena, eikä se koske yrityksiä. Yhdysvalloissa ei ole EU:ta vastaavaa yksityisyyden suojaan liittyvää henkilörekisterilakia kuin ja terveystiedon käsittelyä koskevien määrittelyjen osalta.

Muita yksityiseen tietoon liittyviä säädöksiä ovat ECPA (Electronic Communications Privacy Act of 1986, US DoJ 1986) ja Telecommunications Act of 1996 (US DoJ 1996). ECPA koskee lähinnä liittovaltion oikeuksia salakuunteluun ja Telecommunications Act puolestaan lähinnä henkilötietojen keräämistä laskutuksessa, mutta se myös rajaa henkilötietojen luovuttamista kolmansille osapuolille. Näiden lisäksi vuoden 2002 E-Government Act määrittää eräitä velvollisuuksia, kuten yksityisyyden suojan vaikutusten arviointipakkoa liittovaltion organisaatioille yksityiseksi (PII) katsottavan tiedon käsittelyssä. Yhdysvalloissa ei ole lainsäädäntöä sijaintitiedon käsittelystä, joskin joitain osavaltiokohtaisia määrityksiä on olemassa.

Kuten jo aikaisemmin todettiin, USA:ssa yksityisyyteen liittyvän tiedon käsittelyssä nojaudutaan yritysten omaan sääntelyyn. Sijaintitiedon osalta tällainen käytäntö on esim. ”Best practices and Guidelines for LBS providers”, jonka on laatinut CTIA (International Association for the Wireless Telecommunications Industry, CTIA 2013). Sen sisältö on pääpiirteissään yhdenmukainen OECD:n yleisten yksityisyyden suojan suositusten kanssa:

- Käyttäjillä tulee olla kontrolli omaan sijaintitietoonsa, ja henkilökohtaista päätöksentekoa sen jakamisesta avustetaan informoimalla käyttäjää tiedon käsittelystä, jakamisesta ja hävittämisestä. Välitettäessä tietoa edelleen kolmansille osapuolille käyttäjiä on valistettava tiedon sisällöstä, jotta heille muodostuisi käsitys jakamiseen liittyvistä riskeistä.
- Kun käyttäjä tekee valinnan paikkatietoisten palveluiden käytöstä, hänellä tulisi olla oikeus päättää, siirretäänkö tietoa myös kolmansille osapuolille.
- Vaikka edelliset periaatteet ovatkin kannatettavia, käytännössä yritysten ”parhaat käytännöt” eivät tutkimusten mukaan toimi. Ongelmina ovat mm. yritysten tietoturvakäytäntöjen läpinäkyvyyden puutteet: esim. Google Playn palvelutarjonnassa yksityisyyskäytännöt puuttuivat kokonaan 52 %:lta sovelluksista ja Applelta 36 %:ssa tapauksista (FPF 2012).

Jo aiemmin mainittu GAO (Government Accountability Office) selvitti 2013 autoiluun liittyvien palveluiden tietoturvasäännösten tilaa ja totesi, että lähes kaikki johtavat palveluntarjoajat noudattavat jopa teollisuusalan omia suosituksia huonosti. Niistä palveluista, joita selvityksessä käytiin läpi, voidaan mainita mm. Google Maps, TOMTOM Live Service, Garmin Traffic, GM Onstar, Crysler UConnect sekä eräiden japanilaisten autonvalmistajien palvelut.

Yhdysvaltain kaupallisten palveluiden yksityisyydensuojakäytännöt ovat olleet niin huolestuttavassa tilassa, että Federal Trading Commission FTC on haastanut 23 yritystä oikeuteen kuluttajien yksityisyyden suojan rikkomuksista. Esimerkiksi Google joutui 2012 maksamaan 22,5 miljoonaa dollaria siviilioikeudessa FTC:n kanteen sovittelemiseksi.

Vuonna 2013 joukko senaattoreita ehdotti sijaintitietoa koskevaa ”The Geolocation Privacy and Surveillance Act” -lakialoitetta, joka koskee niin liittovaltion kuin yksityistenkin yritysten sijaintitiedon hallintaa ja käyttöä (Wyden 2013). Toinen samantyyppiseen tavoitteeseen tähtäävä aloite on senaattori Al Frankenin ”The Location Privacy Protection Act” (LPPA) vuodelta 2014 (Franken 2014). Se koskee mm. autonavigaattoreiden tiedonkäsittelyä. Molemmat lakialoitteet ovat tällä hetkellä (2015) kongressin kuultavana.

4.1.3 EU:n ja Yhdysvaltain Safe Harbour -sopimus

Kuten aiemmin todettiin, EU:n ja Yhdysvaltojen välillä on kitkaa yksityiseksi katsottavan tiedon käsittelyn periaatteista ja tällä hetkellä yhteistoiminnassa nojaudutaan OECD:n vuoden 1980 suositukseen ”Recommendation of the Council Concerning

Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" (OECD 1980). Tämä suositus asettaa mm. seuraavia perusperiaatteita:

- Tiedonkeruun rajoittaminen, ts. tietoa voidaan kerätä vain laillisia ja reiluja (fair) tarkoitusperiä varten kohteen suostumuksella.
- Keräämisen ja käsittelyn tarkoitusperät täytyy tehdä käyttäjille selväksi, ja tiettyä tarkoitusperää palvelevan tiedon tulee olla tarkkaa, laadukasta ja ajantasaista ja se tulee suojata asianmukaisesti
- Avoimuus, ts. yksityisen tiedon käyttöön ja jakeluun täytyy olla käytännöt ja menettelytavat ja, kohteella tulee olla mahdollisuus tarkistaa itseään koskevaa tietoa kohtuullisessa ajassa ja kohtuukustannuksin.
- Tahon, joka kerää, säilyttää, prosessoi tai jakaa henkilötietoa, täytyy olla valmis tilivelvollisuuteen ja esittämään noudattavansa edellä kuvattuja periaatteita.

Kyseisiä OECD:n suosituksia on päivitetty edellisen kerran 2013 ilman suurempia muutoksia varsinaisiin periaatteisiin. EU linjasi vuonna 2002, että EU:n kansalaisten henkilötietoja ei saa levittää EU:n ulkopuolelle, ellei ole takeita riittävästä yksityisyyden suojasta. Poikkeuksena tästä on ns. Safe Harbour -menettely, joka on Euroopan komission ja Yhdysvaltojen välinen kompromissisopimus EU:n lainsäädännön ja Yhdysvaltojen yritysten itsesäätelyperiaatteiden välillä. Periaatteessa Safe Harbour tukeutuu edellä kuvattuihin OECD:n suosituksiin tietyin tarkennuksin.

Yhdysvalloissa FTC on aktiivisesti markkinoinut Safe Harbour -ohjelman tarjoavan "riittävän" yksityisyydensuojan, mutta todellisuudessa se ei takaa EU:n suosituksen mukaista perussuojaa. Safe Harbour -ohjelma perustuu yritysten omaan ilmoitukseen, eikä sen noudattamista todenneta millään tavalla. Vuosien 2002 ja 2004 aikana EU katselmoi ohjelman ja totesi siinä olevan vakavia ongelmia. Vuonna 2008 yksityisyyden suojaan erikoistunut konsultti Chris Connoly selvitti (Connoly 2008), kuinka hyvin yritykset noudattivat Safe Harbour -ohjelman seitsemää kohtaa, ja osoitti, että osa yhdysvaltalaisista yrityksistä, jotka ilmoittivat sitä noudattavansa, eivät edes olleet mukana koko ohjelmassa (Safe Harbour Framework). Niistäkin, jotka olivat mukana, vain kolmannes pystyi täyttämään ohjelman minimivaatimukset. Vuonna 2013 EU:n komissio teki 13 parannusehdotusta Safe Harbour -ohjelman toiminnan kohentamiseksi, mutta käytännön tuloksia ei kuitenkaan ole vielä saatavilla.

Lokakuussa 2015 EU:n tuomioistuin Court of Justice of the European Union (CJEU) teki merkittävän Safe Harbour -menettelyä koskevan päätöksen (Maximillian Schrems vs. Data Protection Commissioner, Judgment in Case C-362/14), jonka mukaan eurooppalaisia koskevien tietojen siirtäminen Yhdysvaltain palvelimille on laitonta ja rikkoo EU:n tietosuojasuositusta (Data Protection Directive). Kyseisessä tapauksessa Facebookin irlantilaisissa palvelimissa olevia tietoja oli lähetetty käsiteltäväksi Yhdysvaltoihin. EU:n tuomioistuimen päätöksessä viitataan mm. Edward Snowdenin paljastuksiin NSA:sta ja todetaan, että Yhdysvaltojen

tietosuojakäytäntöjen ei voida katsoa takaavan riittävää yksityisyyden suojaa. Samassa yhteydessä EU:n tuomioistuin totesi, ettei Safe Harbour -menettely ole lainvoimainen. (CJEU 2015.)

Päätöksen käytännön merkitys ei ole vielä selvillä, mutta oikeusoppineiden käsityksen mukaan päätöksestä seuraa toistaiseksi ainakin se, että eurooppalaisten yritysten ja tietosuojaviranomaisten on estettävä palveluiden käyttäjien yksityisyyden suojaan kuuluvien tietojen siirtyminen Yhdysvaltoihin niin kauan kuin Yhdysvaltojen turvallisuusviranomaisilla on pääsy ko. tietoihin. Päätöksellä voi olla suuria vaikutuksia käynnissä oleviin Yhdysvaltain ja EU:n välisiin vapaakauppasopimusneuvotteluihin (TTIP, Transatlantic Trade and Investment Partnership).

4.2 Yksityisyyden suojaamisen tekniikkaa

Teknisten yksityisyyden suojan (PET, Privacy Enhancing Technologies ja TET, Transparency Enhanching Technologies) menetelmien tarkoituksena on vähentää yksityisyyden suojan rikkomuksia, minimoida henkilötietojen keruu, tarjota yksilöille henkilötiedon hallinnan mahdollisuus ja lisätä osapuolten välistä luottamusta. Teknologiset vaihtoehdot yksityisyyden suojan tukemiseksi jakaantuvat kahteen pääperiaatteeseen (Fritsch 2007):

- Läpinäkyvyyden lisäämisen menetelmät (transparency tools, privacy management) osoittavat, kuinka tietoa käsitellään ja keiden toimesta. Teknisiä mahdollisuuksia ovat esim. lokitiedostot ja ns. ”audit trailit” eli katkeamattomien kirjausketjujen vaatimukset.
- Piilottamisen menetelmät (opacity tools, privacy protection) pyrkivät puolestaan hävittämään käyttäjän identiteetin. Teknisiä esimerkkejä ovat erilaiset anonymisointiin liittyvät periaatteet.
- Jotta menetelmät olisivat käytännöllisiä, tulee niiden olla yleisesti sovellettavissa olevia, luotettavia, tehokkaita ja pitää lupauksensa. Jos menetelmää soveltava järjestelmä suojaa käyttäjää käyttökokemuksen kustannuksella, se yleensä hylätään.

Suojausmenetelmiin liittyvät tärkeimmät käsitteet, joihin seuraavissa alaluvuissa viitataan, voidaan määritellä seuraavasti (käytössä Pfitzmannin ja Hansenin [2005] termistöä):

- Anonymiteetillä tarkoitetaan sitä, ettei kohde (henkilö) ole erotettavissa muiden kohteiden joukosta ts. mahdollinen hyökkääjä/vastustaja (attacker/adversary) ei pysty riittävästi identifioimaan yksittäistä kohdetta kohdejoukosta. Suomen kielessä voidaan käyttää myös termiä nimettömyys ja sen vastakohtana identiteettiä.
- Pseudonymiteetti on kohteen tunniste, joka on muu kuin henkilön todellinen nimi. Suomen kielessä pseudonyymi (johdettu kreikasta sanoista speudo ja onuma, väärä nimi) on salanimi.

- Kahden tai useamman kiinnostavan objektin yhdistämättömyys (linkittämättömyys) tarkoittaa, että hyökkääjä/vastustaja ei voi riittävän suurella varmuudella erottaa, liittyvätkö kohteet toisiinsa vai eivät.

Sijaintitietoon perustuvissa palveluissa käyttäjän täytyy yleensä paljastaa todellinen sijaintinsa – esim. GP-koordinaattinsa tai katuosoitteensa – mahdollisesti epäluotettavalle palveluntarjoajalle, joka puolestaan tuottaa sijaintiin liitetyn tiedon, kuten karttalehden, kuvan tai muun datan. Joitakin palveluista voidaan käyttää täysin anonyymisti, jolloin käyttäjän todellista identiteettiä tai pseudonyymiä ei tarvita. Palveluntarjoaja on kuitenkin kasvavassa määrin tietoinen käyttäjän identiteetistä joko suoraan (käyttäjä rekisteröitynyt maksulliseen palveluun) tai epäsuorasti esim. laitetunnisteiden perusteella. Ongelmaksi muodostuu se, että palveluntarjoaja varastoi käyttäjän identiteetin ja sijainnin tietovarastoonsa. Käyttäjä ei voi muuttaa tai poistaa tietojaan jälkeenpäin, ja tietovarasto mahdollistaa käyttäjän käyttäytymisen analysoinnin. Analysoitu tieto voidaan sitten myydä joko sellaisenaan tai anonymisoituna eteenpäin siitä kiinnostuneille osapuolille.

Kun paikkatietopalvelujärjestelmien tavoitteena on antaa mahdollisimman tarkkaan paikkatietoon liittyvää oikeaa informaatiota, paikkatiedon yksityisyyden suojan menetelmien tavoitteet ovat siihen nähden päinvastaiset. Tarkoituksena on vaikeuttaa kohteen tunnistusmahdollisuutta ja paikkatiedon tarkkuutta, jolloin joudutaan puolestaan tyytymään heikompaan informaation laatuun ja sen myötä heikentyneeseen tiedon käyttökelpoisuuteen.

Paikkatiedon yksityisyyden suojaa voidaan määrittää kolmen suureen avulla (Liu 2009):

- k-anonymiteetti
- l-diversiteetti
- s-diversiteetti.

K-anonymiteetti ja l-diversiteetti ovat alun perin lähtöisin relaatiotietokantoihin liittyvästä anonymisoinnin tutkimuksesta. Tietojoukon sanotaan täyttävän k-anonymiteetin, jos jokainen tietue (tuple) tietojoukossa ei ole erotettavissa k -1 muusta tietueesta käyttämällä näennäistunnisteita (quasi-identifier). Näennäistunnisteet ovat attribuutteja, kuten syntymäaika, sukupuoli, sijainti jne., jotka voidaan linkittää ulkoiseen tietoon henkilön tunnistamiseksi. Täten hyökkääjä ei voi tunnistaa kohdetta kuin todennäköisyydellä 1/k, ja jos k saadaan riittävän suureksi, anonymiteetti voi olla käytännössä tyydyttävä. Vaikka k-anonymiteetti onkin perusidealtaan yksinkertainen, sen optimaalinen laskennallinen hakeminen on NP-täydellinen ongelma. Toisin sanoen tietueiden määrän kasvaessa laskenta-aika kasvaa ei-polynomisesti, mikä tekee eksaktin matemaattisen ratkaisun hakemisen käytännössä mahdottomaksi.

K-anonymiteetti on valitettavasti huono menetelmä mm. monidimensioisen (monista attribuuteista) koostuvan tietojoukon anonymisointiin. L-diversiteetti on k-anonymiteetin muunnos, joka hyödyntää tietojoukon tilastollisia ominaisuuksia. Menetelmässä lisätään uusi rajoite siten, että ekvivalenssiluokan jokaisen attribuutin on esiinnyttävä vähintään l kertaa, jotta hyökkääjä jää aina attribuuttien suhteen

huomattavan epävarmaksi, vaikka hänellä olisikin taustatietoa jostakin kohteesta. Tämä tarkoittaa, että tietoaineistossa (tai sen osassa) on oltava vähimmäismäärä valitun ominaisuuden esiintymiä, jolloin tunnistamisriski pienenee.

S-diversiteetti on kehitetty tieverkkoon liittyvien sijaintitietojen k-diversiteettiongelman lieventämiseksi niissä tapauksissa, kun jokin satunnaistettu alue koostuu vain yhdestä tiesegmentistä. Sijainnin sanotaan olevan s-diversioituva, jos on olemassa vähintään s ($s > 1$) segmenttiä, johon ko. sijainti voidaan kiinnittää.

Anonymisoinnista ja k- ja l-diversiteetistä kiinnostuneita lukijoita kehotetaan tutustumaan lähteeseen 0829/14/FI WP216 (Tietosuojaryhmä 2014) eli Tietosuojaryhmän lausuntoon 5/2014 anonymisointitekniikoista. Siinä kyseisiä menetelmiä ja niihin liittyviä ongelmia on kuvattu tarkemmin.

4.3 PET-menetelmiä ja niiden hyödyt

Piilottamisen menetelmät voidaan jakaa kahteen lähestymistapaan: anonymisointiin (anonymization) ja monimutkaistamiseen (obfuscation), joiden välinen raja on häilyvä, ja menetelmiä käytetäänkin usein yhdessä.

Paikkatiedon verhoamisella (spatial cloaking) tarkoitetaan menetelmiä, joilla käyttäjän tarkka sijainti häivytetään maantieteellisellä alueella. Menetelmien tehokkuuksia voidaan arvioida k-anonymiteetin ja sen suhteen, kuinka suurella todennäköisyydellä kohde voidaan tunnistaa tietyllä maantieteellisellä alueella. Lähestymistapoja tavoitteen saavuttamiseen ovat mm. Gauss-jakautuneen kohinan lisääminen sijaintitietoon ja mahdollisilta vaikuttavien valepisteiden lisääminen sijaintitiedoista muodostuviin polkuihin. Valitettavasti kuitenkin useat verhoamismenetelmät huonontavat sijaintipalvelun laatua eivätkä ole sellaisenaan sovellettavissa rajoitettuja liikkumisen mahdollisuuksia sisältäviin ympäristöihin, kuten tieverkkoihin.

Toimintaperiaatteen puolesta menetelmät voivat olla yhteistoiminnallisia (collaborative, TTP) tai yksintoimivia (non-collaborative, TTP-free) (Liu 2009). Yhteistoiminnalliset menetelmät perustuvat usein ajatukseen luotetusta kolmannesta osapuolesta (TTP, Trusted Third Party), esim. luotetusta välityspalvelimesta (proxy) tai vertaisverkosta (P2P, peer to peer), kun taas yksintoimivat eivät luota muihin osapuoliin kuin ainoastaan käyttäjän omaan päätelaitteeseen. Esimerkkeinä eri lähestymistavoista käytetään tässä yhteydessä ns. sekoitusaluemenetelmää (mix zones) ja valepisteiden lisäämistä paikkatietoon.

Sekoitusaluemenetelmä (Beresford & Stajano 2004, Palanisamy 2012, Palanisamy 2013) on yhteistoiminnallinen ja perustuu siis luotetun välityspalvelimen käyttöön, joka ylläpitää tietoa käyttäjän todellisesta identiteetistä ja pseudonyymistä, joista jälkimmäinen välitetään varsinaiseen sijaintipalveluun halutun tiedon saamiseksi. Jokainen tietyllä alueella (zone) liikkuva käyttäjä saa aina alueelle saapuessaan uuden käyttämättömän pseudonyymin siten, ettei vanhaa ja uutta pseudonyymiä voida yhdistää toisiinsa. Teoreettisesti tarkasteltuna k käyttäjää

saapuu jossain järjestyksessä alueelle, eikä kukaan heistä poistu ennen kuin kaikki ovat ko. alueella. Alueen sisällä kenenkään tarkkaa sijaintia ei välitetä eteenpäin, ja he poistuvat siitä eri järjestyksessä kuin saapuivat. Kun alueelle tuloja ja lähtöjä on molempia k kappaletta, voidaan käyttää k!-permutaatiomatriisia pseudonyymien välittämisessä varsinaiseen paikkatietopalveluun. Ajallisista ja maantieteellisistä rajoitteista (esim. tieverkon ominaisuudet) johtuen matriisi on kuitenkin harva, jolloin on mahdollista hyökätä sitä vastaan esim. graafialgoritmien avulla. Menetelmän tehokkuutta rajoittavat siis käyttäjämäärä, alueen geometria, paikkatiedon spatiaalinen tarkkuus jne. Menetelmän heikkouksia on pyritty analysoimaan useissa tutkimuksissa (Freudiger ym. 2007, Buttyan ym. 2007, Palamisamy ym. 2012).

Yksintoimivista järjestelmistä mielenkiintoinen on valesijaintien liittäminen polkuun (Kido ym. 2005). Ideana on siis lisätä mahdollisilta vaikuttavia ja todellisista sijainneista erottautumattomia pisteitä syötevirtaan siten, että käyttäjän oma päätelaite erottaa valepisteiden tuottaman informaation. Valepisteitä ei siis voida generoida satunnaisesti, vaan menetelmän keskeinen ongelma onkin kehittää algoritmeja ajallisesti ja sijainniltaan uskottavien jälkien (trajectory) joukkojen tuottamiseksi. Erilaisia algoritmeja onkin esitetty useita (Kido ym. 2005, Shankar ym. 2009, Xu ym. 2012), mutta niiden kaikkien heikkoutena on se, että mikäli muuta kontekstitietoa (esim. karttatieto) on käytettävissä ja käyttäjää voidaan tarkkailla pitkään, on mahdollista tunnistaa käyttäjien todelliset liikkeet. Toisena heikkoutena on lisääntynyt liikenne päätelaitteen ja paikkatietopalvelun välillä.

Alustavasti on tarkasteltu myös, miten loppukäyttäjät hyväksyvät erilaiset paikkatiedon yksityisyyden suojan menetelmät. Brush (Brush ym. 2010) ryhmineen esitteli pienelle joukolle (otos 32 henkilöä) erilaisia menetelmiä GPS-jälkien häivyttämiseen:

- diskreettien pisteiden poistaminen 100–1000 metrin etäisyydeltä sensitiivistä kohteista kuten kodista
- Gauss-jakautuneen kohinan liittäminen diskreetein askelin (50–1000 metriä) sijaintipisteisiin
- raja-arvoistaminen, jossa sijaintitieto kvantisoitiin johonkin kynnysarvoon 50–1000 metrin tarkkuudella
- alinäytteistäminen, jossa näytteenottotaajuutta pienennettiin viidestä sekunnista tuntiin kerätystä näytejoukosta
- k-anonymisointi kymmenen henkilön joukossa.

Jotta käyttäjille muodostuisi kuva menetelmistä käytännössä, esiteltiin aineiston karttapohjaisia visualisointeja eri häivytysmenetelmien vaikutuksista. Käyttäjät näyttivät niiden perusteella ymmärtävän menetelmien erot. Tutkimuksen perusteella mieluisimmat keinot olivat k-anonymisointi, diskreettien pisteiden poistaminen ja kohinan liittäminen tietoihin. Vaikuttaa siis siltä, että käyttäjille on mahdollista osoittaa erilaisten menetelmien merkitys ja heitä voi auttaa tekemään hyvin informoituja päätöksiä yksityisyyden suojaamisen menetelmien soveltamisesta heitä koskevan aineiston käsittelyssä.

London School of Economics on tutkinut PET-menetelmien hyötyjä taloudelliselta kannalta Euroopan unionin toimeksiannosta käyttämällä haastattelu- ja käyttötapaustutkimusta (case study) (LSE 2010). Suoritetun kustannus-hyötyanalyysin mukaan PET-menetelmien soveltaminen ei ole lainkaan suoraviivaista. Käyttäjien henkilötietojen ylläpito ja PET-menetelmien soveltaminen nähtiin kyllä yleisesti hyödylliseksi niin käyttäjien, yritysten kuin viranomaisten mielestä – mitä isommasta liiketoiminnasta oli kysymys, sen arvokkaammaksi hyödyt arvioitiin.

Päätelmänä kuitenkin oli, että jos PET-menetelmien soveltamiseen olisi todellista käyttäjätarvetta, ne yritykset, jotka siihen panostaisivat, saisivat siitä kilpailuetua. Tästä ei kuitenkaan ole mitään näyttöä kuluttajamarkkinoilla (B2C, Business to Customer), sen sijaan yritysmarkkinoilla (B2B, Business to Business) merkitys on jo tunnistettu. Keskeinen johtopäätös onkin se, että kuluttajapaine on harvoin ajava tekijä PET-menetelmien soveltamisessa käytäntöön.

Koska PET-menetelmät vaativat panostusta (investointeja) teknologiaan, koulutukseen ja ylläpitoon kustannuksien ja hyötyjen ollessa epäselviä, menetelmien käyttöönottoa on lykätty. Yritykset ovat myös haluttomia PET-menetelmien soveltamiseen niiden mahdollisesti henkilötiedon käyttökelpoisuutta vähentävien tekijöiden takia, etenkään kun eduista ei ole selvää näyttöä. Toisaalta mitä paremmin yritys oli tietoinen suojauksen menetelmistä, sen suuremmiksi hyödyt arvioitiin. Erityisesti yksityisyyden suojan lainsäädäntö nähtiin ajavana voimana PET-teknologioiden soveltamisessa.

4.4 TET ja luottamuksen synnyttäminen

Luottamuksella tarkoitetaan olettamusta siitä, että osapuolet käyttäytyvät tietyissä tilanteissa odotusten mukaisesti. Luottamuksen käsitteen tarkka määrittely on haasteellista, ja sitä onkin tarkasteltu useissa tutkimuksissa (Mayer ym. 1995, Wang & Emurian 2004, Urban ym. 2009, Bamberger 2010), joiden perusteella voidaan päätellä seuraavaa:

- Luottamus viittaa tulevaisuuteen ja sisältää siten aina epävarmuutta.
- Joku, joka luottaa (trustor) vapaaehtoisesti, luovuttaa tai on pakotettu luovuttamaan toimintojen hallinnan luottamuksen kohteelle (trustee), ja luottamuksen luovuttaja voi vain kuvitella ja arvioida luovuttamiseen liittyvät mahdolliset riskit ja lopputuloksen.
- Luottamus tuottaa toimintoja, jotka riippuvat tilanteesta ja koskevat joko jotain käsin kosketeltavaa tai aineetonta kohdetta.
- Luottamus perustuu yksilöiden subjektiiviseen käsitykseen, ja sen rooli on eri tilanteissa ja eri henkilöiden kohdalla erilainen.

Luottamuksen merkitys yhteiskunnassa on keskeinen sen toimiessa ”voiteluaineena”, koska ilman sitä kaikki mahdolliset kuviteltavissa olevat mahdollisuudet pitäisi käydä läpi etukäteen. Taloudelliselta kannalta luottamuksen puute kasvattaa taloudellisen vaihdannan kustannuksia (transaktiokustannuksia), koska ilman luot-

tamusta yksilöiden tulisi valmistautua toisen osapuolen opportunistiseen käyttäytymiseen jatkuvasti. Luottamus vähentää siis sosiaalista monimutkaisuutta ja on taloudellisen toiminnan kannalta toivottava päämäärä.

Verkkopalveluissa (online) luottamuksen puute on suurin este niiden käytölle. Jos palvelu ei saa käyttäjää vakuuttuneeksi luotettavuudesta, se ei saa käyttäjien hyväksyntää ja käyttäjäkuntaa. Verkkopalveluiden luottamuksen synnyttäminen on oppimisprosessi (loop of trust action), jossa alkuvaikutelma on keskeinen (Wang & Emurian 2004). Yksityisyys, turvallisuus ja lupausten pitäminen (esim. toimitusvarmuus) ovat niitä perusasioita, joiden perusteella käyttäjä muodostaa käsityksen verkkopalvelusta. Mikäli riittävän luottamuksen vaikutelma syntyy, käyttäjä luovuttaa helpommin sensitiivistä henkilötietoa (käyttäjätiedot, luottokortin numero jne.) palveluntarjoajan käyttöön.

On kuitenkin huomattava, etteivät turvallisuus ja yksityisyys ole ainoita tekijöitä, joiden perusteella tehdään päätös verkkopalveluiden toimittajasta. Sosiaalipsykologiset tutkimukset ovat jo 1940-luvulla osoittaneet, että fyysinen viehättävyys on merkittävä luottamuksen lähde. Siksi miellyttävä käyttöliittymä, helppo liikkuminen palvelussa ja sisällön esittäminen ovat yhtä tärkeitä lähtökohtia luottamuksen synnyttämisessä kuin turvallisuus ja yksityisyys. Muita käytettyjä keinoja luottamuksen kasvattamiseen ovat vertaissuositteleminen ja erilaiset arvostelujärjestelmät (ranking systems), joita tarkastellaan myöhemmin.

World Ecomic Forum (WEF) on voimakkaasti korostanut henkilötietojen merkitystä uusien taloudellisten mahdollisuuksien lähteenä arvonluonnissa, innovaatioissa ja talouskasvussa. Myös EU on havahtunut henkilötietojen merkitykseen, ja mm. EU:n tietosuojakomissaari (EDPS, European Data Protection Supervisor) Peter Hustinx on pannut merkille henkilötietojen muodostavan uuden ”valuutan” ilmaiseksi katsottujen palveluiden maksussa ja todennut, ettei EU:n yksityisyyden ja tietosuojan valvonta ole pysynyt kehityksen perässä. On arvioitu, että henkilötiedon perusteella käytettävien ilmaisten palveluiden liikevaihto on tällä hetkellä n. 300 miljardia euroa, ja sen odotetaan kolminkertaistuvan vuoteen 2020 mennessä.

Henkilötietojen nopea kaupallistaminen on kuitenkin heikentämässä kuluttajien luottamusta palveluntarjoajiin ja herättämässä kasvavaa huolta tietojen mahdollisesta väärinkäytöstä. WEF (2010) näkee lähitulevaisuudessa yksityisyyden suojaan liittyvän suuria haasteita:

- Henkilötietojen keruu ja käsittely kehittyy yhä enemmän laitteelta-laitteelle (machine to machine, M2M) -pohjaiseksi ja passiiviseksi, ja henkilöihin liitettyä tietoa syntyy palveluiden käytön sivuvaikutuksena (luottokorttiostokset, kanta-asiakkuudet, puhelinten paikkatieto jne.) ilman käyttäjien havainnointia ja tietoisuutta siitä.
- Perinteiset käyttäjien yksityisyyteen liittyvät tietoisuuden lisäämisen mekanismit eivät toimi. On laskettu, että keskimääräiseltä käyttäjältä veisi yli 30 päivää vuodessa perehtyä käyttämiensä verkkopalveluiden yksityisyydensuojamenettelytapoihin (privacy policy). Tästä aiheutuisi vuosittain n. 780 miljardin dollarin kustannukset. (McDonald 2008.)

WEF suosittaakin, että käyttäjän omaa kontrollia henkilötietoihin, digitaaliseen identiteettiin ja yksityisyyteen kasvatetaan. Henkilötietoja tulisikin WEFin suosituksen mukaan käsitellä pankkien tapaan hallitusti, turvallisesti ja luottamus säilyttäen. Vastaavia ajatuksia ovat esittäneet tutkijat (Weitzner 2012), joiden mukaan yksityisyyden suojan ajattelutapaa pitäisi muuttaa tietojen käyttöä painottavaan suuntaan. Tämä tarkoittaisi läpinäkyvyyden ja jäljitettävyyden lisäämistä yksityiseksi katsottavan tiedon käsittelyssä:

- Käyttäjien tulisi olla selvillä, mitä tietoa, miten ja kuka sitä heistä kerää.
- Luottamusta – ts. käyttäjien tulisi pystyä luottamaan järjestelmiin ja palveluihin siten, että heillä on turvallinen pääsy yhtenäiseen ja eheään tietoon.
- Hallintaa – ts. käyttäjien tulisi itse pystyä hallitsemaan, missä määrin heitä koskevaa tietoa jaetaan, ja heillä tulisi olla mahdollisuus korjata, päivittää ja muuttaa tietoa ja sitä koskevia asetuksia.
- Arvoa – ts. käyttäjien tulisi tunnistaa se arvo, jota henkilötiedon perusteella luodaan, ja miten he saavat korvausta tiedon käytöstä.

Luonnollisesti arvonluontiin liittyy kysymys siitä, kuka viime kädessä omistaa henkilötiedon, ja toisaalta se, mitkä saattaisivat olla taloudelliset kannustimet yrityksille luovuttaa käyttäjille hallintaoikeus heistä kerättyyn aineistoon.

4.5 TET- lähestymistapoja

Läpinäkyvyyden ja luottamuksen kasvattamiseen on olemassa useita keinoja, joista tässä yhteydessä esitellään miData-, Privacy by Design- ja Privacy Impact-assessment -lähestymistavat.

MiData (aiemmin MyData, jota termiä Suomessa käytetään edelleen) -ajatus on syntynyt osittain kansalaisjärjestöjen – Suomessa esim. Open Knowledge Foundationin – ja viranomaisten – lähinnä brittien UK Mistry for Employment Relations, Consumer and Postal Affairs – toimesta. MiDatan tavoitteena on lisätä käyttäjien pääsyä ja kontrollia heistä kerättyyn henkilökohtaiseen tietoon. Briteissä tarkoituksena on ollut luoda yrityksille vapaaehtoinen ohjelmakehikko, joka (BIS 2011)

- antaisi käyttäjille turvallisen pääsyn heistä kerättyyn tietoon siten, että he voisivat tehdä valistuneempia kulutuspäätöksiä. Brittien ministeriön tavoitteena olikin tarjota kuluttajille heidän kulutustapojensa tuntemusta ja siten auttaa paremmin perusteltujen kulutuspäätösten valintaa (”Better Choices – Better Deals” -ohjelma).
- antaisi yrityksille mahdollisuuden vuoropuheluun kuluttajien kanssa ja kehittää uusia innovatiivisia palveluita ja työkaluja siitä saatavan tiedon perusteella.

Yksi kantava ajatus on henkilökohtaisten tiedonhallintajärjestelmäpalveluiden (PIMS, Personal Information Management Services) syntyminen. On arvioitu (CtrlShift 2014), että Englannissa PIMS-palveluiden kypsien markkinoiden arvo olisi n. 16 miljardia puntaa (1,2 % brittien talouden kokonaisvolyymista) eli ne ovat merkitykseltään suurempi kuin autoteollisuus tai lääketeollisuus. Lisäksi on hahmoteltu eräänlaista turvallista verkkopalvelua (”henkilökohtaista tietovarastoa”, Personal Data Inventory), johon yritykset ja muut yhteisöt voisivat kerätä tietoa mm. seuraavista asioista: henkilötiedot, sopimukset yritysten kanssa, maksujärjestelmätiedot ja palveluiden ja ostosten historiatiedot.

Tällaiselle tietovarannolle nähdään suuria taloudellisia hyödyntämisen mahdollisuuksia (GovUK 2013,CtrlShift 2014):

- Rikas ajantasainen asiakastieto parantaa palveluiden kohdennettavuutta ja merkitystä.
- Rikkaampi käyttäjätieto mahdollistaa uusien innovaatioiden, tuotteiden ja palveluiden syntymisen.

Toisaalta järjestelmä synnyttää mahdollisia taloudellisia uhkia:

- Yritysten tuotot kärsivät, kun kuluttajien on mahdollista entistä tehokkaammin vertailla tuotteita ja palveluita omien tarpeidensa tueksi (tosin kilpailun lisääminen oli ministeriön alkuperäinen tavoite).
- Kuluttajat välttelevät sellaisia yrityksiä, joihin he eivät luota tai joiden kanssa he eivät halua olla tekemisessä. PIMS-operaattorista voisi tulla tässä tapauksessa eräänlainen ”portinvartija” yritysten ja kuluttajien väliin.

Käytännössä miData-järjestelmää on kokeiltu Britanniassa energia-, tietoliikenne- ja rahoitussektorilla, ja siinä ovat olleet mukana UK Cards Association, Lloyds Banking, VISA, MasterCard, British Gas, EDF Energy, EON jne. Myös Google on osallistunut hankkeeseen. Yksi hankkeen käytännön saavutuksista on ollut miData Innovation Lab (mIL) -laboratorio, jonka tarkoituksena on ollut tuottaa kuluttajasovelluksia ja palveluita kerätyn todellisen kuluttajatiedon perusteella. Varsinaisten kuluttajien innostumisesta miData-ajatteluun tai siihen liittyviin palveluihin ei valitettavasti toistaiseksi ole raportoitu julkisesti. Epävirallisten lähteiden mukaan kuluttajien innostus on kuitenkin ollut laimeaa.

Suomessa miData-konseptia on viety eteenpäin Open Knowledge Finlandin ja liikenne- ja viestintäministeriön toimesta (Poikola ym. 2014). Poikola työryhmineen on kuvannut raportissa ”MyData – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen” PIMS-palvelun roolia ja etuja eri kohderyhmien näkökulmasta ja esitellyt siihen liittyviä erilaisia toteutus- ja operointimalleja. Keskeinen elementti Poikolan ryhmän hahmottelemassa palveluinfrastruktuurissa on turvallinen ja todennettu välitysjärjestelmä, joka mahdollistaa henkilötietojen turvallisen siirtämisen eri osapuolten välillä henkilön antaessa siihen valtuuden.

Toinen paljon huomioita saanut läpinäkyvyyden lisäämisen ajatus on ns. ”Privacy by Design” -periaate, jota on markkinoinut etenkin Ann Coucovian (Ontario’s Information and Privacy Commissioner). PET-tekniikoista poiketen PbD on kokonaisvaltainen lähestymistapa, jossa huomioidaan suunnittelu- ja operointiprosessit (työprosessit, johtaminen, infrastruktuuri jne.). PbD-periaatteen tarkoituksena on ottaa yksityisyyden suojaan liittyvät kysymykset keskiöön jo järjestelmien suunnittelun lähtökohdissa, ja se perustuu seitsemään perussääntöön (Cavoukian 2009):

- Proaktiivisuuden korostaminen reaktiivisuuden kustannuksella ts. pyritään jo etukäteen estämään yksityisyyden loukkaukset ennen kuin ne tapahtuvat.
- Yksityisyys oletusarvoisena asetuksena ts. henkilötiedon tulisi olla automaattisesti suojattuna ilman henkilön omaa aloitetta ja tämän tulisi olla järjestelmiin jo sisäänrakennettuna.
- Yksityisyyden suojan tulisi olla sulautettuna IT-järjestelmiin ja niiden arkkitehtuureihin keskeisenä komponenttina siten, ettei se kuitenkaan heikennä järjestelmien käytettävyyttä.
- PbD pyrkii ottamaan huomioon kaikkien sidosryhmien intressit siten, että päästään joka osapuolta hyödyttävään lopputulokseen (”win-win”).
- Yksilöön liitettävien tietojen elinkaaren hallinta on suoritettava siten, että koko elinkaari on turvattu ja tiedot hävitetty asianmukaisesti elinkaaren lopussa.
- Läpinäkyvyys – ts. kaikkien sidosryhmien jäsenten tulisi toimia annettujen tavoitteiden ja lupausten mukaisesti, ja heidän toimintansa pitäisi olla riippumattoman tahon todennettavissa.
- Yksityisyyden suojan kunnioitus ja käyttäjälähtöinen toteutus.

PbD-periaatteita voidaan pitää kuitenkin lähinnä pyrkimyksenä ja niitä onkin kritisoitu varsinaisen konkretian puutteista – etenkin siitä, miten ne käytännössä toteutettaisiin. Erityisesti ”win-win”-periaatetta eli kaikkien sidosryhmien intressien yhtäaikaista toteutumista on pidetty epärealistisena (Rubinstein 2013 Gurses ym. 2011, Spiekerman 2012) nykyisessä henkilötietoihin pohjautuvassa taloudessa.

Spiekerman (2012) on mm. todennut, että korkeat yksityisyyden suojan vaatimukset rajoittavat tiedon analysoinnin mahdollisuuksia ja yritysten strategisia valintoja ja ovat vastakkaisia yritysten tämänhetkisiin pyrkimyksiin nähden. Tällä hetkellä ei siis ole yleisesti hyväksyttyä käsitystä siitä, miten PbD-periaatetta voitaisiin parhaiten tukea systemaattisilla menetelmillä ja kuinka se ohjaisi käytännön insinöörityötä.

Eräänä keskeisenä ongelmana PbD:n toteuttamisessa on puuttuva yhteys liiketoimintamallien ja yksityisyyteen liittyvän riskinhallinnan välillä. Spiekerman (2012) on todennut kaksi käytännön tapaa PbD:n toteuttamiseen:

- nykyinen menettelytapaperustainen (privacy policy) toteutus yksityisyyden suojan lainsäädännön ja FIPS-periaatteiden noudattamiseksi

- yksityisyydensuoja-arkkitehtuurit, jotka tähtäävät tiedon minimointiin, ts. henkilötietojen keruun rajoittaminen, anonymisointi sekä tiedon prosessointi ja tallentaminen käyttäjien omille laitteille (client side data processing).

Ensimmäinen lähestymistapa toteutuu yksityisyyden vaikutusten arvioinnin PIA-menettelyn (Privacy Impact Assessment) kautta, joka pyrkii riskinhallinnassa lainsäädännön ja FIPS-periaatteiden huomioimiseen tuotteita ja palveluita suunniteltaessa. Jälkimmäinen arkkitehtuuripohjainen lähestymistapa taas keskittyy uhka-analyyseihin ja tietoturvamenetelmien soveltamiseen pienentämiseksi. Arkkitehtuuripohjaista lähestymistapaa vaikeuttaa se, että yhteistä yksityisyydensuojakehikkoa/-menetelmää on vaikea löytää, koska järjestelmien kehitystavat poikkeavat huomattavasti toisistaan (esim. ns. vesiputousmallit vs. ketterän kehityksen menetelmät).

Privacy Impact Assessment (PIA) (Spiekerman 2012) on joukko systemaattisia lähestymistapoja, joilla voidaan arvioida henkilötiedon käsittelyn vaikutuksia ja ehkäistä niistä syntyneitä ongelmia ennakolta. Useita erilaisia kansallisia PIA-menetelmiä on käytössä mm. Yhdysvalloissa, Australiassa, Kanadassa, Englannissa sekä Uudessa Seelannissa, ja ne poikkeavat toisistaan siinä, milloin arviointia tehdään, kuka johtaa prosessia, missä vaiheessa sidosryhmät otetaan mukaan prosessiin ja kuinka arviointi suoritetaan.

Muunnelmat ovat ymmärrettäviä, sillä sama lähestymistapa ei sovi kaikkiin tapauksiin. PIA-prosessien edut ovat kuitenkin kiistattomia ja käytännössä toimivia, sillä prosessit käsittävät mm. riskien tunnistuksen ja hallinnan, sidosryhmien tarpeiden huomioinnin ja vastakkaisten tavoitteiden tasapainottamisen sekä turvallisuuden parantamisen. Menetelmien kriitikot arvostelevat niitä kuitenkin byrokraattisiksi ja hankkeita viivyttäviksi (Wright & Hert 2012).

Kanadassa PIA-prosessi on pakollinen kaikissa valtion hankkeissa, joissa voi syntyä henkilötiedon käsittelyn ongelmia. Prosessi on pääpiirteissään seuraava:

- Tarkastellaan, onko aihetta PIA-prosessin soveltamiselle. Myönteisessä tapauksessa prosessin laajuus määritellään ja kootaan tarvittavat resurssit (tiimi).
- Suoritetaan tietovuoanalyysi, jossa tarkastellaan, kuinka sensitiivistä informaatiota kerätään, käsitellään, jaetaan ja miten sitä säilytetään. Ehdotetut liiketoimintaprosessit kuvataan ja sensitiiviset tiedot liittyen näihin liiketoimintaprosesseihin tunnistetaan ja kuvataan vuokaavioina ja liiketoimintakaavioina.
- Käyttäen ennalta laadittua kysymyslistaa arvioidaan käsiteltävään tietoon liittyvät riskit.
- Vaikutusten arviointi -raportti kokoaa uhat ja niiden vakavuuden arvioinnit, mahdollisuudet niiden torjumiseen ja vaadittavat toimenpiteet.

Kanadalaisessa mallissa ei määritellä, missä vaiheessa sidosryhmät tunnistetaan ja otetaan mukaan prosessiin, mutta esim. brittien vastaavassa vapaaehtoisessa

menettelyssä tehdään valmisteluvaiheessa sidosryhmäanalyysi ja sidosryhmien edustajat otetaan mukaan jo heti prosessin alkuvaiheessa.

PIA-prosessia on käytetty mm. RFID-sovellusten vaikutusten arviointiin, jotta voitaisiin olla vakuuttuneita, että ne noudattavat EU:n tietosuojadirektiiviä. Yksinkertaisimmillaan RFID-PIA-prosessia voi käydä läpi GS1-yrityksen tuottamalla Excel-taulukolla (GS1 EPC/RFID PIA tool), jonka avulla voi varmistua sovellusten yhteensopivuudesta EU:n lainsäädäntöpyrkimysten kanssa. Useat PIA-prosessin kannattajat ovat ehdottaneet, että vastaavantyyppiset menettelyt ja yksinkertaiset työkalut voitaisiin kehittää useille eri toimialueille Euroopassa.

5. Luottamus ja mainejärjestelmät

Kouvo (2014) on yleistä luottamusta (lähinnä yhteiskunnallista luottamusta) käsittelevässä väitöskirjassaan tarkastellut luottamuksen lähteitä. Hänen mukaansa luottamuksen synnystä on esitetty useita eri teorioita, joista keskeisimmät ovat kansalaisyhteiskuntakeskeinen hypoteesi ja instituutiokeskeinen hypoteesi. Ensimmäisen mukaan kansalaiset, jotka viettävät aikaansa sosiaalisissa verkostoissa, oppivat luottamaan paitsi täysin tuntemattomiin ihmisiin myös yhteiskunnallisiin instituutioihin. Instituutiokeskeinen hypoteesi puolestaan korostaa luottamuksen syntymistä ja kollektiivista ongelmanratkaisua yhdessä silloin, kun poliittiset ja lainsäädännölliset instituutiot pystyvät luomaan tähän tarvittavan toimintaympäristön sääntöineen.

Yksilöiden luottamusta tuotteisiin, palveluihin ja niitä tarjoaviin henkilöihin voidaan rakentaa sopimusten, sääntöjen, normien ja lakien (asetusten) pohjalta. Sääntely, kuten elintarvikkeiden ja hygienian tarkastus tai taksiliikenteen asetukset, ammatilliset pätevyysvaatimukset, kuten lääkärin tutkinto sairauksien hoidossa, sekä teollisuuden omat sertifikaatit lisäävät kuluttajien luottamusta. Luottamuksen ylläpitoon on kuitenkin olemassa myös epävirallisempia mekanismeja. Maineverkostoilla (reputation networks) on pitkä historia luottamuksen rakentamisessa yhteisöissä ennen valtiovallan lakien säätämistä ja niiden toimeenpanovaltaa. Maine on ollut keskeisimpiä tekijöitä, joka on ylipäätänsä mahdollistanut sosiaalisen ja kaupallisen toiminnan varhaisissa yhteisöissä. (Dellacoras 2005.)

Kovalaisen ja Österbergin (2000) mukaan luottamus (trust) voidaan jakaa kolmeen osaan: etuun tai uhkaan perustuvaan luottamukseen, kokemukseen perustuvaan luottamukseen (vrt. luottavaisuus) ja samaistumiseen perustuvaan luottamukseen. Ensimmäisenä syntyy toisensa tuntemattomien osapuolien välille etuun ja uhkaan perustuva luottamus, jossa toimijat käyttäytyvät siten, miten heiltä odotetaan osittain seuraamuksia peläten tai edun saamiseksi. Toisessa vaiheessa luottamus on kokemuspohjaista ja kolmannessa vaiheessa on kyse samaistumiseen perustuvasta luottamuksesta, jossa osapuolet ymmärtävät ja kunnioittavat toistensa toiveita.

Tuotteiden ja palveluiden vaihdossa voidaan katsoa toimittavan kahden ensimmäisen luottamuksen muodon piirissä. Toisaalta luottamusta kasvattavat myös brändit, joiden merkitys selittyy tunnettavuuden kautta. Luhmannin (1979, 2000) mukaan luottamus rakentuu tunnettavuuden varaan. Tunnettavuus on esiehto

luottamuksen syntymiselle: ”Luottamus (trust) on mahdollista vain tutussa maailmassa, se tarvitsee historiaa luotettavaksi taustakseen” (Luhmann 1979). Toisaalta luottamusta tarvitaan erityisesti tilanteissa, joissa on suuri riskin toteutumisen mahdollisuus, kun taas luotettavuus (confidence) tai tunnettavuus (familiarity) riittävät useimmissa muissa yhteyksissä.

Kuluttajilla on taipumusta vähentää riskejä käyttämällä tunnettuja brändejä, koska niillä uskotaan taattavan tuotteiden ja palveluiden laatu ja turvallisuus (Aaker 1991). Vahvat bändit mahdollistavat tuotteiden ja palveluiden helpomman hahmottamisen (tunnettavuus) ja tarjoamisen sekä pienentävät epätietoisuutta ja havaittuja riskejä, jotka liittyvät brändien hankkimiseen ja kuluttamiseen.

Luottamukseen liittyy läheisesti myös maineen (reputation) käsite. Maineella tarkoitetaan yhteisön muodostamaa kollektiivista käsitystä luotettavuudesta (trustworthiness), joka näkyy kaikille sen jäsenille. Maine syntyy toimijan aiemmasta käyttäytymishistorian havainnoinnista. Maine voi liittyä yksilöön, yhteisöön, organisaatioon (yritykseen) tai abstraktimpaan kohteeseen, esim. tuotteeseen. Ryhmän tai organisaation maine voi määrittyä siinä toimivien yksilöiden maineen kautta sen perusteella, miten ulkopuoliset keskimäärin hahmottavat yhteisöön kuuluvat yksilöt. Toisaalta yksityisen ihmisen maine voi määrittyä yhteisöön kuulumisen kautta; sen yksittäisestä jäsenestä muodostetaan ennakkomielikuva yhteisön mukaan (Jøsang ym. 2007). Nyt maine varhaisena luottamuksen rakentamisen mekanismina on otettu käyttöön verkkopalveluissa.

5.1 Luottamus- ja mainejärjestelmät

Internetin verkkopohjaisissa järjestelmissä esim. kaupalliset transaktiot tapahtuvat usein osapuolten välillä, jotka eivät mahdollisesti koskaan ole kohdanneet aikaisemmin. Tuotteen tai palvelun ostajalla ei välttämättä ole myöskään riittävää tietoa myyjästä tai hänen tarjoamistaan tuotteista ja palveluista (informaation asymmetrisyys). Tietotekniikkavälitteinen kommunikaatio kaventaa myös perinteisesti käytössä olevia mahdollisuuksia huijausten havaitsemiseen. Onkin varsin helppoa ja kustannuksiltaan edullista luoda esim. houkuttelevalta vaikuttava kauppapaikka tai myyjäprofiili epärehellisten päämäärien saavuttamiseksi.

Perinteisen taloustieteen näkökulmasta opportunistinen käyttäytyminen olisi rationaalisesti oletettavaa ilman jonkinlaista ulkoista kontrollia tai insentiiviä. Jos kummallakaan kaupankäynnin osapuolella ei ole mahdollisuutta palkita tai rangaista toisiaan tai ei olisi minkäänlaista laillisuuteen perustuvaa pakotetta, esimerkiksi myyjä voisi hyötyä siitä, ettei hän toimittaisi kauppatavaraa lainkaan tai toimittaisi lupaustaan huonompilaatuisen tuotteen. Kyseisen riskin takia rationaalinen asiakas ei ole puolestaan halukas maksamaan myyjän haluamaa hintaa. Hyvää tuotetta tai palvelua myyvä osapuoli ei taas ole valmis hyväksymään liian alhaista tarjousta, ja ajan myötä ko. markkinoilta häviävät korkealaatuisia tuotteita ja palveluita kauppaavat henkilöt. Lopulta jäljelle jäävät vain heikompilaatuisia hyödykkeitä tarjoavat myyjät (”Market of Lemons, adverse selection”, Akerlof 1970).

Opportunismista aiheutuva ”moraalikato” (moral hazard) on yleisesti tunnistettu oikeus- ja taloustieteellinen tilanne, jossa osapuoli lisää riskinottoaan siksi, että osa riskien seurauksista koituu jollekulle muulle. Tällainen riski voi syntyä sääntelyhäiriön seurauksena tai siksi, että toinen sopimuksen osapuolista voi muuttaa käytöstään toisen osapuolen tappioksi sopimisen jälkeen. Verkkopalveluissa kyseistä ”moraalikadon ongelmaa” pyritään suitsemaan erilaisilla online-järjestelmillä, joita tarkastellaan seuraavaksi lähemmin.

Tietotekniikka-avusteiset luottamusjärjestelmät perustuvat ajatukseen, jossa osapuolten aikaisempi toiminta antaa kuvan osapuolten taipumuksista sekä mahdollisesta tulevasta käyttäytymisestä. Luottamusjärjestelmät ikään kuin luovat ”tulevaisuuden varjon” aiempien transaktioiden ja interaktioiden pohjalta, joiden avulla osapuolet voivat arvioida toistensa luotettavuutta (Resnick ym. 2000).

Tyypillisessä online-mainejärjestelmässä interaktion osapuolet voivat arvostella transaktion, esim. kauppatapahtuman, antamalla arvion kaupan toteutumisesta (esim. positiivinen, neutraali tai negatiivinen tai skaalalla 1–5) sekä liittämällä siihen kommentteja. Mainejärjestelmät eivät koske ainoastaan internetkauppapaikkoja, kuten eBayta, Amazonia tai muita vastaavia, vaan niiden lisäksi esim. verkkopohjaiset asiantuntijaportaalit (AskMe, AllExpert jne.) ja lukemattomat muut järjestelmät (Epinions, Slahsdot, BizRate, Yelp, Uber, Lyft jne.) sisältävät vastaavan mahdollisuuden arvioida vastauksen tai tiedon asiantuntevuutta, palvelun laatua jne. Luottamuksen synnyttämisen kannalta näissä järjestelmissä arvioiden ja arvostelujen suuri määrä korvaa niiden laadun.

Mainejärjestelmien merkitystä käytännössä ei ole syytä aliarvioida. Nielsen-tutkimuslaitoksen vuoden 2012 otannan mukaan, johon osallistui yli 28 000 ihmistä 56 eri maasta, esimerkiksi online-kuluttaja-arviot olivat toiseksi luotettavin brändejä koskeva tietolähde omien tuttavien ja sukulaisten suosittelujen jälkeen. Noin 70 % kuluttajista piti erilaisia suosittelujärjestelmiä luotettavina. (Aral 2014.) Dellarocasin (2010) mukaan mainejärjestelmien tehtävänä onkin mm. luottamuksen rakentaminen, laadun mainostaminen, yrityksen ja yksilön välisen yhteistyön parantaminen ja asiakasuskollisuuden kasvattaminen. Se, mitä näistä ominaisuuksista halutaan painottaa, riippuu online-järjestelmälle asetettavista tavoitteista (Dellarocas 2010). Esim. Amazonin rating-järjestelmän tavoitteena on lähinnä tiedottaminen (laadun mainostaminen), kun taas eBayn vastaavan tehtävänä on luottamuksen rakentaminen potentiaalisten kauppatapahtumien osapuolten välille.

Mainejärjestelmät ovat elektronisille kauppapaikoille niin tärkeitä, että esim. Amazon haastoi lokakuussa 2015 oikeuteen yli tuhat toistaiseksi tunnistamatonta henkilöä, jotka tekaisivat maksusta positiivisia tuotearvioita Amazoniin Fiverr-nimisen joukkoistamisperiaatteella toimivan tehtävänvälityksen kautta (Gani 2015).

Jotta mainejärjestelmät (reputation systems) olisivat toimivia, Resnickin ja Zeckhauserin (2002) mukaan niillä täytyy olla seuraavat ominaisuudet:

- Niihin liittyvien entiteettien (esim. nimimerkkien) tulee olla pitkäikäisiä, jotta olisi mahdollisuus tulevaisuudessakin tapahtuvaan kanssakäyntiin. Tämä tarkoittaa käytännössä sitä, ettei järjestelmässä voisi ”nollata” aiempaa käyttäytymishistoriaa vain identiteettiä vaihtamalla.

- Palaute olemassa olevista interaktioista on talletettu ja jaettavissa sekä käytettävissä myös tulevaisuudessa. Tämä luonnollisesti edellyttää, että käyttäjät ovat ylipäätänsä halukkaita antamaan arvioita kanssakäymisistä (esim. kauppatapahtumista) ja että palautetta on riittävästi (yli kynnysarvon), jotta sillä ylipäätänsä olisi merkitystä (Dellacoras 2005).
- Aiemmista palautteista täytyy seurata uusia päätöksiä interaktioon ryhtymisestä.

Jøsangin ym. (2007) mukaan luottamus- ja mainejärjestelmien erona voidaan pitää sitä, että luottamusjärjestelmä heijastaa yksilön subjektiivista käsitystä entiteetin luotettavuudesta, kun taas mainejärjestelmässä kyse on enemmän kollektiivisesta luotettavuuden arvioinnista.

Mainejärjestelmät perustuvat käyttäjien arvioihin niistä interaktioista, joihin he ovat olleet osallisia, ja järjestelmä kerää yhteen kaikille näkyville järjestelmän piirissä tapahtuneiden interaktioiden arviot (ratings). Järjestelmä määrittää jonkin algoritmin mukaan osapuolesta kokonaisarvion, esim. pisteytyksen diskreettinä arvona, jonka perusteella potentiaalinen osapuoli voi arvioida osapuolen mainetta (luotettavuutta) ja halukkuutensa interaktioon. Jotta järjestelmä toimisi, tarvitaan

- tietoliikenneyhteiskäytännöt (communication protocols), joiden avulla osapuolet voivat antaa arvionsa transaktiosta ja saada näkyviin tiedot kiinnostavista osapuolista
- maineenlaskentakone (reputation computation engine), joka ”pisteyttää” jokaisen järjestelmän piiriin kuuluvan osapuolen. Pisteytys tapahtuu järjestelmään kerääntyneen informaation ja mahdollisesti muualta saatavan tiedon perusteella.

Teknisesti järjestelmät voivat olla keskitettyjä (centralized) tai hajautettuja (distributed). Keskeistä järjestelmissä on se, miten osapuolta koskeva kokonaisarvio muodostetaan. Yksinkertaisimmassa tapauksessa näkyvä arvio, esim. pisteytys, muodostetaan interaktioista muodostuneiden positiivisten ja negatiivisten arvioiden erotuksesta (esim. eBayn mainejärjestelmä). Tämä tavan etuna on ymmärrettävyys, mutta toisaalta haittana on yksinkertaisuus ja sen antama mahdollinen väärä kuva osapuolten luottavuudesta. Kyseisessä järjestelmässä on mahdollista, että esim. sata positiivista arviota ja kymmenen negatiivista arviota saanut katsotaan yhtä luotettavaksi toimijaksi kuin 90 positiivista, muttei yhtään negatiivista arviota saanut toimija. Toinen yksinkertainen mahdollisuus on muodostaa keskiarvo kaikista arvioista, ja tätä menetelmää käytetäänkin useissa kauppapaikoissa, esim. Amazon-verkkokaupassa ja erilaisissa hotellivarausjärjestelmissä. Edelleen kehitetty versio edellisestä on arvioiden painotettu keskiarvo, jossa painokertoimina käytetään arvioijien omaa luotettavuutta, arvioinnin tuoreutta (aikaa) jne.

Kehittyneemmät rating-algoritmit ovat olleet erityisesti akateemisen mielenkiinnon kohteena. Näitä ovat mm. (Jøsang ym. 2007, Tavakolifard & Almeroth 2012)

- Bayesin binäärilogiikan tilastolliseen todennäköisyyteen (PDF, Bayesian beta probability density function) perustuva menetelmä, jonka etuna on vahva teoreettinen pohja, mutta heikkoutena suhteellisen hankala ymmärrettävyys peruskäyttäjien näkökulmasta
- heuristiset diskreetit luottamusmallit
- transitiiviseen luottamuksen ketjutukseen perustuvat menetelmät
- sumeaa logiikkaa (fuzzy logic) hyödyntävät menetelmät
- erilaiset transitiiviseen iteraatioon (ns. flow-mallit) perustuvat menetelmät (eräs esimerkki näistä on mm. Googlen alkuperäisessä hakukoneessa käytetty PageRank-algoritmi)
- peliteoreettiset lähestymistavat
- stokastiset mallit, esim. Markovin ketjut, joissa pyritään ennustamaan tulevaa käyttäytymistä menneisyyden maineen perusteella.

Näiden menetelmien taustalla olevaa teoriaa ja toimintaa ei lähdetä tässä yhdessä syvällisemmin selvittämään. Hyvin olennainen ominaisuus pisteytysalgoritmeille on kuitenkin niiden kyky havainnoida epäreilu palaute sekä huijaukset ja pyrkiä minimoimaan niiden vaikutukset. Nämä ongelmia aiheuttavat piirteet liittyvät lähinnä ihmisen käyttäytymiseen, ja niiden vaikutusta voidaan jossakin määrin ottaa huomioon järjestelmiä suunniteltaessa.

5.2 Mainejärjestelmiin liittyviä ongelmia

Yksi tärkeimmistä mainejärjestelmän toiminnoista on riittävän tarkan palautteen antaminen. Arvostelu interaktiosta annetaan mainejärjestelmissä tyypillisesti jälkikäteen, ja monesti käyttäjillä ei ole enää insentiiviä antaa vastapuolesta arvostelua esim. kauppatapahtuman jälkeen. Joissakin järjestelmissä on tutkimusten mukaan ollut kuitenkin korkeana pidettävä 50–60 %:n osallistumisprosentti kaupanteon jälkeen (esim. eBay), mutta yleensä ongelmana on pikemminkin arvostelujen vähäisyys (Resnick ym. 2000). Periaatteessa kyseessä on taloustieteestä tuttu vapaamatkustajan (free rider) ongelma, jossa yksittäinen toimija hyötyy muiden panostuksesta antamatta kuitenkaan omaa osuuttaan yhteiseen hyvään. Ratkaisuksi tähän ongelmaan mainejärjestelmien osalta on esitetty mm. rahallista palkitsemista (esim. alennusta tulevaisuuden ostoksista) vilpittömistä ja käyttökelpoisista arvosteluista. Arvostelut voivat puuttua tai viivästyä myös sen vuoksi, ettei kukaan ota riskiä uuden toimijan ja tuotteen kanssa, ennen kuin joku toinen on tehnyt sen.

Toinen edellisen kanssa läheinen ongelma on arvostelujen painottuminen hyvin positiivisiksi eli ns. J-käyräjakauma tavanomaisen normaalijakauman sijasta (Hu ym. 2009). Esimerkiksi Resnickin ja Zeckhauserin (2002) tutkimuksen mukaan vain n. 0,6 % ostajien arvioista oli negatiivisia eBayssa, ja se ei melkoisella varmuudella kuitenkaan vastaa käyttäjien kokemuksia. Dellarocas (2005, 2010) on

arvioinut, että tyytymättömien osuus olisi todellisuudessa n. 10–20 %:n luokkaa. Mahdollisia selityksiä negatiivisesta palautteesta vaikenemiseen voivat Resnickin ja Zeckhauserin (2002) mukaan olla, että positiivisilla arvioilla pyritään varmistamaan oma positiivinen arviointi vastakauppana tai toisaalta välttämään mahdollisesta negatiivisesta palautteesta aiheutuvat ongelmat. Niitä voivat olla kosto (vastavuoroisesti aiheettoman negatiivisen palautteen antaminen) tai oikeudelliset ongelmat. Hu ym. (2009) selittävät J-käyrän syntymistä myös ostoennakkoasenteella ja ”aliraportoinnilla” ts. ne henkilöt, jotka ylipäätänsä arvostelevat kohteen, arvostelevat sen jompaankumpaan laitaan, joko ennakkoasenteitaan vahvistaen tai pettymystään purkaakseen (ns. ”rehentely-ruikutus”-efekti).

Uskottava selitys siihen, miksi arviot painottuvat positiivisuuteen, on myös se, että muiden mielipiteet ja arvostelut vaikuttavat omaan arvostelukäyttäytymiseen. Ihmisen ns. laumavaisto toimii tässäkin tapauksessa. Aralin (Aral 2014, Muchnik ym. 2013) tutkimusryhmän kokeissa, joissa satunnaisesti manipuloitiin uutisartikkelien suosiota, positiivinen manipulointi lisäsi positiivisen arvioinnin todennäköisyyttä 32 % ja muutti lopullista arviointia 25 % positiiviseen suuntaan. Negatiivisen manipuloinnin merkitys taas oli vähäisempi, ja se saattoi kyllä lisätä negatiivisen arvioinnin todennäköisyyttä, mutta ns. joukkokorjaamisen ilmiö neutralisoi negatiivisen manipuloinnin vaikutuksen. Toinen merkittävä havainto oli, että ensimmäinen positiivinen arviointi vaikutti vastaavasti positiiviseen pisteytysjakaumaan ja lisäsi todennäköisyyttä J-käyrän mukaiseen jakaumaan.

Kolmas inhimilliseen käyttäytymiseen liittyvä ongelma on epäreilujen arvostelujen antaminen tai arvostelujen suoranainen väärentäminen. Epäreilujen tai vääristelyjen arvostelujen antaminen on mahdollista, koska verkossa toiminta on kuitenkin melko anonyymiä (esim. pseudonyymin suojasta toimien), vaikka useissa järjestelmissä vaaditaan rekisteröityminen ja jonkinlaisen käyttäjäprofiilin muodostaminen. Yksittäisten vääristeltyjen arvostelujen tunnistaminen ja poissulkeminen voi perustua joko arvostelujen tilastollisiin ominaisuuksiin ja niiden perusteella tapahtuvaan suodattamiseen tai arvostelijan omaan maineeseen (joka tosin sekin on manipuloitavissa). Sen sijaan on hankalampi estää useamman identiteetin turvin tehtyä tai useamman todellisen toimijan kollektiivista arvostelujen manipulointia. Dellacoras (2005, 2010) on tunnistanut kolme päätyyppiä tällaisille väärinkäytöksille:

- Äänestyksen täyttäminen (ballot stuffing), jossa siihen osallistuvat osapuolet keinotekoisilla transaktioilla parantelevat mainettaan ja arviointiaan. Tätä voidaan jossain määrin hallita keräämällä arviointeja vain todellisten kauppatapahtumien jälkeen tai sallimalla kerrallaan vain yksi arviointi samalta identiteetiltä, jolloin vain uusin arvio jää voimaan.
- Negatiivisen tiedon välittäminen (bad-mouthing), jossa yksi henkilö useamman pseudonyymin turvin tai useampi henkilö kollektiivisesti antaa huonon arvion kohteesta vähentääkseen yhteisön luottamusta kohteeseen (esim. yksilö, tuote tai palvelu jne.). Toisaalta aiheellisen negatiivisen palautteen ja mustamaalaamisen välistä eroa on käytännössä vaikea havaita.

- Positiivisen ja negatiivisen palautteen diskriminointi, jossa esim. myyjä voi toimittaa kaikille muille asianmukaisen tuotteen lukuun ottamatta muutamia, jolloin yleinen arviointi luotettavuudesta muodostuu positiiviseksi (On-Off- ja CB-hyökkäykset).

Koska online-palveluissa identiteetin eli pseudonyymin tai käyttäjätunnuksen muodostaminen on tyypillisesti helppoa, syntyy tästä monia tunnistettuja ongelmia (Tavakolifard & Almeroth 2012, Sun ym. 2012, Spitz & Tuchelmann 2011). Tässä yhteydessä voidaan käsitellä niistä esimerkin omaisesti muutamia; täydellisempiä ja systemaattisempia mainejärjestelmien tietoturvauhkien kartoituksia löytyy esim. lähteestä Spitz ja Tuchelmann (2011). Periaatteessa yksinkertaisin ja tehokkain tapa vähentää väärinkäytöksiä olisi vaatia identiteetin vahva tunnistus (ID verification) järjestelmään rekisteröitymisen yhteydessä, mutta tähän ei ole kuitenkaan lähdetty lähinnä kustannus- tai mukavuussyistä (Spitz & Tuchelmann 2011).

Sybil-hyökkäyksessä (Sybil attack) yksi henkilö voi luoda useita pseudonyymejä, joiden avulla mainejärjestelmään voidaan vaikuttaa suhteettoman paljon. Manipulointia on tehty jopa kaupallisesti: esim. Sun ja Yuhong (2012) esittävät kiinalaisten pienyritysten tarjoavan Taobao-kauppapaikan ”reputation ting” -palveluita. Sybil-hyökkäyksestä on olemassa eri versioita, kuten oskillaatiohyökkäys, jossa pseudonyymit jaetaan samanaikaisesti useisiin ryhmiin, joilla nostetaan omaa arviointia ja huononnetaan kilpailijoiden vastaavaa. RepTrack-hyökkäyksessä keskitytään vain jonkin kohteen arvioinnin huonontamiseen. (Sun & Yuhong 2012.)

Toinen ongelma on jo aiemmin mainittu identiteetin helppo vaihtaminen (ns. churn attack), jolloin aikaisempi huono maine voidaan helposti nollata (whitewashing). Tämän tyyppistä käyttäytymistä voidaan estää tekemällä identiteetin monistamisesta ja vaihtamisesta hankalaa esim. autentikoinnin tai identiteetin todentamisen (esim. digitaaliset sertifikaatit) avulla, vaatimalla rekisteröitymismaksu, kytkemällä IP-osoitteita identiteettiin tai tekemällä toiminnasta kannattamatonta pienentämällä juuri rekisteröityneen luotettavuutta. Jälkimmäiseen tapaan liittyy kuitenkin ns. kylmäkäynnistysongelma (cold start), jolla tarkoitetaan sitä, että uuden yhteisöön liittyneen käyttäjän on hankala saada kasvatettua mainettaan. Esimerkiksi verkkokaupoissa (kuten eBay) käyttäjät yleensä asioivat vain järjestelmän korkealle rankkaamien toimijoiden kanssa, jolloin uuden käyttäjän on hankalaa päästä muiden kanssa interaktioon ja kasvattaa omaa luottamustaan.

Petollisen toimijan ei välttämättä edes tarvitse vaihtaa ID:tä, vaan hän voi omalla toiminnallaan pitää maineensa tavoittelemallaan tasolla tekemällä esim. reilua kauppaa pieniarvoisilla transaktioilla ja korkean rankkauksen avulla huijata vastaavasti suurissa kaupoissa (Sun & Yuhong 2012). Tämän tyyppistä toimintaa, eli ns. On-Off- tai CB (Conflicting Behaviour) -hyökkäyksiä, voidaan pyrkiä estämään adaptiivisilla algoritmeilla, jotka alentavat mainetta huomattavasti vain muutamasta huonosta palautteesta. Tähän liittyvät luonnollisesti jälleen epärehellisestä palautteesta syntyvät ongelmat, joten monia eri tekniikoita on yhdisteltävä halutun turvatason saavuttamiseksi. Toinen mahdollisuus on arvottaa suuriarvoiset ja pieniarvoiset transaktiot eri tavalla siten, että pienillä transaktioilla ei voi kasvattaa mai-

netta samalla tavalla kuin suurilla. Tämäkään menetelmä ei ole aukoton ja vaatii tiettyjä erikoisehtoja toimiakseen (Spitz & Tuchelmann 2011).

Koska mainejärjestelmillä on käytännössä suuri merkitys, syntyy helposti kysymys, miksei mainetta voisi siirtää järjestelmien välillä (Alnemr & Meinel 2011, Steinbrecher 2011). Tällöin esim. kylmäkäynnistysongelmaan saataisiin helpotusta. Maineen siirto järjestelmien välillä koostuu kahdesta osasta:

- identiteetin siirrosta
- identiteettiin liittyvän maineen siirrosta.

Identiteetin siirtoon liittyy selkeä yksityisyydensuojaongelma, koska mainejärjestelmät pitävät kirjaa esim. siitä, kenen kanssa ollaan tekemisissä, millaisia kauppatapahtumia yksilö on tehnyt, minkä tyyppisistä asioista hän on kiinnostunut tai minkä tyyppisiä mielipiteitä hän on tullut arvioineeksi. Teknisesti ongelma voitaisiin ratkaista yksityisyyden suojan huomioivalla käyttäjäkeskeisellä identiteetin hallinnalla (PE-IMS, Privacy Enhanced Identity Management Systems) (Steinbrecher 2011), joka mahdollistaisi eri pseudonyymit eli toisiinsa linkittämättömissä olevat osaidentiteetit eri järjestelmissä. Tähän menettelyyn liittyy kuitenkin Sybil-hyökkäyksen mahdollisuus (Steinbrecher 2011).

Toinen ehkä merkittävämpi ongelma on itse maine ja siihen liittyvä käsitteenmuodostus (ts. ontologia tietojenkäsittelyn näkökulmasta). Tietojärjestelmien välillä tapahtuva maineen siirtäminen vaatisi melko yksikäsitteisen sopimuksen maineen esittämistavasta eli sen rakenteen ja siihen liittyvän laajennusmekanismin määrittelyä tai vähintäänkin sopivien muunnosalgoritmien kehittämistä eri mainejärjestelmien välillä. Erilaisia ehdotelmia maineen ontologian kuvaamiseksi on tehty useampiakin (Casare & Sichman 2005, Chang ym. 2005, Alnemr & Meinel 2011), mutta perusongelmaksi jää edelleen se, että maine sosiaalisena rakenteena on subjektiivinen ja kontekstisidonnainen. Kontekstisidonnaisuus viittaa mm. jo aiemmin tunnistettuun eroon eri mainejärjestelmien funktionaalisuuden välillä (luottamuksen rakentaminen vs. laadun mainostaminen) ja toisaalta eroihin eri kohdealueiden (esim. kauppatapahtuma vs. asiantuntijalausunto) välillä. Lisäksi on huomioitava, että eri kulttuuripiireissä on erilaiset normit ja säännöt, joissa maine ja luottamus (sosiaalinen kontrolli) muodostuvat eri tavoin. Käytännössä tämä tarkoittaa, että eri mainejärjestelmissä on jo lähtökohdiltaan epäyhteensopivat mainemallit.

Jokaisessa mainejärjestelmässä on myös omaa mainemallia hyödyntävä algoritmi rating-funktion muodostamiseen. Funktioiden antaman tuloksen tulkinta (esim. yksittäisen rating-arvon) ja siirtäminen mahdolliseen yhteisesti hyväksyttyyn esitystapaan on haastavaa. Kattavat maineen ontologian määrittelyn pyrkimykset ovatkin jäämässä lähinnä akateemisen mielenkiinnon kohteeksi. Myös muunnoksien mahdollisuuksia eri mainejärjestelmien välillä on tutkittu (Pinyol ym. 2007, Vercouter ym. 2007, Steinbrecher 2011). Näissä tarkasteluissa joudutaan kuitenkin heti samankaltaisiin ongelmiin (yhteisen mallin luomiseen) kuin yhteisen ontologian määrittelyssä. Joissakin käytännön järjestelmissä on kuitenkin yritetty yhdistää mainetta useista muista järjestelmistä. iKarma oli yleinen mainejärjestelmä

maineen ylläpitoon eri järjestelmissä, mutta sen toiminta tosin lopetettiin 2015. Toisena esimerkkinä voidaan mainita Trivago-hotellivarausjärjestelmä, joka kokoaa arvostelun useiden muiden matkanvälittäjien mainejärjestelmistä.

Koska maine on yrityksille ja yhteisöille tärkeä imagoon liittyvä tekijä, maineen tarkkailuun ja analysointiin on saatavana lukemattomia erilaisia kaupallisia työkaluja ja palveluita. Näille järjestelmille (esim. Marchex, Yext, Reputation.com jne.) on tyypillistä erilaisten online-kanavien seuraaminen ja yrityksille kielteisen palautteeseen tunnistaminen ja siihen reagoiminen eli yleensä pyrkimys kielteisen palautteen poistamiseen. Kyseessä onkin eräs muoto maineen manipulointijärjestelmistä, jotka laajamittaisesti käytettynä ja toimintatavastaan riippuen saattavat heikentää yleistä luottamusta mainejärjestelmien toimintaan.

6. Yksityisyyden huomiointi eräissä liikennepalveluissa

Nykyisin jo käytössä olevissa liikennepalveluissa on jouduttu ottamaan kantaa niihin mekanismeihin, joilla liikkumistiedon yksityisyyden suoja otetaan huomioon palveluntarjonnassa. Tässä yhteydessä tarkastellaan esimerkin omaisesti satelliittiperustaista tiemaksujärjestelmää Saksassa. Vastaavan kaltaista järjestelmää on ehdotettu käytettäväksi yksityisautoilun osalta myös Suomessa ja sitä on tarkasteltu yleisiltä periaatteiltaan ns. Ollilan työryhmän (LVM 2013) raportissa[2]. Tämän lisäksi esitellään niitä yksityisyyden suojaan liittyviä ratkaisuja, joita on tehty Uber-kyytipalvelussa ja Kutsuplus-joukkoliikennepalvelussa.

6.1 Tiemaksujärjestelmät

EU:n pitkän aikavälin tavoitteena on ”käyttäjä maksaa, saastuttaja saa” -periaate (Sikow-Magny 2004). Useissa Euroopan maissa moottoritiet ja päätiet ovat ruuhkautuneita kasvaneen liikenteen takia ja lisäksi huonossa kunnossa, koska valtiovallalla ei ole varaa teiden ylläpitoon. Liikenteen hinnoittelua pidetään yleisesti tehokkaimpana kysynnän hallitsemisen keinona ja sitä kautta päästään vaikuttamaan liikennejärjestelmän kapasiteetin hallintaan ja tieverkon ylläpidon rahoitukseen. Tästä johtuen useissa Euroopan maissa onkin otettu käyttöön tiemaksut (RUC, Road Usage Charging) eli tieverkon käytöstä perittävät maksut, jotka koskevat toistaiseksi lähinnä raskasta liikennettä muutamaa Euroopan maata lukuun ottamatta. Suomi on niiden maiden joukossa, jotka eivät sovella tiemaksuja raskaaseen liikenteeseen.

Tiemaksut otettiin käyttöön esim. 1995 Tanskassa, Ruotsissa, Belgiassa, Hollannissa, Saksassa ja Luxemburgissa ns. ”eurovinjettinä” eli aikapohjaisena tiemaksuna. EU-direktiivi 1999/62/EC säätelee näitä tiemaksujärjestelmiä, jotka koskevat yli 12-tonnisia ajoneuvoja, joille on säädetty erilaisia maksuja ja alennuksia mm. päästöjen perusteella. Vuonna 2006 tiemaksusuositusta tarkistettiin ulot-

[2] Järjestelmään liittyviä teknisiä haasteita esim. GPS-häirinnän osalta on tarkasteltu Virtasen ja Lehtosen raportissa: Liikenteen sähköisten palveluiden tietoturva – niihin kohdistuvat tietoturvariskit ja häirintämenetelmät sekä näiden vaikutukset ja ennaltaehkäisy, VTT 2016.

tumaan vuoden 2012 jälkeen myös 3,5 tonnia painaviin ajoneuvoihin ja moottoriteiden lisäksi tiemaksuja saatetaan periä myös muilla pääteillä.

Saksan nykyinen raskaiden ajoneuvojen tietullijärjestelmä perustuu satelliittipohjaiseen LKW-Maut (Lastkraftwagen-Maut eli kuorma-autotulli) -järjestelmään, joka on julkisen ja yksityisen sektorin yhteishanke. Järjestelmää operoi yhteisyritys, jonka omistavat DaimlerChrysler Financing (45 %), Deutsche Telecom (45 %) ja ranskalainen tietullimaksuoperaattori Cofroute (10 %), ja järjestelmän noudattamisen valvonnan hoitaa Saksan valtion viranomainen, Bundesamt für Güterverkehr (BAG). Tiemaksujen keruusopimuksen aika on 12 vuotta, ja vuotuisen tuoton arvioidaan olevan n. 650 miljoonaa euroa.

Yksityisyyden suoja on Saksassa otettu huomioon jo järjestelmää rakennettaessa siten, että kahdesta vaihtoehtoisesta lähestymistavasta (Eisses ym. 2006, Vodafone 2006) ns. keskitetty keruu (central aggregation) vs. hajautettu keruu (onboard aggregation) on otettu käyttöön jälkimmäinen. Vastaavasti toteutuksen yhteydessä voidaan puhua verkkopäätelaitteista (thin client) ja älykkäistä päätelaitteista (thick client), joista Saksassa siis valittiin käyttöön jälkimmäinen.

Keskitetyllä keruulla tarkoitetaan menetelmää, jossa OBU lähettää ajoittain (lähettäjän tunnistamista varten) allekirjoitetun viestin, jossa on ajoneuvopäätteen (OBU:n) yksikäsitteinen tunniste (ID) ja aikaleimoineen kaikki ne koordinaattipisteet (esim. GPS), jotka ovat uusia edelliseen viestiin nähden. Keskitetty palvelu tunnistaa lähetettyjen tietojen perusteella ajetun reitin ja laskee sille hinnan tiesegmenttien hinnoittelun mukaan ja vähentää ennakolta määriteltyä tilin saldoa (pre-paid optio) tai laskuttaa jälkikäteen liikennöijää. Hyvänä puolena tässä pilvipalveluiden kanssa samantyyppisessä menetelmässä on muutosten hallinta, esim. tiesegmenttien hintatietojen ja karttatietojen päivitettävyys on helppoa. Huonoa on taas seurattavan kohteen lähes täydellisen liikkumistiedon välittäminen keskitettyyn palveluun, jossa tietojen väärinkäyttö (tietomurto tms.) ja yksityisyyden suojaan kohdistuvat loukkaukset ovat helpommin mahdollisia. Tässäkin järjestelmässä on saavutettavissa jonkinlainen anonymiteetti samaan tapaan kuin puhelinliittymissä on pre-paid-menettelyjä. Toisaalta OBU:n ID:n on oltava edelleen tiedossa, mutta ID:n ja laskutustiedon välinen yhteys voidaan salata.

Hajautetulla paikalliseen älykkyyteen perustuvalla järjestelmällä tarkoitetaan puolestaan laskutusmenetelmää, jossa OBU itse ylläpitää jatkuvasti aikaleimoilla varustettua koordinaattitietoa ja kuljettua matkaa, mutta laskee hinnan kuljetulle matkalle ja rekisteröi sen peruuttamattomasti OBU:n muistiin, josta OBU:n tunniste, kuljettu matka ja hinta lähetetään määrävälein laskutusta varten tietullien hallintakeskukseen.

Jälkimmäinen menetelmä edellyttää, että päätelaitteella on käytettävissä tarkka karttatieto, tiesegmenttien hintatiedot, varmennettu (esim. sertifioitu) hintojen laskenta-algoritmi ja tietoturvaelementit, jotka tekevät tietojen laskemisesta ja tallentamisesta turvallisen. Luotettavuuden takaamiseksi tarvitaan esim. tapahtumalokeja ja erillisiä varautumia virhetilanteiden (esim. GPS-signaalin häviäminen ja täydentäminen ”Dead-Reckoning”-tekniikalla) hallintaan. Ylläpidon kannalta järjestelmä on huomattavasti monimutkaisempi esim. päivittää (karttatiedot, segmenttien

hintatiedot, laskenta-algoritmit jne.), mutta yksityisyyden suojan kannalta taas menettely on huomattavasti keskitettyä turvallisempi.

Molemmissa tapauksissa väärinkäytösten (OBU:n vahingoittamisen, päältä pois ottamisen tai häirinnän jne.) estämiseen tarvitaan lisäksi riittävät pelotteet (sanktiot sakkoina tms.) ja valvonta. Valvonta on helposti järjestettävissä pistokokein, rekisterikilpien automaattisella tunnistuksella jne.

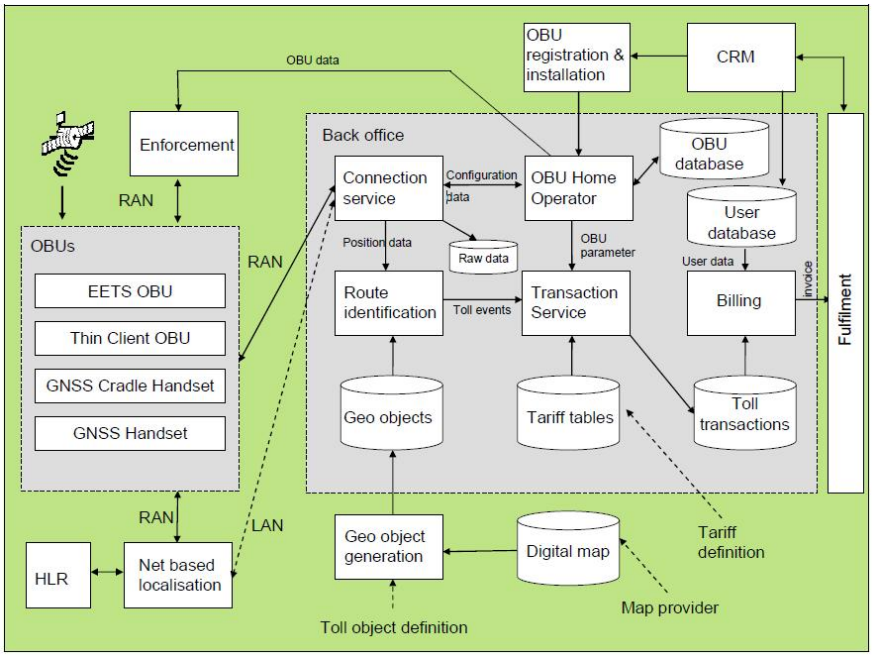
Tiemaksujen maksuun Saksassa on olemassa kaksi vaihtoehtoa:

- ajoneuvolaite (OBU, On Board Unit), jonka valtuutettu tullinkeräysosapuoli asentaa ajoneuvoon
- internetin tai tienvarsipäätelaitteiden kautta tapahtuva maksaminen. Tienvarsipäätelaitteita on käytännössä kaikilla rekkojen pysähdyspaikoilla Saksassa (yli 3500 päätelaitetta käytettävissä).

Molemmissa tapauksissa menettely on samankaltainen: järjestelmä laskee lyhyimmän reitin, ja liikennöijä rekisteröi sen käyttöönsä ja saa varausnumeron kuittina. Käytännössä ajoneuvolaite on kuitenkin kätevämpi usein tapahtuvaan liikennöintiin, ja tällöin GPS-perustainen OBU-järjestelmä tunnistaa käytetyt tiesegmentit kartasta, laskee käytön hinnan ja lähettää laskutustiedot säännöllisin väliajoin tietullien keruun keskukseen.

Ajoneuvolaitteen paikanmäärityksen tueksi ja paikannuksen tarkkuuden maksimoimiseksi käytetään lisätunnistimia (dead reckoning), kuten gyroskooppia ja nopeusmittarin signaalin tunnistusta (suunta ja liike), ja satelliitti- ja lisäpaikannuksen tuloksia verrataan toisiinsa. OBU laskee maksettavan tiemaksun reittitietojen ja tiemaksujen sekä syötettyjen ja tallennettujen ajoneuvotietojen perusteella ja lähettää maksutiedot salattuina Toll Collect -keskukseen.

Saksan kaltaista järjestelmää suunniteltiin myös Hollantiin (kuva 2), mutta toteutuksesta on toistaiseksi luovuttu osittain järjestelmän monimutkaisuuden, luotettavuuden (Zijderhand ym. 2006) ja kustannussyiden ja osittain yksityisyyden suojaan liittyvien ongelmien (ITSinternational 2011) takia. Saksankaan järjestelmä ei ole ollut ongelmaton, etenkin käyttöönottovaiheessa vaikeuksia oli runsaasti ja hanke viivästyi aikataulustaan. Vuoden 2016 alusta Saksassa otettiin henkilöautoliikenteessä käyttöön elektroninen vinjettityyppinen ratkaisu satelliittiperustaisen seurannan sijaan.



Kuva 2. Hollantiin suunnitellun satelliittipohjaisen tietullijärjestelmän toiminnallinen arkkitehtuuri (Vodafone 2006).

6.2 Uber-kyydinvälitysjärjestelmä

Toinen esimerkki modernista sijaintitietoa soveltavasta liikennepalvelusta on Uber-taksi- ja matkanjakojärjestelmä. Uber on vuonna 2010 San Franciscosta liikkeelle lähtenyt taksi- ja matkanvälitykseen tarkoitettu palvelu, joka hyödyntää tekstiviestejä ja älypuhelinsovelluksia (iPhone ja Android) siten, että käyttäjä voi tilata kyydin nykyisestä tai osoittamastaan paikasta (Uber 2015). Vastaavia järjestelmiä on useita, esim. Lyft ja Sidecar USA:ssa sekä LeCar ja CarPooling.com Euroopassa, mutta Uber lienee saanut näistä eniten huomiota osakseen julkisuudessa. Uber toimii myös Suomessa, ja sen kilpailija on lähinnä virolainen Taxify, jonka toimintaperiaatteet muistuttavat Uberia. Uber-palvelun laillisuuteen ei tässä yhteydessä oteta kantaa, mutta useissa Euroopan maissa sen eräiden muotojen on katsottu rikkovan lainsäädäntöä.

Uber ja vastaavat toimijat käyttävät palveluistaan nimitystä ”peer-to-peer transportation” -alustat eivätkä suoraan viittaa kuljettajapalveluihin lisensointi-, sääntely- ja vakuutusteknisistä syistä. Uber-kuljettajat ovat joko itsenäisiä toimijoita tai jonkin taksiyritystyyppisen yrityksen palveluksessa. Uberin ansaintamalli perustuu jokaisesta matkasta otettuun n. 20 %:n provisioon; 80 % tuloista jää kuljettajalle, joka vastaa kaikista liikennöinnistä aiheutuvista kustannuksista.

Palvelun käyttö on yksinkertaista. Asiakas luo Uber-tilin, johon tarvitaan nimi, sähköpostiosoite, puhelinnumero ja laskutustiedot. Tilin luonti tapahtuu Uber-

verkkopalvelun kautta, ja saatuaan varmistusviestin rekisteröitymisestä asiakas voi ladata Uber-sovelluksen omaan puhelimeensa. Sovelluksen avulla voi valita mieleisiä optioita palvelusta ja ilmoittaa paikan, josta haun halutaan tapahtuvan. Hakupiste voi olla esim. käyttäjän nykyinen sijainti tai kartasta Uber-sovelluksella osoitettava paikka.

Palvelu varmistaa tilauksen ja maksutavan sekä ilmoittaa oletetun hakuajan ja matkan hinnoitteluun liittyvät tiedot. Taksin tapaan matkan kokonaishintaa ei ilmoiteta, koska määränpäätä ei kysytä. Hinnoittelu muistuttaakin taksihinnoittelua eli on aika- ja matkaperustainen, ja laskutus tapahtuu matkan päätyttyä. Tämän jälkeen käyttäjä voi arvioida kuljettajan toiminnan sovelluksen kautta, ja vastavuoroisesti kuljettaja voi arvioida kyyditettävän.

Sinänsä Uber ei tarjoa Suomen taksijärjestelmään verrattuna juurikaan suurta palveluinnovaatiota (paitsi parantuneen käyttöliittymän), koska täällä on jo käytössä paikkatietoon perustuva taksinvälitys. Kuitenkin niillä markkinoilla, joissa välitysjärjestelmä on kehittymättömämpi, Uber helpottaa huomattavasti kysynnän ja tarjonnan kohtaamista ja muuttaa markkinarakenteita. Yhdysvalloissa on arvioitu, että taksit seisovat 47 % kokonaisajasta, mikä aiheuttaa liikennöitsijöille laskennallisesti viiden miljardin menetykset vuodessa. Uberin käyttömukavuus antaa kuitenkin nykyisiin kotimaisiin välitysjärjestelmiin nähden selkeää kilpailuetua.

Koska Uber-palvelu perustuu kokonaan sijaintitietoon, yksityisyyden suojan haasteet ovat ilmeiset. Kun asiakas käyttää Uber-palvelua, se paikantaa käyttäjän sijainnin ja mahdollistaa lähimmän vapaan Uber-kuljettajan tavoittamisen lähettämällä tälle tilauspyynnön sijaintitietoineen. Asiakkaalle näytetään reaaliaikaisesti, kuinka tilattu kuljettaja lähestyy asiakasta. Paikkatieto menee myös Uberin helpdesk-palveluun mahdollisia ongelmia varten. ”Share my Ride” -optio, eli kimppakyytimahdollisuus, antaa myös ajonaikaisen sijaintitiedon käyttäjän valitsemille henkilöille.

Uber-kyydin aikana kerätään n. 15 metrin tarkkuudella sijaintitiedot koko reitin varrelta kuljettajan Uber-sovelluksesta. Kun kyydin ottaja tiedetään, Uber kerää siis koko reitin kyyditettävästä. Tämä tieto on välttämätön laskutusta ja kuittia varten sekä mahdollistaa myös valitusten käsittelyn, tulivat ne sitten asiakkaan tai kuljettajan taholta. Uber käyttää kerättyjä tietoja anonymisoidusti tekemällä analyysiä sen perusteella, mitä palvelun piirteitä käytetään useimmin, minkälaisia tunnistettavia käyttökuviota esiintyy ja minne palvelu kannattaa suunnata. Uber myös jakaa kerättyä anonymisoitua tietoa kolmansille osapuolille Uberin omia tarpeita silmällä pitäen palvelun kehittämistä varten.

Uber määrittelee yksityisyydensuojamenettelynsä erikseen Yhdysvaltain ja globaalien markkinoiden mukaan. Globaaleja markkinoita varten Uber on rekisteröitynyt Alankomaihin ja noudattaa Alankomaiden tietosuojalainsäädännön mukaisia periaatteita. Dutch Data Protection Authority (DDPA) valvoo, että Alankomaiden lainsäädännön mukaista tulkintaa Euroopan tietosuojasuosituksesta noudatetaan Uber-palvelussa. Uber on myös rekisteröitynyt EU:n ja Yhdysvaltojen väliseen Safe Harbour -ohjelmaan. Palveluun rekisteröitymisvaiheessa asiakas hyväksyy Uberin käyttösopimuksen ja sen yksityisyydensuojaperiaatteet.

6.3 Kutsuplus

Hieman Uber-palvelua vastaava suomalainen kutsuliikennekokeilupalvelu on HSL:n Kutsuplus (Kutsuplus 2015), jota Helsingin Seudun Liikenne (HSL) operoi minibusseilla. Kutsuplus-palvelu perustuu tilaus-, ajoitus- ja laskutusjärjestelmään, jonka on kehittänyt ja jota operoi Ajelo Oy, Aalto-yliopiston teknisen korkeakoulun spin-off-yritys. Palvelun käyttö perustuu Kutsuplus-tilin avaamiseen web-liittymän kautta ja rahansiirtoon luottokortilta tai pankkitililtä virtuaaliseen lompakkoon, jota käytetään matkojen maksamiseen.

Kuljetuksen tilaus tehdään ilmoittamalla lähtö- ja kohdepysäkit katuosoitteiden tai HSL:n pysäkkinumeroiden mukaan, ja kuljetukset tapahtuvat HSL:n normaalin liikennöintiverkon puitteissa. Tilauksen voi älypuhelinsovelluksen lisäksi tehdä SMS-viestillä ja tilauksen yhteydessä voi määrittää lähtöajaksi heti tai viisi tai kymmenen minuuttia tai korkeintaan tunti nykyhetkestä. Tilaus vahvistetaan varauskoodilla, joka toimii samalla matkalippuna ja joka esitetään kuljettajalle ajoneuvoon noustessa. Kuittaus tilauksesta sisältää myös olettavan odotusajan ja liikennöivän minibussin ajoneuvonumeron. Kuittauksen jälkeen muutoksia tai peruutuksia ei enää voi tehdä. Kutsuplus-laskutus perustuu kiinteään osaan (3,5 euroa) ja 0,45 euron kilometriperustaiseen laskutukseen ns. suoran reitin mukaan.

Toimiakseen Kutsuplus tarvitsee samantyyppisiä tietoja kuin Uber eli käyttäjän nykyisen sijainnin, noutopisteen (bussipysäkin) tiedot sekä ajoneuvon sijainnin. Liikenteenohjaukseen käytetyn ajoitusalgoritmin täytyy myös tietää kohdeosoite, jotta optimaalinen ajoneuvon reititys kyytejä tarvitsevien reittien mukaan onnistuu.

HSL ja Ajelo noudattavat EU:n tietosuojasuosituksia, ja lisäksi käyttäjille tarjotaan läpinäkyvyys kerättyyn tietoon, eli asiakas voi tarkistaa itsestään kerätyn tiedon, johon kuuluvat HSL:n osalta nimi, osoite, sähköpostiosoite, puhelinnumero, äidinkieli, sukupuoli ja ikä ja Ajelon osalta näiden lisäksi syntymäaika, puhelinnumero, asuinpaikka jne. HSL käyttää tietoja oman toimintansa kehittämiseen, statistiikkaan ja markkinointiin eikä jaa tietoja kolmansille osapuolille.

Ajelon keräämä palvelutieto sisältää lisäksi laskutustiedot ja reittitietoja, jotka ovat melko kattavia, esimerkiksi vuoronumeron, käyttäjäprofiilitunnisteen, hinnan, kuljettajan tunnistetiedot ja ajoneuvontiedon. Näitä tietoja säilytetään reklamointien käsittelyä varten kaksi kuukautta, jonka jälkeen ne automaattisesti poistetaan. Käyttäjillä on mahdollisuus poistaa myös näitä historiatietoja yksittäisistä matkoista Ajelon web-palvelun kautta. Ajelo ei välitä tietoja edelleen kolmansille osapuolille, jotka eivät osallistu palvelun tuottamiseen. Käyttäjä hyväksyy käyttöehdot rekisteröityessään palveluun www.kutsuplus.fi ja luodessaan käyttäjätilin. Mikäli käyttäjä ei käytä palvelua viiteen vuoteen, käyttäjätili poistetaan palvelusta. Kutsuplus-palvelua ollaan rahoitusongelmien takia ajamassa alas vuoden 2016 aikana.

6.4 ITS-palveluiden yksityisyyden suoja

Liikenteen älypalveluiden yksityisyyden suojaa on laajemmin tarkasteltu Algoe Consultants- ja RappTrans-konsulttiyhtiöiden selvityksessä (Eisses ym. 2012) EU:n toimeksiannosta vuonna 2012. Tarkoituksena oli selvittää, mitkä liikennepalvelut ja palvelutyypit ovat altteimpia kohtaamaan yksityisyyteen liittyviä haasteita. Raportissa käytettiin kolmentyypistä uhkaluokitusta:

- T1 – luvaton pääsy henkilötietoihin
- T2 – henkilötiedon uudelleenkäyttö muihin kuin niihin tarkoituksiin, joita varten sitä on alkuperäisesti kerätty käyttäjän suostumuksella
- T3 – tiedon ylimääräinen käsittely alkuperäiseen tarkoitukseen nähden.

EU:n lainsäädännössä paikkatietoa ei ole luokiteltu erityisen sensitiiviseksi tiedoksi, kuten etninen alkuperä, uskonto, poliittiset mielipiteet, terveystieto jne. Mutta kuten aiemmin todettiin, sijaintitieto voi epäsuorasti paljastaa edellisen kaltaiset ominaisuudet henkilöstä. Raportin (Eisses ym. 2012) tuloksista esitetään yhteenveto taulukossa 3. Tässä yhteydessä ei kuitenkaan lähdetä erittelemään jokaisen palvelun saamaa luokitusta tämän enempää ja arvioimaan luokituksen perusteita ja oikeellisuutta. Kiinnostuneita lukijoita suositellaankin tutustumaan alkuperäiseen lähteeseen (Eisses ym. 2012).

Taulukko 3. Eräiden älyliikennepalveluiden yksityisyyden suojan uhkatekijöiden luokittelua (perustuu lähteeseen Eisses ym. 2012).

Palvelu/sovellus	T1 – luvattoman pääsyn riski	T2 – henkilötiedon uudelleenkäytön riski	T3 – ylimääräinen tiedonkäsittelyn riski
Digitaalinen ajopiirturi	matala	matala	keskimääräinen
e-Call	matala	matala	keskimääräinen
Käyttömaksut tietullein	keskimääräinen	keskimääräinen	keskimääräinen
Satelliittiperustaiset tienkäyttömaksut	keskimääräinen	korkea	korkea
Pysäköinnin verkkomaksaminen	matala	keskimääräinen	keskimääräinen
Sähköinen matkalippu julkisessa liikenteessä	keskimääräinen	korkea	korkea
Ajoperustainen vakuutusmaksu (PAYD)	matala	korkea	korkea
Autokannan satelliittiperustainen hallinta (fleet management)	keskimääräinen	keskimääräinen	korkea
Liikenteen tilannekuvan muodostaminen paikannusjärjestelmän (satelliittitieto) pohjalta	keskimääräinen	korkea	keskimääräinen
Liikenteen tilannekuvan muodostaminen soluverkkojärjestelmätiedon pohjalta	matala	keskimääräinen	matala
Yhteistoiminnalliset ajojärjestelmät (co-oprative driving)	korkea	korkea	keskimääräinen

7. Älyliikennepalveluekosysteemit, yksityisyyden suoja ja luottamus

Teoreettisista lähtökohdista tarkasteltuna liiketoimintaekosysteemi määritellään joukkona toimijoita, jotka muodostavat laajennetun, toisiaan tukevan järjestelmän. Mooren (1993) mukaan liiketoimintaekosysteemit syntyvät osittain tarkoituksella, osittain itseorganisoituvasti tai jopa sattumalta. Yksinkertaistettuna liiketoimintaekosysteemi on joukko yrityksiä, jotka kollektiivisesti tuottavat integroidun teknologiaperustaisen järjestelmän, joka luo asiakkailleen arvoa.

Innovaatiorahoituskeskus Tekes määrittää liiketoimintaekosysteemin eri alojen yritysten yhteistyön muodoksi, jossa ne kilpailevat ja luovat yhdessä kyvykkyyksiä uusien innovaatioiden ympärille. Liiketoimintaekosysteemi voidaan Tekesin mukaan nähdä liiketoimintaverkostoina, joissa ”toimijat tekevät yhteistyötä luodakseen toisiaan täydentävien kyvykkyyksien ja voimavarojen ja yritysten järjestelmän tuotteen tai palvelun asiakasarvon kasvattamiseksi”.

Iansiti ja Levien (2004) ovat yrittäneet määritellä ekosysteemin jäsenten rooleja ja niitä tekijöitä, jotka luovat pohjaa liiketoimintaekosysteemin onnistumiselle. Tutkijoiden mukaan ekosysteemissä tunnistettavat roolit ovat kulmakivet (keynotes), hallitsijat (dominators) ja markkinarakopelurit (niche players):

- Kulmakivet (ekosysteemialustan johtajat) mahdollistavat koko ekosysteemin olemassaolon ja vaikuttavat suoraan muiden sen jäsenten (ja itsensä) menestymiseen tarjoamalla pysyvän ja ennustettavan joukon etuja (assets). Tällaisia ovat mm. teknologialustat ja alustan päälle rakentuvat eri palvelut, jotka yksinkertaistavat ja helpottavat monimutkaisten tehtävien suorittamista.
- Hallitsijat (”wannabes”) valtaavat ja jakavat suuren osan ekosysteemistä ja pyrkivät maksimoimaan oman hyötynsä (arvonkaappauksensa) siitä. Hallitsijoilla on taipumuksena eliminoida muita yrityksiä ekosysteemistä omaksumalla niiden toimintoja.
- Markkinarakojen etsijät muodostavat suurimman joukon ekosysteemissä ja vaikka niillä ei yksinään olekaan suurta vaikutusta ekosysteemissä, ne luovat suurimman osan sen arvosta tarjonnallaan. Markkinarakojen etsijät ovat hyvin erikoistuneet ja erottuvat selkeästi toisistaan.

Seuraavien kahden ehdon tulisi täyttyä, jotta ekosysteemi voi muodostua:

- Liiketoimintakonsepti tuottaa arvoa suurelle joukolle asiakkaita.
- Konsepti skaalautuu tämän markkinapotentiaalin saavuttamiseksi.

Suomalaisten liikennepalveluiden älyliikennepalveluiden ekosysteemiä (koskien ITS-palvelutarjontaa) ei toistaiseksi ole syntynyt luonnollisen kysynnän kautta toivotulla vauhdilla. Suurin ongelma ekosysteemin arvonluonnin kannalta on ns. muna-kanaongelma, jossa kahden ryhmän arvolupaukset ovat riippuvaisia toisistaan. Tämä ilmenee seuraavasti:

- Yritykset ovat haluttomia ottamaan riskiä vasta kehittymässä olevilla markkinoilla ja kehittämään uusia palveluita potentiaalisten asiakkaiden puuttumisen takia.
- Asiakaskysyntää ei puolestaan ole, koska käyttäjien kannalta arvokkaiksi koettujen ITS-palveluiden tarjonta puuttuu.

Selvää toki on, että arvokkaaksi koettua liikennepalvelutarjontaa on jo monessa muodossa olemassa sekä julkisessa liikenteessä että yksityisissä kuljetus- ja logistiikkapalveluissa. Sen sijaan informaatiotekniikkaan perustuvat, kuluttajille tarjotut liikenteen lisäarvopalvelut ovat vasta kehittymässä ja toistaiseksi hajanaiset.

Eräät älyliikennettä tukevat informaatiopalvelut ovat jo käyttäjien saatavilla ja suosittuja, esim. HSL:n reittiopasta käyttää 150 000 asiakasta päivittäin. Vastaavia koko maan kattavia ”multimodaalisia” eri liikkumistapoja yhdisteleviä reittitietopalveluita ovat esim. Liikenneviraston ylläpitämä matka.fi, joka perustuu julkisen liikenteen koontitietokantaan syötettyihin tietoihin. Valitettavasti matka.fi-koontitietokannan liikennöitsijöiltä saatujen reitti- ja pysäkkitietojen kattavuus ei ole paras mahdollinen, koska kaikki vastuutahot eivät ole toimittaneet sinne tarvittavia tietoja (Bäckström ym. 2012). Yksityisellä puolella esimerkiksi Google ja Here tarjoavat sekä yksityisautoiluun että julkiseen liikenteeseen liittyviä informaatiopalveluita, kuten Google Mapsin liikennetiedot tai Here Transit ja Here Omat matkat.

Edellä mainittuja muutamia poikkeuksia lukuun ottamatta älyliikenteen informaatiopalvelut ovat kuitenkin toisistaan hajallaan ja epäyhteensopivia, jolloin:

- Tiedot, joita palvelut tuottavat ja käyttävät, ovat pääasiassa vain yksittäisten palveluntarjoajien käytössä, eikä niitä hyödynnetä muissa palveluissa. Yhteisen alustan hyödyt, tiedon uudelleenkäyttö ja mahdollisuudet avoimiin innovaatioihin jäävät näin hyödyntämättä.
- Markkinoiden ollessa vahvasti segmentoituneet ja hajanaiset käyttäjien tietoisuus palveluista on vähäistä, ja siten palvelun tarjonnan ja kysynnän kohtaaminen on haasteellista.

Julkisen sektorin palveluissa on ongelmana se, etteivät käyttäjät välttämättä näe palvelun hyötyjä suoraan. Vaikka tehokkaampi liikenteenohjaus reaaliaikaisen

tilannekuvan avulla pystyisi hallitsemaan liikennevirtoja entistä paremmin, käyttäjien subjektiivinen kokemus liikenteen sujuvuudesta voi olla aiempaa huonompi, jos liikenneruuhkat kasvat edelleen liikennemäärien kasvun seurauksena.

Kilometriperustaisen verotuksen hyötyjen näkeminen voi olla vieläkin haastavampaa, koska järjestelmä on aiempaa kalliimpi ylläpitää ja se vaatii ajoneuvokohtaisia pakollisia investointeja seurantalaitteeseen (OBU). Jos käyttäjät eivät koe saavansa mitään suoraan havaittavaa hyötyä järjestelmästä ja pelkona on lisäksi ”isoveli valvoo” -seuranta (yksityisyyden suojaan kohdistuvat uhat) sekä kasvaneet kustannukset, järjestelmähyötyjä on vaikea markkinoida, vaikka alustavat tutkimustulokset (Aula 2014, Innamaa ym. 2015) antavatkin viitteitä siitä, että osa liikkujista näkee ”kilometriperustaisen verotuksen reiluna liikenteenä kaikille”.

Edellä mainittua taustaa vasten yksityisen sektorin tuottamat älykkäät liikenteen lisäarvopalvelut ovat viranomaisten kannalta vähintäänkin toivottavia, ja Liikennelabra-hankkeessa[3] julkisen sektorin tarkoituksena on edesauttaa niiden syntymistä public-private-partnership-periaatteella.

Liikennelabran lisäksi tällä hetkellä on näköpiirissä muutama kansallisesti merkittävä aloite, joilla on mahdollisuus kehittyä merkittäviksi ITS-palvelualustoiksi. Ne kokoaisivat eri toimijoita ja palveluita niin yksityiseltä kuin julkiseltakin sektorilta yhteiseen ekosysteemiin. Näitä mahdollisia kehityspolkuja edustavat joukkoliikenteen palvelualusta (”matkatili”) sekä MaaS-operoinnin ympärille syntyvät palvelukokonaisuudet, jotka myös nivoutuvat toisiinsa.

7.1 Joukkoliikenteen palvelualusta

Vuonna 2013 perustettiin kaupunkien ja valtion yhteinen TVV lippu- ja maksujärjestelmä Oy. Sen tarkoitus on ylläpitää ja kehittää yhdessä Tieto Oy:n kanssa kilpailutetussa liikenteessä käytettävää uutta lippu- ja maksujärjestelmää. Järjestelmällä tähdätään

- kaupunkiseutujen yhtenäiseen lippu- ja maksujärjestelmään korvaamalla käytössä olevia useita eri toimijoiden maksujärjestelmiä ja matkakortteja. Nykyisin Suomessa on käytössä sadoittain (ehkä jopa tuhat) erilaista lipputuotetta.
- tiedon tuottamiseen liikenteen suunnittelun ja päätöksenteon tueksi sekä tehokkaan julkisen rahoituksen kohdentamisen edistämiseen
- kustannussäästöihin, kun yksittäisten kaupunkien ei tarvitse hankkia ja ylläpitää omaa järjestelmää. Tällä hetkellä maksujärjestelmän kustannukset sisältyvät toimittajan lipputuotteisiin ja palkkioihin.
- liikennepalveluiden tasapuoliseen kilpailuttamiseen ja helpottamaan liikennöitsijöiden alalle tuloa ja osallistumista tarjouskilpailuihin.

[3] www.liikennelabra.fi

- hallitusohjelman ja liikennepoliittisen selonteon tavoitteiden tukemiseen yhteiskäyttöisistä joukkoliikennepalveluista, kun yhtenäinen palvelu helpottaa matkustamista eri puolella maata. Tavoitteeksi on asetettu kasvattaa joukkoliikenteen matkamäärää 200 miljoonalla uudella matkalla vuodessa vuoteen 2022 mennessä.

ELY-keskuksia edustava Liikennevirasto ja 22 joukkoliikenteestä vastaavaa toimivaltaista kaupunkia perustivat TVV lippu- ja maksujärjestelmä Oy:n hallinnoimaan viranomaisten yhteistä järjestelmää nimeltä Waltti, jolla pyritään vastaamaan edellä mainittuihin tulevaisuuden haasteisiin. Waltti-korttiin voi ladata halutun lipputyypin joko käyttöaikaan, matkojen määrään tai tiettyyn summaan perustuen.

Waltti-järjestelmä ei kuitenkaan yksin pysty vastaamaan Suomen joukkoliikenteen haasteisiin. Joukkoliikenteen muutosta suunniteltaessa todettiin, etteivät nykyiset järjestelmät ole keskenään yhteensopivia, eikä niillä voi muodostaa eri kulkumuotoja yhdistäviä ”ovelta ovelle -matkaketjuja”. Suomen joukkoliikenteessä tehdään vuosittain n. 550 miljoonaa matkaa eli yli sata matkaa jokaista suomalaista kohti.

Waltti-kortin piiriin arvioidaan kuuluvan noin neljä miljoonaa asukasta, joista matkakortin hankkinee 300 000–600 000 henkilöä, ja matkoja tehdään n. 200 miljoonaa vuodessa. Helsingin seudun liikenteen (HSL) piirissä on n. 1,4 miljoonaa asukasta ja alueella käytössä on noin miljoona matkakorttia (Finnberg 2014). Matkoja tehdään vuodessa n. 350 miljoonaa. Jotta joukkoliikenteen matkaketjuista saataisiin aukottomia, tarvitaan mukaan myös kaukoliikenteen palvelut sekä tavanomaista joukkoliikennettä täydentäviä palveluja.

Pitemmän aikavälin tavoitteena olisi HSL- ja Waltti-matkakorttien sekä muiden joukkoliikennepalveluiden (kaukoliikenne, VR) yhdistäminen yhteistoimivaksi järjestelmäksi, jolloin voitaisiin puhua ”kansalaisen matkatilistä” (Finnberg 2014). Kehityksen esteenä ovat kuitenkin sekä toimijoiden keskinäiseen yhteistoimintahaluun että tekniikkaan liittyvät ongelmat. Pelkästään Waltti- ja HSL-matkakorttien yhdistäminen on ollut teknisesti hankalaa lähinnä tietoturvasyistä. Nykyisissä korttijärjestelmissä rahastustieto on itse älykortissa ja rahastuksen käsittelylogiikka ajoneuvoissa sijaitsevissa päätelaitteissa eli kortinlukijoissa. Tietoturvaratkaisut (ns. tietoturvamodulit) ovat eri korttijärjestelmissä toisistaan poikkeavat, jolloin niiden yhdistäminen on ollut teknisesti työlästä, joskin yhteentoimivaan ratkaisuun on päädytty.

Tulevaisuudessa on tavoitteena tunnisteperustainen (ns. ID-pohjainen) ratkaisu, jossa rahastuksen käsittelylogiikka on taustajärjestelmässä. ID-pohjaisuus mahdollistaisi helpommin saumattomat matkaketjut. Tunnistepohjaisessa yhteiskäytössä siirretään tietoja maksujärjestelmien välillä järjestelmien kesken ostetuista matkoista. Tunniste voidaan kortin sijasta tallettaa vaikka matkapuhelimeen. Matkoihin liitetään vain asiakkaan hallussa oleva tunniste ja itse matkustajasta välitetään vain sellaisia tietoja, jotka ovat välttämättömiä matkalipun kelpoisuuden var-

mistamiseksi. Järjestely on siis yksityisyyden suojan kannalta suotuisa, eikä koko matkaketjua koskeva tieto keräänny yhdelle maksuoperaattorille[4].

Yhtenäinen koko maan kattava ”matkatili” (liikkumisen palvelualusta tai pikemminkin tapahtumanvälitysjärjestelmä) mahdollistaisi kuluttajille (Finnberg 2014)

- keinon suunnitella matkaketju luotettavasti tarjolla olevan, eri liikennemuotojen reitti- ja aikataulutietoja yhdistelevän tietopalvelun avulla
- matkojen selkeän hinnoittelun ja ostamisen helppouden. Liikenteen toimijoiden myyntijärjestelmärajapintojen avulla matkustaja voisi pystyä hyödyntämään kaukoliikenteessä yleistyneitä tarjoushintoja (dynaamista hinnoittelua), joilla on suuri vaikutus eri liikennevälinein matkaamiseen matkaketjun kokonaishintoja vertailtaessa.
- mahdollisuuden lisäarvopalveluihin, jotka liittyvät julkisella liikenteellä matkustamiseen (esim. majoitukset jne.).

Lippu- ja maksujärjestelmien yhteiskäyttöisyyden toteuttamiseksi on aloitettu eri toimijoita yhdistävän palvelualustan suunnittelu, jossa ovat mukana Waltti, HSL, Turun ja Tampereen kaupungit (jotka ovat myös Waltissa mukana), Pohjolan Liikenne ja Taksiliitto.

Tavoitteena on määritellä palvelu, jonka avulla eri toimijat voivat myydä myös muiden järjestelmään kuuluvien osapuolten lipputuotteita. Tavoitteena on tietynlainen avoimuus, jolloin myös muut kaupalliset toimijat voivat tuottaa matkustajien tarvitsemia lisäarvopalveluja palvelualustan avulla. Palvelualustan käyttöönottoa tavoitellaan jo vuosina 2016–2017.

7.2 MaaS-palvelut

MaaS-palveluiden (ks. Liite A) keskeisinä elementteinä ovat informaatiojärjestelmät, joiden avulla käyttäjät voivat suunnitella liikkumisensa, hoitaa kulkuneuvoihin liittyvät varaukset ja maksut sekä saada valtuutuksen (tai valtuutukset) matkareitillä käytettyihin kuljetusvälineisiin (esim. polkupyörä, bussi, vuokra-auto, taksi, juna) helppokäyttöisellä tavalla (esim. mobiililippuna) siten, että koko matkaketjusta tulee käyttäjän kannalta saumaton.

Käyttäjän näkökulmasta keskeinen informaatiopalveluelementti kehittyneissä MaaS-järjestelmissä on ns. multimodaalinen reitinsuunnittelujärjestelmä, joka optimoi eri liikkumistapojen käytön jonkin annettavan parametrin (aika, matka, kustannus) tai niiden yhdistelmien perusteella. Esimerkiksi UbiGo-palvelu sai kritiikkiä juuri siitä, ettei siinä oleva reitinsuunnittelujärjestelmä kyennyt vertailemaan eri liikkumistapojen välisiä kustannuseroja (Sochor ym. 2014).

[4] Nykyisissä matkakorttijärjestelmissä (HSL, Waltti) matkakortti ei myöskään suoraan identifioi käyttäjää ja kortti voi olla esim. henkilökohtainen tai haltijakohtainen. Käyttäjän ja kortin yhdistävää tietoa voidaan ylläpitää asiakkuuden hallintajärjestelmässä (CRM, Customer Relation Management).

Tällä hetkellä kattavat multimodaaliset matkansuunnittelujärjestelmät ovat vielä kehittelyn asteella ja niistä useimmat pystyvät optimoimaan liikkumista toistaiseksi vain yhden parametrin (yleensä ajan) perusteella. Esimerkkinä tällaisesta järjestelmästä voidaan käyttää Liikenneviraston ylläpitämää matka.fi-palvelua, jonka toiminta perustuu joukkoliikenteen koontitietokannan antamiin tietoihin. Matka.fi pystyy suosittelemaan ajallisesti sopivan matkaketjun julkista liikennettä hyödyntäen. HSL:ssä kehitteillä oleva Avoin Reittiopas tulee lähitulevaisuudessa parantamaan entisestään multimodaalisen reitinsuunnittelun mahdollisuuksia, sillä se ottaa huomioon hinnan ja matka-ajan lisäksi muita liikkumismahdollisuuksia ja tarjoaa esim. tiedot liityntäpysäköinnistä.

MaaS-palveluissa reitinsuunnittelun tulee kattaa kaikki liikkumisen muodot kävelystä yksityisautoiluun ja joukkoliikenteeseen, ja reitinsuunnittelusta on päästävä suoraan yksinkertaiseen maksamiseen ja liikkumisvaltuuksien (esim. matkalippujen ja vuokra-autojen avainkoodien) saamiseen. Reitinsuunnittelujärjestelmän on osattava huomioida reitin suunnittelussa oman auton käytön lisäksi taksipalvelut (esim. Uber-tyyliset, mahdolliset kimppakyydit jne.) uusina liikkumisen välineinä. Lisäksi tietojärjestelmän tulee ylläpitää tietoja käytetyistä liikkumisen muodoista, sillä matkan aikana kuluttajalle saattaa tulla matkaketjuun muutoksia, jotka joudutaan huomioimaan esimerkiksi laskutuksessa. Koska laskutustieto välttämättä tarvitaan, kerääntyy MaaS-operaattorille kattava tietokanta asiakkaidensa todellisesta liikkumisesta jollakin tarkkuudella. Tämä tarkkuus voi olla esim. matkaketjun aikana suoritetut liikkumistavan vaihtopisteet ja niihin mahdollisesti liittyvä pysäkkitieto tai koordinaattitieto.

Tällä hetkellä ollaan vielä muutaman askeleen päässä saumattomuudesta, kun jokaiseen kulkutapaan tarvitaan oma liputus- tai tunnistejärjestelmä. Kaupunkialueiden matkoissa sekä busseissa että junissa on käytössä yleensä NFC-tekniikkaan (Near Field Communication) perustuva matkakortti, VR:n kaukomatkaliikenteessä ja Finnairin lentoliikenteessä puolestaan visuaalinen 2D-viivakoodi (semacode) joko paperimuotoisena tai mobiilipäätelaitteen ruudulla luettavana tunnisteena. Tilanne ei näytä oleellisesti helpottuvan lähivuosinakaan, koska sekä pääkaupunkiseudun (HSL) että muun maan kattavaa (Waltti) liputusjärjestelmää ollaan juuri uusimassa ja tehtävät investoinnit tulevat palvelemaan joukkoliikennettä seuraavan vuosikymmenen ajan.

MaaS-operoinnissa voidaankin teknisten ratkaisujen perusteella nähdä ainakin kaksi erilaista versiota:

- matkaketjuun liittyvien käyttöoikeuksien välityspalvelu
- ”reaaliaikainen” MaaS-operointi.

Matkaketjuun liittyvien käyttöoikeuksien välityspalvelulla tarkoitetaan UbiGon kaltaista reitinsuunnittelu- ja liputusjärjestelmää, joka puolestaan on lähinnä laajennettu ”matkatili” kattaen myös taksikuljetukset, kimppakyydit, autojaot (car sharing), autonvuokrauksen jne. Käyttäjällä on siis kullakin hetkellä mahdollisuus tehdä valinta liikkumismuodostaan, ja hän itse huolehtii esim. tarvittaessa taksin tilaamisen nykyiseen tapaan omatoimisesti osana matkaketjua. MaaS-operaattori

huolehtii lähinnä siitä, että jokaiseen kulkuvälineeseen on olemassa käyttövaltuus ja että laskutus tapahtuu käytön mukaisesti ja rahaliikenteeseen liittyvät selvitykset (clearing) toimivat asianmukaisesti.

Kun MaaS-palveluiden personointia lähdetään kasvattamaan riittävän houkuttelevaksi auton omistamisen sijaan, tulisi palvelutason olla huomattavan lähellä omistusauton tai taksiliikenteen tarjoamaa palvelua (odotusajan lyhyys, matkareitin suoruus ja matkaan käytetty aika). Tämä taas edellyttää entistä reaaliaikaisempaa tietoa kuljetettavien sijainnista, jotta sopiva resurssi, esim. vuokra-auto tai kyytipalvelu, voidaan tarjota kyytiä kaipaavalle ajantasaisesti ja jotta kyetään reagoimaan käyttäjien reitinmuutoksiin ongelmatilanteissa. Tämänkaltainen reaaliaikainen MaaS-operointi lähestyy kalustonhallinnan ja logistiikan optimointijärjestelmiä, joissa ollaan resurssien hallinnan kannalta jatkuvasti tietoisia käytössä olevien kuljetusvälineiden sijainnista ja kuljetettavista kohteista – tässä tapauksessa rahdin sijasta henkilöistä. Toiminnallisesti tilanne muistuttaa Kutsuplus- ja Uber-palveluiden toimintatapaa, jossa järjestelmä on jatkuvasti tietoinen kulkuneuvojen sijainnista sekä käyttäjien kulkemasta reitistä, joista jää yksityiskohtainen jälki sijaintitietoineen järjestelmän tietokantaan.

7.3 Yksityisyyden huomiointi liikenteen ekosysteemimalleissa

Edellisissä alaluvuissa käsiteltiin erilaisten liikennepalveluekosysteemien muotoutumisen mahdollisia lähtökohtia. Yhteisenä piirteenä niistä jokaiselle on käyttäjiä koskevan liikkumistiedon kasautuminen tietovarastoihin keskitetysti. Käyttöoikeuksia ylläpitävien ”kansalaisen matkatilin” ja käyttöoikeuksia jakavan MaaS-operoinnin kaltaisessa järjestelmässä tietoturvaan liittyvät ongelmat ovat samantyyppiset kuin jo tämän hetkisissä joukkoliikennejärjestelmissä. Järjestelmät ylläpitävät lähinnä kulkutapojen vaihtoja (esim. juna, bussi, metro) koskevia reittipisteitä ja tuottavat siten harvoja liikkumismatriiseja (lähde- ja kohdepisteet). Toisaalta koska reittiliikenne tapahtuu nimensä mukaisesti ennakolta määriteltyjen reittien mukaan, matkustajan aika- ja paikkatiedosta voidaan tehdä tarvittaessa melko tarkka approksimaatio.

Sen sijaan muiden, ennakolta määritetyistä joukkoliikenteen reiteistä riippumattomien liikkumismuotojen, esim. taksinkäytön, kimppakyytien ja vuokra-autoilun, reittien seurannan osalta reaaliaikainen MaaS-operointi tuottaa hyvinkin tarkkaa tietoa, koska liikkumistiedon kerääminen on keskeistä järjestelmän toiminnan kannalta (resurssien allokointi, kilometriperustainen laskutus). Tässä suhteessa niiden yksityisyyden suojalle asettamat haasteet muistuttavat Uber- tai Kutsuplus-järjestelmien yksityisyyden suojaan liittyviä kysymyksiä. Kutsuplus-järjestelmässä reittitiedon yksityisyyteen liittyvää ongelmaa on pyritty ratkaisemaan tarjoamalla käyttäjälle mahdollisuus poistaa yksityisyyden kannalta haitalliseksi katsomansa jäljet.

Tässä käsitellyt liikennepalveluekosysteemien aihiot, ”matkatili” ja MaaS-operointi yleisesti, ovat yksityisyyden suojan osalta hieman paremmassa valinta-asemassa kuin käyttäjille ”ilmaisia informaatiopalveluita” tarjoavat järjestelmät. Googlen ja Applen laite- ja informaatiopalveluekosysteemien kaltaisissa kaksipuolisissa markkinoissa kuluttajapuolen ”ilmaiset” palvelut rahoitetaan toiselta osapuolelta (esim. mainostajat) käyttäjistä kerätyn ja jalostetun yksityisen tiedon myynnistä hankittuina tulovirtoina.

Matkatilin ja MaaS-operoinnin liiketoimintamallit eivät välttämättä edellytä vastaavaa ansaintalogiikkaa, koska ihmiset ovat tottuneet maksamaan liikkumispalveluista. Täten liiketoimintamallit voidaan rakentaa perinteisempiin eli varaus- ja maksutransaktioiden välittämiseen perustuviin tulovirtoihin. Tämä ei tietenkään poissulje sitä mahdollisuutta, ettei yksilöjä koskevia liikkumistietoja voitaisi luovuttaa esim. maksua vastaan kolmansille osapuolille joko sellaisenaan tai anonymisoituna. Todennäköisesti tämä ansaintamalli ei kuitenkaan ole lippujärjestelmä-operaattorin tai MaaS-operaattorin liiketoiminnan ensisijainen tulolähde.

Saattaa toki olla myös mahdollista, että uudet liiketoimintamallit mahdollistavat matkustamisen hinnoittelun sen perusteella, kuinka paljon käyttäjä on halukas luovuttamaan kulkemistaan reiteistä tietoa kolmansille osapuolille. Esimerkiksi MaaS-operoinnissa voitaisiin matkustamisen hinnoittelussa käyttää tietoa siitä, että matkustaja käyttää liikennepalveluita kuormitushuippujen ulkopuolella. Matkatilin (joukkoliikenteen) osalta tämä ei kuitenkaan ole todennäköistä, koska matkustaminen on jo muutenkin yhteiskunnan varoin tuettua.

Jotta MaaS-operoinnista ja matkatilistä voitaisiin puhua laajemman liikennepalveluiden ekosysteemin mahdollistajina, tulisi niiden keräämä käyttäjiä koskeva reittitieto saattaa kolmansien osapuolten käyttöön kiinnostavien lisäarvopalveluiden toteuttamiseksi. Nämä käyttäjien reittitietoon perustuvat palvelut voisivat olla joko personoituja tai ei-kohdennettuja, joista jälkimmäiset voisivat olla anonyymiin reittitietoon perustuvia.

Anonyymiin reittitietoon liittyvät lisäarvopalvelut voivat olla yleisesti hyödyllisiä, mutta palvelujen paremman kohdennettavuuden ja suuremman käyttöarvon luomiseksi tarvittaisiin lisätietoa käyttäjien tarpeista ja mieltymyksistä. Tähän ongelmaan voidaan vastata MyData-ajattelun mukaisella toimintaperiaatteella, jossa käyttäjä (eli reittitiedon haltija) voisi valtuuttaa kolmannen osapuolen yhdistämään hänen useista lähteistä koostetun intressiprofiilinsa (jota mahdollisesti MyData-operaattori ylläpitäisi) hänen reittiinsä ja tuottamaan sen perusteella esim. suosituksia reittiin liittyvistä lisäarvopalveluista. Näin mahdollistettaisiin liikkumispalveluekosysteemissä personoidut lisäarvopalvelut niille, jotka sellaisia kokevat tarvitsevansa. Ne kuluttajat puolestaan, jotka ovat hyvin tarkkoja liikkumisen yksityisyyden suojasta, voisivat sen edelleen säilyttää.

Toistaiseksi edellä kuvatun skenaarion esteenä ovat helposti siirrettävien ja automaattisesti käsiteltävien kuluttajien reittitiedon esitystapojen puuttuminen (ns. reittitiedon ”interchange format”), MyData-infrastruktuurin puuttuminen (MyData-operaattorit) ja varsinaisten MaaS- ja matkatilioperaattorien puuttuminen sekä teknisen infrastruktuurin kypsymättömyys. Kaikki elementit ovat kuitenkin kehittymässä, joten organisatorisella yhteistyöllä sekä laadukkaalla suunnittelulla ja to-

teutuksella on mahdollista synnyttää ekosysteemin muodostumista tukeva alusta, jonka käyttökelpoisuuden kuluttajapalveluiden tarjonta ja kysyntä viime kädessä mittaavat. Teknisesti toimintaa tukevan alustan komponenteilta edellytetään yhteentoimivuutta, joten tietojärjestelmien avoimet rajapinnat ja tietojen esitystapojen standardointipyrkimykset helpottavat toimivien kokonaisuuksien rakentamista.

7.4 Luottamus ja liikennepalvelut

Suomessa julkisiin liikennepalveluihin, kuten joukkoliikenteeseen ja taksijärjestelmään, liittyvä luottamus on ollut korkea. Julkisen liikenteen kohdalla luottamus kohdistuu lähinnä toimivuuteen ja ajantasaisuuteen ts. vuorot liikennöidään ajallaan ja matkustaminen koetaan turvalliseksi. EPSI Finlandin vuonna 2014 tuottaman julkisen liikenteen asiakastyytyväisyystutkimuksen mukaan (EPSI 2014) erityisen tyytyväisiä ollaan taksiliikenteeseen (yli 80 %:n tyytyväisyys), linja-autoliikenteen kaukovuoroihin (77 % tyytyväisiä) ja HSL:n toimintaan (75 % tyytyväisiä) ja ainoastaan tyytyväisyys junaliikenteeseen on keskiarvon (75 %) alapuolella – n. 70 % haastatelluista 1400 henkilöstä oli kuitenkin tyytyväinen VR:n palveluihin.

Julkinen liikenne on perinteisesti ollut säädelty toimiala, jossa viranomaiset määrittävät toimintaympäristön viitekehyksen ja valvovat sen toimintaa. Koska kansalaisilla on tutkimusten mukaan suhteellisen korkea luottamus yhteiskuntaa ja sen instituutiota kohtaan, syntyy tätä kautta luottamusta myös julkisen liikenteen toimijoihin. Liikennepalveluissa ollaan kuitenkin höllentämässä viranomaisperustaista ohjausta, ja monet aiemmin säädellyt toiminnot ovat jo vapautuneet kilpailulle tai niiden vapauttamista valmistellaan (ks. liite B).

Linja-autoliikenteen vapauttaminen vuonna 2009 ja sen käytännön vaikutukset, jotka näkyivät lähinnä vasta aivan viime vuosien aikana lähinnä kaukoliikenteen kilpailussa, eivät ole juurikaan muuttaneet asiakastyytyväisyyttä säätelyn ajan tasoon nähden. Jonkin verran tyytyväisyyden laskua on kuitenkin ollut havaittavissa vuonna 2014 (tyytyväisiä n. 77 %) vuoteen 2013 nähden (tyytyväisiä 80 %) (EPSI 2014). Erityisesti taksiliikennejärjestelmän uudistaminen on aiheuttanut paljon julkista keskustelua ja kannanottoja sääntelyn asteittaisesta purkamisesta. Pääsääntöisesti keskustelussa on tuotu esille pelkoina palvelutason huonontuminen syrjäseuduilla, turvallisuus ja hinnoittelun arvaamattomuus. Toinen vielä sääntelyn piirissä ja lähitulevaisuudessa vapaamman kilpailun piiriin tuleva liikennöinti on tavaraliikenne.

Tietoteknisten menetelmien avulla on mahdollista pyrkiä ylläpitämään ja kasvattamaan käyttäjien luottamusta sääntelystä vapaaseen taksi- ja tavaraliikennejärjestelmään. Tekniikan avulla voidaan vaikuttaa kuluttajien turvallisuuden tunteeseen, kyydin tai kuljetuksen hinnoitteluun sekä yhteiskunnan kannalta harmaan talouden kitkemiseen eli lähinnä epärehellisen taksitoiminnan estämiseen ja sen valvontaan tai tavaraliikenteen harjoittamisesta syntyneiden tulojen pimittämiseen. Esimerkkeinä näistä luottamusta lisäävistä mekanismeista voidaan käyttää sekä nykyistä taksamittarijärjestelmää että Uber- tai Lyft-palveluiden toteutuksia (GPS-

perustainen ajonseuranta älypuhelimella), joilla voidaan tarvittaessa seurata taksitoimintaa. Matkan tai kuljetuksen hinta voi selvitä asiakkaalle jo ennakkoon mobiilipalvelua käytettäessä, jos asiakas on halukas ilmoittamaan hakuosoitteensa lisäksi matkan kohdeosoitteen.

Kuluttajien kokemus taksipalveluiden laadusta voi jatkossa pysyä nykyisellä tasolla tai jopa parantua Uber/Lyft-tyylisten palveluiden kaksipuolisilla ranking-mekanismeilla – asiakas voi arvostella saamansa kyydin laadun ja kuljettaja puolestaan asiakkaan. Vastaavasti sääntelystä vapaassa tavaraliikenteessä olisi periaatteessa kenen tahansa mahdollisuus toimia tavarankuljettajana (Waris & Paloheimo 2015) ja kuljetuksen sujuvuuden laatua voitaisiin arvioida rating-järjestelmän avulla. Tässä yhteydessä on kuitenkin syytä ottaa huomioon arvostelu- (rating) ja mainejärjestelmiä koskevat ongelmat.

Taksijärjestelmä saattaa olla muutenkin suurten muutosten edessä lähivuosikymmeninä, jos autonominen ajaminen toteutuu. Koko taksiliikenteen luonne muuttuu radikaalisti nykyisestä työvoimavaltaisesta yrittämisestä entistä pääomavaltaisempaan ajoneuvokaluston hallintaan ja niillä suoritettavaan liikennöintiin. Toisaalta voi syntyä myös osa-aikataksinkuljettajien ammattikunta Yhdysvaltojen tyyliin, jossa esim. Uber PoP -palvelussa lähes kuka tahansa välityspalvelun seulan läpäisevä toimija voi tarjota kyytipalveluita. Vastaavasti tavaraliikennepalveluissa saattaa olla edessä vastaavankaltainen murros erityisesti pienten tavaroiden kuljetuksessa joukkoistamisen avulla. (Waris & Paloheimo 2015.)

Kyydin ja kuljetusten välityspalvelut (vrt. MaaS-operointi) toimivat kohtauspaikkana asiakkaan ja palveluntarjoajan välillä, jolloin niiden merkitys muodostuu jatkossa entistä keskeisemmäksi, kun yhä useammat kuluttajat siirtyvät älypuhelinten verkkopalveluiden käyttäjiksi. Kuten monessa muussakin tietotekniikkaan pohjautuvassa ratkaisuissa (ns. platform-economy), eräänä mahdollisuutena on välityspalvelun monopolisoituminen tai keskittyminen muutaman suuren kansainvälisen toimijan käsiin.

Kamppailu nykyisten välityspalveluiden (Uber vs. muut) välillä voidaan nähdä asetelmien hakemisena tulevaisuutta varten: mukana ovat esim. nykyiset välityspalvelut Uber ja Lyft ja toisaalta autonomista ajamista kehittävät tietotekniikkayritykset Google ja Apple. Jos viranomaisia (esim. verottajaa) huolettaa säätelyn vapauttamisen seurauksena syntyvä mahdollinen harmaa talous, välitysjärjestelmät olisivat keskeinen tietolähde todellisista tapahtuneista transaktioista. Luonnollisesti ns. pimeään taksi- tai kuljetustoimintaan edellä mainituilla menetelmillä tai välityspalveluiden tarkemmalla seurannalla ei ole vaikutusta sen enempää kuin nykyisellä säätelylläkään.

On kuitenkin vielä ennenaikaista arvioida, voisivatko esim. rating-järjestelmät toimia ainoana tavarankuljetusten tai esim. taksikuljettajien laatua ylläpitävänä mekanismina nykyisen koulutusvaatimuksen (taksikurssi) ja kokemuksen sijaan. Kaikkea taksiliikennettä voidaan tuskin viedä pelkästään luottamusjärjestelmien varaan, esim. subventoidut Kela-kyydityksen ja koululaiskyydit saattavat edelleen vaatia viranomaisten tarkempaa kontrollia. Tavaraliikenteessä tilanne on hieman helpompi siinä suhteessa, ettei kuljetuksissa ole suoranaisia henkilöturvallisuusriskejä. Tavaraliikenteen riskejä voidaankin pienentää vakuuttamalla kuljetettava

tavara, ja periaatteessa olisi mahdollista hinnoitella riski kuljetuskohtaisesti kuljettajan toimintahistorian (vrt. maine) ja tavaran arvon perusteella.

8. Johtopäätökset ja yhteenveto

Tässä tutkimuksessa on pyritty valottamaan paikkatietoon liittyviä, yksityisyyden suojaa ja luottamusta koskevia näkökohtia useista eri suunnista liikenteen sähköisten palvelujen alueella. Yritysten ja valtiollisten organisaatioiden lähtökohdista keskeinen kysymys kehitettäessä liikkumisen liiketoimintamalleja ja palveluita on se, missä määrin yksityisyyden suojaa kannattaa ottaa huomioon sijaintiin perustustuvissa liikkumispalveluissa.

Liiketoiminnan tavoitteiden (henkilötiedon hyödyntämisen) ja yksityisyyden suojan välillä näyttää olevan toistaiseksi selvät tavoite-erot. Käyttäjien yksityisyyden suojan vaatimukset ja heidän sijaintitiedolle antamansa yksityisyyden arvo ovat käytännössä olleet vaatimattomia, vaikka kasvavaa huolestuneisuutta tietojen mahdollisesta väärinkäytöstä onkin alkanut tutkimusten perusteella ilmetä. Koska selkeää käyttäjätarvetta ei kuitenkaan toistaiseksi ole ja yksityisyyden suojalla ei saavuteta kilpailuetua, on ilmeistä, ettei kuluttajamarkkinoilla toimivilla yrityksillä ole vielä merkittävää halua nykyisten menettelytapojen muuttamiseen tai uusien kehittämiseen.

Esimerkiksi Heikkilä ym. (2010) ovat todenneet, että liikenteen liiketoimintamallit kiinnittävät kyllä huomiota tarpeisiin, resursseihin, tarjontaan ja rahoitukseen, mutta jättävät huomioimatta luottamuksen ja yksityisyyden merkityksen. De Reuverin ja Haakerin haastattelututkimus (2009) kontekstitietoisten palveluiden liiketoimintaa harjoittavien yritysten keskuudessa osoittaa, että nämä toimijat näkevät luottamuksen erääksi tärkeimmäksi näkökulmaksi sijaintia hyödyntävien palveluiden suunnittelussa. Alalla toimivien yritysten asiantuntijat myös painottavat erityisesti käyttäjien mahdollisuutta oman yksityisyytensä tason määrittämiseen. Täten liiketoimintamalleja suunniteltaessa luottamus ja yksityisyys tulisi ottaa jo hyvin varhaisessa vaiheessa mukaan joko liikkumisen palveluiden arvonmuodostuksen määrittelyssä tai liiketoimintaprosesseja luotaessa.

Liikennepalveluiden yksityisyyden suojan kehittämiseksi olisi mahdollista määritellä kansallisesti esim. oma PIA-viitekehys, joka kuvaisi prosessin yksityiskohdat ja tarjoaisi alan toimijoille systemaattisen tavan ottaa yksityisyys ja luottamus huomioon jo liiketoimintasuunnitelmia ja palveluita hahmoteltaessa. Lähtökohtana voisi toimia esim. yhdistelmä brittien ja kanadalaisten prosesseista, ja sen kehittämisessä voitaisiin hyödyntää Kanadassa (Alberta 2001) ja Britanniassa (ICO

2009) käytettyjä kysymyslistoja, joita täydennettäisiin Uudessa-Seelannissa luodulla ohjeistolla (Shroff 2007).

Tietosuojalainsäädännön uudistus on muutos nykytilanteeseen verrattuna. Loppukäyttäjän asema ja valta itseään koskeviin tietoihin lisääntyy, mutta sen voi nähdä myös kasvavana vastuuna omien tietojen käytön valvonnasta. Toisaalta palveluntarjoajan asema selkiytyy. Kuluttajan näkökulmasta on otettava huomioon:

- Omien tietojen hallinta – vastuu omien tietojen käsittelystä kasvaa, ja jokainen päätös sallia tietojen käsittely on punnittava tarkoin. Tärkeää on, että kuluttajat saavat riittävästi tietoja ja ohjeita omien tietojensa käsittelyn seurantaan.
- Yksityisten palvelujen osalta kuluttajalla on mahdollisuus valita, käyttääkö palvelua vai ei. Viranomaispalveluiden tai rekistereiden osalta tällaista valinnanvapautta ei yleensä ole.

EU:n tietosuojalainsäädännön kiristäminen tuskin tulee Suomessa aiheuttamaan merkittäviä muutoksia yritysten nykyisiin mahdollisuuksiin hyödyntää henkilötietoja niiden edelleen myynnissä tai analysoinnissa. Tietojen myyntiä tehdään jo tällä hetkellä esim. Trafin ja Väestörekisterikeskuksen toimesta suoramarkkinoinnin tarpeisiin. Kuluttajat eivät yleensä voi vaikuttaa rekisteröintiin ja heitä koskevien tietojen keruuseen. Vaikka periaatteessa jokaisella henkilöllä on oikeus kieltää tietojensa luovuttaminen, harvat siihen vaivautuvat tai edes ovat tietoisia kyseisestä mahdollisuudesta. Yksityisyyden suojan kannalta voisi olla mielekästä tarkastella, onko tarvetta estää oletusarvoisesti esim. viranomaisten keräämän ja ylläpitämän tiedon levittäminen muita kuin viranomaisten välttämättömiä tarpeita varten.

Suuntaa yksityisen tiedon hallintaan tulevaisuuden palveluissa antaa miDatan/MyDatan kaltainen läpinäkyvyyden lisäämiseen perustuva lähestymistapa (PIMS/MyData-operointi). Tässä periaatteessa käyttäjillä on aiempaa suurempi kontrolli ja helpompi pääsy itseään koskevaan tietoon. Yritysten keräämän henkilötiedon avoimempi keskinäinen vaihto, käyttäjien antaessa siihen valtuutuksen ja sitä itse kontrolloidessa, mahdollistaa tiedon entistä monipuolisemman käytön ja uusien innovatiivisten palveluiden synnyttämisen. Yritysten intensiivinä tiedon luovuttamiselle voisi toimia se, että yritykset saavat vastavuoroisesti käyttöönsä sellaista hyödyllistä henkilöön liittyvää tietoa, jota ne eivät itse kykene muodostamaan.

Toimivat ja ilman jatkuvaa laillisuusperiaatteiden noudattamisen rajankäyntiä vaativat henkilötiedon markkinat (esim. liikkumistieto) olisivat niin yritysten kuin kuluttajienkin etu. Esimerkiksi liikkumistiedosta tuotetun liikkumisprofiilin antaminen käyttäjän suostumuksella palveluntarjoajien käyttöön helpottaisi palvelutarjonnan kohdentamista. Tällaisten markkinoiden syntyminen saattaa olla kuitenkin epävarmaa sääntelyn jatkuvasti kiristyessä. Ahdas lainsäädännöllinen tulkinta saattaisi näin heikentää eurooppalaisten palveluntarjoajien kilpailumahdollisuuksia väljemmillä säännöillä toimiviin globaaleihin – lähinnä yhdysvaltalaisiin – toimijoihin nähden.

On arvioitu, että liikkujien käyttäytymisen analysointiin perustuvien, paikkatietoa hyödyntävien palveluiden kokonaismarkkinoiden liikevaihto oli 2014 n. 8 miljardia dollaria ja että se kasvaa vuoteen 2019 mennessä n. 40 miljardiin dollariin. Kyse on siis taloudellisesti hyvin merkittävästä asiasta. Näistä vuosittain 25 %:n vauhdilla kasvavista markkinoista myös suomalaisten palveluntarjoajien on hyvä saada oma osansa, etenkin kun uhkana on edelleen, että palveluiden tarjoaminen keskittyy globaalien toimijoiden käsiin kotimarkkinoillakin (vrt. case Uber).

Lähteet

Aaker D., 1991. Managing Brand Equity. Capitalizing on the Value of a Brand Name. Free Press: New York.

Acquisti A. & Grossklags J., 2007. What Can Behavioral Economics Teach Us About Privacy? [verkkodokumentti] Saatavissa: http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf. [Viitattu 19.10.2015]

Acquisti A., Friedman A. & Telang R., 2008. Is There A Cost To Privacy Breaches? An Event Study. [verkkodokumentti] Saatavilla: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf. [Viitattu 20.10.2015]

Afroz S., Islam A., Santell J., Chapin A. & Greenstadt R., 2013. How Privacy Flaws Affect Consumer Perception. 2013 Third Workshop on Socio-Technical Aspects in Security and Trust (STAST). 29–29 June 2013. Pp. 10–17. [verkkodokumentti] Saatavilla: https://www.eecs.berkeley.edu/~sa499/papers/stast-privacy.pdf. [Viitattu 20.10.2015]

Akerlof G., 1970. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics, Vol. 84, Issue 3 (Aug., 1970), pp. 488–500. [verkkodokumentti] Saatavilla: http://staff.bath.ac.uk/ecsjgs/Teaching/Advanced%20Microeconomics/Articles/akerlof.PDF. [viitattu 22.10.2015]

Alberta, 2001. Privacy Impact Assessment: Instructions and Annotated Questionnaire Office of the Information and Privacy Commissioner Alberta, Canada. Version 1.1.2001. [verkkodokumentti] Saatavilla: http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf. [Viitattu 21.10.2015]

Alnemr R. & Meinel C., 2011. Why Rating is not Enough: A Study on Online Reputation Systems. 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). 15–18 Oct. 2011. Pp. 415–421. [verkkodokumentti] Saatavilla: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6144828 [Viitattu 22.10.2015]

Apple Inc., 2011. Apple Q&A on Location Data. Apple Press Info, April 27, 2011. [verkkodokumentti] Saatavilla: https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html [Viitattu 23.10.2015]

Aral S., 2014. The Problem With Online Ratings. MIT Sloan Management Review. Winter 2014. Saatavilla: http://sloanreview.mit.edu/article/the-problem-with-online-ratings-2/. [Viitattu 22.10.2015]

Aretun Å. & Nordbakke S., 2014. Developments in driver's licence holding among young people. Potential explanations, implications and trends. VTI rapport 824A. [verkkodokumentti] Saatavilla: https://www.vti.se/en/publications/pdf/developments-in-drivers-licence-holding-among-young-people-potential-explanations-implications-and-trends.pdf. [Viitattu 22.10.2015]

Aula, 2014. Kansalaistutkimus – Käyttäjien tarpeet liikkumisessa. Aula Research Oy. Tulosesitys 22.5.2014, Tekes. 56 s. [verkkodokumentti] Saatavilla: https://www.tekes.fi/contentassets/3697b5c6bfed4ef18f9f61cca0f11745/kansalaistutkimus---kayttajien-tarpeet-liikkumisessa.pdf. [Viitattu 22.10.2015]

Balakrishnan M., Mohomed I. & Ramasubramanian V., 2009. Where's that phone?: geolocating IP addresses on 3G networks. IMC '09 Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, pp. 294–300. [verkkodokumentti] Saatavissa: https://www.net.t-labs.tu-berlin.de/teaching/ss10/IM_seminar/pdf/p294-balakrishnan.pdf. [Viitattu 19.10.2015]

Bamberger W., 2010. Interpersonal Trust – Attempt of Defination. Technische Universität München. [verkkodokumentti] Saatavilla: http://www.ldv.ei.tum.de/en/research/fidens/interpersonal-trust/[Viitattu 20.10.2015]

Baum K., Catalano S. & Rand M., 2009. Bureau of Justice Statistics. Stalking Victimization in the United States – Bureau of Justice Statistics Special Report, January 2009, NCJ 224527. [verkkodokumentti] Saatavilla: http://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0 [Viitattu 23.10.2015]

Beresford A. & Stajano F., 2004. Mix Zones: User Privacy in Location-aware Services. [verkkodokumentti] Saatavilla: https://www.cl.cam.ac.uk/~fms27/papers/2004-BeresfordSta-mix.pdf. [Viitattu 20.10.2015]

Biler S., Šenk P. & Winklerová L., 2013. Willingness of Individuals to Participate in a Travel Behaviour Survey using GPS devices. Paper presented at the conference on New Techniques and Technologies for Statistics, Brussels, March 2013. [verkkodokumentti] Saatavilla: http://www.cros-portal.eu/sites/default/files/NTTS2013fullPaper_234.pdf.[Viitattu 19.10.2015].

BIS, 2011. Department for Business and Innovation Skills, UK Cabinet Office. Better Choices: Better Deals – Consumer Powering Growth. April 2011. 51 p. [verkkodokumentti] Saatavilla: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/294798/bis-11-749-better-choices-better-deals-consumers-powering-growth.pdf. [Viitattu 20.10.2015].

Björklund K., 2010. Stalking and violence victimization among Finnish university students. [verkkodokumentti] Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/19721/stalking.pdf?sequence=2 [viitattu 19.10.2015]

Bluetooth, 2015. Skyrocketing demand for Bluetooth appcessories for latest phones. [verkkosivusto] http://www.bluetooth.com/Pages/Mobile-Telephony-Market.aspx [Viitattu 19.10.2015]

Blumberg A. & Eckersley P., 2009. On Locational Privacy, and How to Avoid Losing it Forever. August 3, 2009. [verkkodokumentti] Saatavilla: https://www.eff.org/wp/locational-privacy.[Viitattu 19.10.2015]

Brown B., Court D. & McGuire T., 2014. Views from the front lines of the data-analytics revolution. McKinsey Quarterly Insights & Publications, March 2014. [verkkodokumentti] Saatavilla: http://www.mckinsey.com/insights/business_technology/views_from_the_front_lines_of_the_data_analytics_revolution. [Viitattu 19.10.2015].

Brush B., Krumm J. & Scott J., 2010. Exploring End User Preferences for Location Obfuscation, Location-Based Service, and the Value of Location. UbiComp 2010, September 26–29, 2010. Copenhagen, Denmark. [verkkodokumentti] Saatavilla: http://www.msr-waypoint.net/en-us/um/people/jckrumm/Publications%202010/ubicomp243-brush.pdf. [Viitattu 20.10.2015]

Buttyan L., Holczer T. & Vajda I., 2007. On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs. Kirjassa: Stajano F. et al. (toim.): ESAS 2007, LNCS 4572. Pp. 129–141. [verkkodokumentti] Saatavilla: https://ftp.crysys.hu/publications/files/ButtyanHV07esas.pdf.[Viitattu 20.10.2015]

Bäckström J., Kanerva O., Lähesmaa J. & Telaranta J., 2012. Joukkoliikenteen tietojärjestelmät. Liikennevirasto. Esiselvitys. Liikenneviraston tutkimuksia ja selvityksiä. [Verkkojulkaisu]. Saatavilla: http://www2.liikennevirasto.fi/julkaisut/pdf3/lts_2012-32_joukkoliikenteen_tietojarjestelmat_web.pdf [Viitattu 21.10.2015]

Casare S. & Sichman J., 2005. Towards a Functional Ontology of Reputation. AAMAS'05. July 25–29, 2005, Utrecht, Netherlands. [verkkodokumentti] Saatavilla: http://www.sce.carleton.ca/faculty/esfandiari/agents/papers/casare-aamas05.pdf. [Viitattu 22.10.2015]

Catalano S., 2012. Stalking Victims in the United States – Revised. Page U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics BJS Special Report, September 2012, NCJ 224527. [verkkodokumentti] Saatavilla: http://www.bjs.gov/content/pub/pdf/svus_rev.pdf. [Viitattu 19.10.2015]

Cavoukian A., 2009. "Privacy by Desing" – The answer to Overcoming Negative Externalies Arising from Poor Management of Personal Data. True Economics WorkShop, London, England June 23, 2009. [verkkodokumentti] Saatavilla: https://www.ipc.on.ca/images/Resources/2009-06-23-TrustEconomics.pdf. [Viitattu 20.10.2015]

Chang E., Hussain K. & Dillon T., 2005. Reputation Ontology for Reputation Systems. Kirjassa: Meersman R., Tari Z. & Herrero P. (toim.) On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops Volume 3762 of the series Lecture Notes in Computer Science. Pp. 957–966. [verkkodokumentti] Saatavilla: http://link.springer.com/content/pdf/10.1007%2F11575863_117.pdf [Viitattu 22.10.2105]

Chin E., Porter Felt A., Sekary V. & Wagner D., 2012. Measuring User Confidence in Smartphone Security and Privacy. Symposium on Usable Privacy and Security (SOUPS) 2012. July 11–13, 2012, Washington, DC, USA. [verkkodokumentti] Saatavissa: https://cups.cs.cmu.edu/soups/2012/proceedings/a1_Chin.pdf.[Viitattu 19.10.2015].

CJEU, 2015. Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner. Press and Information Court of Justice of the European Union Press Release No 117/15, Luxembourg, 6 October 2015. [verkkodokumentti] Saatavilla: http://curia.europa.eu/jcms/jcms/P_180250/.[Viitattu 20.10.2015]

CtrlShift, 2014. 'MYDATA' What do the Government's 'mydata' proposals mean for organisations? A Ctrl-Shift Briefing Paper. [verkkodokumentti] Saatavissa: http://www.theidm.com/resources/insights/what-do-the-uk-governments-mydata-proposals-mean-for-organisations/ [Viitattu 20.10.2015]

Cohen J., 2013. What Privacy Is For. (November 5, 2012). Harvard Law Review, Vol. 126. [verkkodokumentti] Saatavilla: http://www.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf. [Viitattu 19.01.2015]

Connoly C., 2008. The US Safe Harbor – Fact or Fiction? [verkkodokumentti] Saatavilla: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf. [Viitattu 20.10.2015]

CTIA, 2013. Best Practices and Guidelines for Location Based Services. Version 2.0. Effective Date: March 23, 2010. [verkkodokumentti] Saatavilla: http://www.ctia.org/docs/default-source/default-document-library/pdf-version.pdf?sfvrsn=0 [Viitattu 20.10.2015]

CVIS, 2007. Cooperative Vehicle-Infrastructure Systems. [verkkosivusto] Saatavilla: http://www.cvisproject.org/ [Viitattu 23.10.2015]

Cvrcek D., Kumpost M., Matyas V. & Danezis G., 2006. A Study on the Value of Location Privacy. WPES'06, October 30, 2006, Alexandria, Virginia, USA. [verkkodokumentti] Saatavissa: http://www.fi.muni.cz/usr/matyas/PriceOfLocationPrivacy_proceedings.pdf. [Viitattu 19.10.2015]

Danezis G., Lewis S. & Anderson R., 2005. How Much is Location Privacy Worth? [verkkodokumentti] Saatavissa: http://infosecon.net/workshop/pdf/location-privacy.pdf. [Viitattu 19.10.2015].

De Reuver M. & Haaker T., 2009. Designing viable business models for context-aware mobile services. Telematics and Informatics, Vol. 26 Issue 3, August, pp. 240–248. [verkkodokumentti] Saatavilla: http://webuser.hs-furtwangen.de/~heindl/ebte-2012ss/context%20aware%20mobile%20services.pdf. [Viitattu 22.10.2015]

Delbosc A. & Currie G., 2013. Causes of youth licensing decline: a synthesis of evidence. Transport Reviews 33, No. 3, pp. 271–290. [verkkodokumentti] Saatavilla: http://www.tandfonline.com/doi/abs/10.1080/01441647.2013.801929#aHR0cDovL3d3dy50YW5kZm9ubGluZS5jb20vZG9pL3BkZi8xMC4xMDgwLzAxNDQxNjQ3LjIwMTMuODAxOTI5QEBAMA== [viitattu 22.10.2015]

Dellarocas C., 2005. Reputation Mechanisms. [verkkodokumentti] Saatavilla: http://www.mv.helsinki.fi/home/aula/Top20/dellarocas-reputation-mechanisms.pdf. [Viitattu 22.10.2015]

Dellarocas C., 2010. Online Reputation Systems: How to Design One That Does What You Need. MIT Sloan Management Review. Magazine: Spring 2010, Vol. 51. No. 3. [verkkodokumentti] Saatavilla: http://sloanreview.mit.edu/article/online-reputation-systems-how-to-design-one-that-does-what-you-need/ [Viitattu 22.10.2015]

Dickinson B., 2011. Infographic: 80% of robbers check Twitter, Facebook, Google Street View. ZDNet November 1, 2011. [verkkodokumentti] Saatavilla: http://www.zdnet.com/article/infographic-80-of-robbers-check-twitter-facebook-google-street-view/ [Viitattu 19.10.2015]

Duckham M., 2010. Moving forward: Location privacy and location awareness. [verkkodokumentti] Saatavilla: http://www.geosensor.net/papers/duckham10.SPRINGL.pdf. [Viitattu 23.10.2015]

Duckham M. & Kulik L., 2006. Location privacy and location-aware computing. [verkkodokumentti] Saatavilla: http://www.geosensor.net/papers/duckham06.IGIS.pdf. [viitattu 19.10.2015]

Dutton W. & Shepherd A., 2006. Trust in the Internet as an experience technology. Information, Communication & Society, 9:4, pp. 433–451. [verkkodokumentti] Saatavilla: http://www.tandfonline.com/doi/abs/10.1080/13691180600858606#aHR0cDovL3d3dy50YW5kZm9ubGluZS5jb20vZG9pL3BkZi8xMC4xMDgwLzEzNjkxMTgwNjAwODU4NjA2QEBAMA== [Viitattu 20.10.2013]

Eagle N. & Pentland A., 2009. Eigenbehaviors: identifying structure in routine. Behavioral Ecology and Sociobiology, May 2009, Vol. 63, Issue 7, pp. 1057–1066. [verkkodokumentti] Saatavilla: http://dspace.mit.edu/openaccess-disseminate/1721.1/49446. [Viitattu 20.10.2015]

eCo-FEV, 2014. eCO-FEV – combining infrastructures for efficient electric mobility. [verkkosivusto] Saatavilla: http://www.eco-fev.eu/ [Viitattu 20.10.2015]

Eisses S., de Jonge W. & and Habers V., 2006. Privacy And Distance Based Charging For All Vehicles On All Roads. ITS London 2006. [verkkodokumentti] Saatavilla: http://www.tipsystems.nl/files/Privacy_and_RUC_ITSLondon-doc.pdf [Viitattu 21.10.2015]

Eisses S., van de Ven T. & Fievée A., 2012. ITS & Personal Data Protection Final Report. ITS Action Plan Framework Contract Tren/G4/FV-2008/475/01. Amsterdam, October 4th, 2012 [verkkodokumentti] Saatavilla:

http://ec.europa.eu/transport/themes/its/studies/doc/2012-its-and-_personal-data-protection_-_final_report.pdf. [Viitattu 21.10.2105]

EPSI, 2014. Tutkimus suomalaisten tyytyväisyydestä julkisiin liikennemuotoihin: junaliikenne saa nuhteita. [verkkotietote] Saatavilla: http://www.epressi.com/tiedotteet/vapaa-aika/tutkimus-suomalaisten-tyytyvaisyydesta-julkisiin-liikennemuotoihin-junaliikenne-saa-nuhteita.html. [Viitattu 22.10.2015]

EU, 1950. European Convention on Human Rights. [verkkodokumentti] Saatavilla: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention_ENG.pdf. [Viitattu 20.10.2015]

EU, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [verkkodokumentti] Saatavilla: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [Viitattu 20.10.2015]

EU, 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). [verkkodokumentti] Saatavilla: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML [Viitattu 20.10.2015]

EU, 2007. Euroopan parlamentin ja neuvoston Asetus (Ey) N:O 1370/2007, annettu 23 päivänä lokakuuta 2007, rautateiden ja maanteiden julkisista henkilöliikennepalveluista sekä neuvoston asetusten (ETY) N:o 1191/69 ja (ETY) N:o 1107/70 kumoamisesta. [verkkodokumentti] Saatavilla: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:315:0001:0013:FI:PDF. [Viitattu 22.10.2015]

EU, 2009a. Euroopan parlamentin ja neuvoston Asetus (Ey) N:o 1071/2009, annettu 21 päivänä lokakuuta 2009, maantieliikenteen harjoittajan ammatin harjoittamisen edellytyksiä koskevista yhteisistä säännöistä ja neuvoston direktiivin 96/26/EY kumoamisesta. [verkkodokumentti] Saatavilla: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:300:0051:0071:FI:PDF. [Viitattu 22.10.2015]

EU, 2009b. Euroopan parlamentin ja neuvoston Asetus (EY) N:O 1072/2009, annettu 21 päivänä lokakuuta 2009, maanteiden kansainvälisen tavaralii-

kenteen markkinoille pääsyä koskevista yhteisistä säännöistä [verkkodokumentti] Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32009R1072&from=FI [Viitattu 22.10.2015]

EU, 2010. Directive 2010/40/Eu Of The European Parliament And Of The Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. [verkkodokumentti] Saatavilla: http://www.eltis.org/sites/eltis/files/celex-32010l0040-en-txt.pdf. [Viitattu 20.10.2015]

EU, 2012. Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). [verkkodokumentti] Saatavilla: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. [Viitattu 20.10.2015]

Finlex, 2006. Laki kaupallisista tavarankuljetuksista tiellä. 21.7.2006/693. [verkkodokumentti] Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2006/20060693 [Viitattu: 22.10.2015]

Finnberg H., 2014. Matkatili-palvelualusta kuluttajan kannalta. Liikennelabra 23.10.2014. [verkkojulkaisu] Saatavilla: http://liikennelabra.fi/wp/wp-content/uploads/2014/10/Matkatili-kuluttajan-kannalta-Helge-Finnberg.pdf. [viitattu 21.10.2015]

Fisher D., Dorner L. & Wagner D., 2012. Short Paper: Location Privacy: User Behavior in the Field. SPSM'12, October 19, 2012, Raleigh, North Carolina, USA. [verkkodokumentti] Saatavissa: https://www.cs.berkeley.edu/~daw/papers/location-spsm12.pdf. [Viitattu 19.10.2015].

FPF, 2012. Future Privacy Forum. June 2012 FPF Mobile Apps Study. [verkkodokumentti] Saatavilla: http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf [Viitattu 20.10.2015]

Franken A., 2014. The Location Privacy Protection Act of 2014 – summary. [verkkodokumentti] Saatavilla: http://www.franken.senate.gov/files/documents/140327Locationprivacy.pdf [Viitattu 20.10.2015]

Freudiger J., Maxim Raya M. & Félegyházi M., 2007. Mix-Zones for Location Privacy in Vehicular Networks. WiN-ITS 2007 Vancouver, British Columbia,

Canada [verkkodokumentti] Saatavilla: https://www.crysys.hu/~mfelegyhazi/publications/FreudigerRFPH07winITS.pdf. [Viitattu 20.10.2015]

Fritsch L., 2007. State of the art of Privacy-enhancing Technology (PET). Deliverable D2.1 of the PETweb project, Report no 1013, 22-Nov-2007. [verkkodokumentti] Saatavilla: http://publications.nr.no/PETweb_D2-1_StateoftheArt_PET_Report.pdf. [Viitattu 20.10.2015]

Gangewere W., 2013. Assessing the Impact of a Privacy Breach on a Firm's Market Value. [verkkodokumentti] Saatavilla: http://www.antolin-davies.com/theses/gangewere.pdf. [Viitattu 20.10.2015]

Gani D., 2015. Amazon sues 1,000 'fake reviewers'. The Guardian, Sunday 18 October 2015. [verkkodokumentti] Saatavilla: http://www.theguardian.com/technology/2015/oct/18/amazon-sues-1000-fake-reviewers [Viitattu 23.10.2015]

GAO, 2013. In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers. GAO-14-81: Published: Dec 6, 2013. [verkkodokumentti] Saatavilla: http://www.gao.gov/assets/660/659509.pdf [Viitattu 19.10.2015]

Gatzlaff K. & McCullough K., 2010. The Effect Of Data Breaches On Shareholder. Wealth Risk Management and Insurance Review, 2010. Vol. 13, No. 1, pp. 61–83. [verkkodokumentti] Saatavilla: http://onlinelibrary.wiley.com/doi/10.1111/j.1540-6296.2010.01178.x/epdf [Viitattu 20.10.2015]

Goldfarb A. & Tucker C., 2011a. Privacy Regulation and Online Advertising. Management Science, Vol. 57, No. 1, January 2011, pp. 57–71. [verkkodokumentti] Saatavilla: http://dx.doi.org/10.2139/ssrn.1600259. [Viitattu 19.10.2015]

Goldfarb A. & Tucker C., 2011b. Privacy and Innovation. NBER Working paper 17124. National Bureau of Economic Research, June 2011. 31 p. [verkkodokumentti] Saatavilla: http://www.nber.org/papers/w17124 [Viitattu 19.10.2015]

González M., Hidalgo C. & Barabási A., 2008. l Understanding individual human mobility patterns. Nature 453, 779–782 (5 June 2008). [verkkodokumentti] Saatavilla: http://www.nature.com/nature/journal/v453/n7196/pdf/nature06958.pdf [Viitattu 20.10.2015]

GovUK, 2013. Department for Business, Innovation & Skills and The Rt Hon Edward Davey MP. The midata vision of consumer empowerment. [verkkodokumentti] Saatavissa: https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment [Viitattu 20.10.2015].

Gurses S., Troncoso C. & Diaz C., 2011. Engineering Privacy by Design. [verkkodokumentti] Saatavilla: https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf. [Viitattu 20.10.2015]

Harrell E., 2015. Victims of Identity Theft, 2014. Bureau of Justice Statistics. [verkkodokumentti] Saatavilla: http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5410 [Viitattu 19.10.2015]

Heikkilä J., Heikkilä M., Xu X. & Makkula J., 2010. Business Modelling of Ubiservices: Concerns of privacy and trust in the context of co-operative traffic. [verkkodokumentti] Saatavilla: http://eberea.org/sites/all/files/users/Marikka/page/2011/02/business_modelling_of_ubiservices_pdf_21771.pdf. [Viitattu 22.10.2015]

Heikkilä S., 2014. Mobility as a Service – A Proposal for Action for the Public Administration, Case Helsinki. [verkkodokumentti] Saatavilla: https://aaltodoc.aalto.fi/bitstream/handle/123456789/13133/master_Heikkil%c3%a4_Sonja_2014.pdf?sequence=1&isAllowed=y [Viitattu 20.1.2016]

Holvast J., 2009. History of Privacy. The Future of Identity in the Information Society. Volume 298 of the series IFIP Advances in Information and Communication Technology, pp. 13–42. [verkkodokumentti] Saatavilla: http://link.springer.com/chapter/10.1007%2F978-3-642-03315-5_2 [Viitattu 19.10.2015]

Hu N., Pavlou P. & Zhang J., 2009. Overcoming the J-Shaped Distribution of Product Reviews. Communications of the ACM, October 2009, Vol. 52, No. 10. [verkkodokumentti] Saatavilla: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369332 [Viitattu 22.10.2015]

Iansiti M. & Levien R., 2004. Strategy as Ecology. Harvard Business Review, March 2004 Issue. [verkkodokumentti] Saatavilla: https://hbr.org/2004/03/strategy-as-ecology/ar/1 [Viitattu 21.10.2015]

ICO, 2009. ICO Privacy Impact Assessment Handbook (2009). Information Commissioner' Office (ICO). [verkkodokumentti] Saatavilla: http://www.adls.ac.uk/wp-content/uploads/2011/08/PIA-handbook.pdf. [Viitattu 21.10.2015]

Innamaa, S., Malin, F. & Rämä, P., 2015. Kilometriveron vaikutukset liikkumiseen. VTT Technology 227. VTT, Espoo. 62 s. + liitt. 45 s. ISBN 978-951-38-8321-8. http://www.vtt.fi/inf/pdf/technology/2015/T227.pdf

ITSinternational, 2011. Dutch survey shows drivers are in favour of road user charging. ITS International March April 2011. [verkkodokumentti] Saatavilla: http://www.itsinternational.com/categories/charging-tolling/features/dutch-survey-shows-drivers-are-in-favour-of-road-user-charging/ [Viitattu 21.10.2015]

Jøsang A., Ismail R. & Boyd C., 2007. A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems, 43(2) 2007, pp. 618–644. [verkkodokumentti] Saatavilla: https://www.oasis-open.org/committees/download.php/28303/JIB2007-DSS-Survey.pdf. [Viitattu 22.12.2015]

Kelly M., 2012. 96 percent of Google's revenue is advertising, who buys it? (infographic). Venture Beat, January 29, 2012. [verkkodokumentti] Saatavilla: http://venturebeat.com/2012/01/29/google-advertising/ [Viitattu 19.10.2015]

Kelsey B., 2011. New Survey: Burglars Use Social Media to Plan Crimes. [verkkodokumentti] Saatavilla: http://socialtimes.com/new-survery-burglars-use-social-media-to-plan-crimes_b79475 [Viitattu 20.10.2015]

Kido H., Yanagisawa Y. & Satoh T., 2005. Protection of Location Privacy using Dummies for Location-based Services. Data Engineering Workshops, 2005. 21st International Conference on. [verkkodokumentti] Saatavilla: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1647865 [Viitattu 20.10.2015]

KKV, 2014. Aloite taksiliikennelain muuttamiseksi, 14.4.2014. [verkkodokumentti] Saatavilla: http://www.kkv.fi/ratkaisut-ja-julkaisut/aloitteet-lausunnot-ja-kannanotot/2014/14.4.2014-kkvn-aloite-aloite-taksiliikennelain-muuttamiseksi/ [Viitattu 22.10.2015].

Kouvo A., 2014. Luottamuksen lähteet – Vertaileva tutkimus yleistynyttä luottamusta synnyttävistä mekanismeista. Akateeminen väitöskirja, Turku 2014. [verkkodokumentti] Saatavilla: http://doria32-kk.lib.helsinki.fi/bitstream/handle/10024/96378/AnnalesC381Kouvo.pdf?sequence=2. [Viitattu 22.10.2015]

Kovalainen A. & Österberg J., 2000. Sosiaalinen pääoma, luottamus ja julkisen sektorin restrukturaatio. Kirjassa: Ilmonen, K. (toim.) Sosiaalinen pääoma ja luottamus. Jyväskylä, Jyväskylän yliopisto, SoPhi 2000.

Krumm J., 2008. A Survey of Computational Location Privacy, Personal and Ubiquitous Computing. [verkkodokumentti] Saatavissa: http://research.microsoft.com/en-us/um/people/jckrumm/Publications%202008/computational%20location%20privacy%20preprint.pdf. [Viitattu 19.10.2015]

Kumaraguru P. & Cranor L., 2005 Privacy Indexes: A Survey of Westin's Studies. ISRI Technical Report (2005). 22 p. [verkkodokumentti] Saatavilla: http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf. [Viitattu 22.10.2015]

Kutsuplus, 2015. Kutsuplus [verkkosivusto] Saatavilla: https://kutsuplus.fi/home [Viitattu 21.10.2015]

Langheirich M., 2009. Privacy In Ubiquitous Computing. John Krumm (ed.): "Ubiquitous Computing". Chapman & Hall / CRC Press, Sep. 2009. ISBN: 9781420093605 [verkkodokumentti] Saatavilla: http://www.ee.oulu.fi/~vassilis/courses/ubicomp10S/papers/privacy_security/langheinrich-09.pdf. [Viitattu 19.10.2015]

Liu L., 2009. Privacy and Location Anonymization in Location-based Services. SIGSPATIAL Special, Vol. 1 Issue 2, July 2009, pp. 15–22. [verkkodokumentti] Saatavilla: http://dl.acm.org/ft_gateway.cfm?id=1567257&type=pdf&CFID=72271370 8&CFTOKEN=69107582 [Viitattu 20.10.2015]

LiVi, 2013. Julkisen liikenteen sanasto. Liikennevirasto oppaita 4/2013. Liikennevirasto, Helsinki. [verkkodokumentti] Saatavilla: http://www2.liikennevirasto.fi/julkaisut/pdf3/lop_2013-04_julkisen_liikenteen_web.pdf [Viitattu 21.10.2015]

LSE, 2010. Study on the economic benefits of privacy enhancing technologies (PETs) – Final Report to The European Commission DG Justice, Freedom and Security, 2010. [verkkodokumentti] Saatavissa: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [Viitattu 20.10.2015]

Luhmann N., 1979. Trust and Power. John Wiley & Sons Inc (May 1982). 208 p.

Luhmann N., 2000. 'Familiarity, Confidence, Trust: Problems and Alternatives'. Kirjassa: Gambetta D. (toim.) Trust: Making and Breaking Cooperative Relations. Electronic edition. Department of Sociology, University of Oxford. Chapter 6, pp. 94–107. [verkkodokumentti] Saatavilla: http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf. [Viitattu 22.10.2015]

LVM, 2012. National Travel Survey 2010–2011. [verkkodokumentti] Saatavilla: http://portal.liikennevirasto.fi/portal/page/portal/e/fta/research_development/national_travel_survey/HLT_2010_2011_esite_ENG_0.pdf. [Viitattu 20.10.2015]

LVM, 2013. Oikeudenmukaista ja älykästä liikennettä. Työryhmän loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 37/2013. [verkkodokumentti] Saatavilla: http://www.lvm.fi/documents/20181/799435/Julkaisuja+37-2013/f04de992-beb1-4ff4-b716-24f70614b50e?version=1.0 [Viitattu 10.2.2016]

LVM, 2014. Vireillä olevien säädösmuutosten taloudelliset vaikutukset henkilöliikenteen yrityksiin. Liikenne- ja viestintäministeriö Julkaisuja-sarja 32/2014. [verkkodokumentti] Saatavilla: https://www.lvm.fi/docs/fi/3082174_DLFE-25794.pdf [Viitattu 22.10.2015]

Manyika J., Chui M., Brown B., Bughin J., Dobbs R., Roxburgh C. & Hung Byers A., 2011. Big data: The next frontier for innovation, competition, and productivity. McKinsey Insights & Publications, 2011. [verkkodokumentti] Saatavilla: http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx [Viitattu 19.10.2015].

Margulis S., 2003. Privacy as a Social Issue and Behavioral Concept. Journal of Social Issues, Vol. 59, Issue 2, pp. 243–261, July 2003. [verkkodokumentti] Saatavilla: http://onlinelibrary.wiley.com/doi/10.1111/1540-4560.00063/epdf [Viitattu 19.10.2015].

Mayer R., Davis J. & Schoorman D., 1995. An Integrative Model of Organizational Trust. The Academy of Management Review, Vol. 20, No. 3, July 1995, pp. 709–734. [verkkodokumentti] Saatavilla: http://www.jstor.org/stable/pdf/258792.pdf [Viitattu 20.10.2015]

McCullagh K., 2008. "What is 'private' data?" 23rd BILETA Conference. Glasgow Caledonian University. Jan. 2008. [verkkodokumentti] Saatavilla: http://works.bepress.com/karen_mccullagh/14 [Viitattu 19.10.2015]

McDonald A. & Cranor L., 2008. Cost of reading privacy policies, the. ISJLP, 4, 543. [verkkodokumentti] Saatavilla: http://technologylawdispatch.ignite.lexblog.com/wp-content/uploads/sites/560/2013/02/Cranor_Formatted_Final1.pdf [Viitattu 23.2.2016]

McLean, 2010. Complete Mobility – Providing Transport as a Service. MRC McLean Hazel September 2010 Report Number 10/105. [verkkodokumentti] Saatavilla: http://www.racfoundation.org/assets/rac_foundation/content/downloadables/achieving%20complete%20mobility%20-%20mrc%20mclean%20hazel%20-%20main%20report.pdf. [viitattu 22.10.2015]

Montjoye Y., Hidalgo C., Verleysen M. & Blondel V., 2013. Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports 3, Article number: 1376 (2013). [verkkodokumentti] Saatavilla: http://www.nature.com/articles/srep01376 [Viitattu 20.10.2015]

Moore B., 1984. Privacy: studies in social and cultural history. Armonk, N.Y.: M.E. Sharpe; New York: Distributed by Pantheon Books.

Moore J., 1993. Predators and Prey: A New Ecology of Competition. Harvard Business Review May-June 1993. [verkkodokumentti] Saatavilla: http://blogs.law.harvard.edu/jim/files/2010/04/Predators-and-Prey.pdf. [Viitattu 21.10.2015]

Muchnik L., Aral S., Sean J. & Taylor S., 2013. Social Influence Bias: A Randomized Experiment. Science, Vol. 341, 9 August 2013. [verkkodokumentti] Saatavilla: http://snap.stanford.edu/class/cs224w-readings/muchnik13bias.pdf. [Viitattu 22.10.2015]

Mullin J., 2012. How Much Do Google and Facebook Profit from Your Data? ARS TECHNICA Oct. 9, 2012, 6:38 AM PDT. [Verkkodokumentti] Saatavilla: http://arstechnica.com/tech-policy/2012/10/how-much-do-google-and-facebook-profit-from-your-data/ [Viitattu 22.10.2015]

Neuvonen R., 2014. Yksityisyyden suoja Suomessa. Lakimiesliiton Kustannus, Helsinki. 257 s.

OECD, 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [verkkodokumentti] Saatavilla: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. [Viitattu 20.10.2015]

OECD, 2007. Taxi Services Regulation And Competition. DAF/COMP(2007)42. JT03373875. [verkkodokumentti] Saatavilla: www.oecd.org/regreform/sectors/41472612.pdf [Viitattu 22.10.2015]

Omtzigt P. & Schirmer G., 2015. Mass surveillance: wrong in practice as well as principle. [verkkodokumentti] Saatavilla: https://www.opendemocracy.net/opensecurity/pieter-omtzigt-

g%C3%BCnter-schirmer/mass-surveillance-wrong-in-practice-as-well-as-principle [Viitattu 22.10.2105]

Palanisamy B. & Liu L., 2013. MobiMix: Protecting Location Privacy with Mix-zones over Road Networks. [verkkodokumentti] Saatavilla: http://www.cc.gatech.edu/~lingliu/papers/2011/MobiMix-icde2011.pdf. [Viitattu 20.10.2015]

Palanisamy B., Liu L., Lee K., Singh A. & Tang Y., 2012. Location Privacy with Road network Mix-zones. [verkkodokumentti] Saatavilla: http://www.sis.pitt.edu/bpalan/papers/MSN2012-mixzone.pdf. [Viitattu 20.10.2015]

Pell, A., Starkl, F. & Menrad, M., 2012. A field study on the acceptance of extended floating car data for real-time monitoring traffic conditions. 2012 IEEE International Symposium on Sustainable Systems and Technology (ISSST). 16–18 May 2012. Pp. 1–4. [verkkodokumentti] Saatavissa: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6227986 [Viitattu 19.10.2015].

Petronio S. & Reierson J., 2009. Regulating the Privacy of Confidentiality. Published in: Afifi T.A. & Afifi W.A. (Eds.) Uncertainty, Information Management, and Disclosure Decisions: Theories and Applications. Pp. 365–383. Routledge, New York. [verkkodokumentti] Saatavilla: http://www.cl.cam.ac.uk/~rja14/shb10/petronio10.pdf. [Viitattu 19.10.2015]

Pfitzmann A. & Hansen M., 2005. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version v0.25 Dec. 6, 2005). [verkkodokumentti] Saatavilla: http://freehaven.net/anonbib/cache/terminology.pdf. [Viitattu 20.10.2015]

Pinyol I., Sabater-Mir J. & Cuní G., 2007. How to talk about reputation using a common ontology: from definition to implementation. Proceedings of the Ninth Workshop on Trust in Agent Societies. Hawaii, USA. Pp. 90–101. [verkkodokumentti] Saatavilla: http://www.dai.ed.ac.uk/groups/ssp/members/openknowledge/Publications/How%20to%20talk%20about%20reputation%20using%20a%20common%20ontology.pdf. [Viitattu 22.10.2015]

Poikola A., Kuikkaniemi K. & Kuittinen O., 2014. My Data – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. Liikenne ja viestintäministeriö, Helsinki. [verkkodokumentti] Saatavilla: https://www.lvm.fi/docs/fi/3082152_DLFE-25061.pdf. [Viitattu 20.10.2015]

Prescient, 2011. Privacy and Emerging Sciences and Technology. [verkkodokumentti] Saatavilla: http://www.prescient-project.eu/prescient/inhalte/about/privacy.php?WSESSIONID=1c08b57fcf4eabc8b7ad7bc9cdad535a [Viitattu 23.10.2015]

Replogle M. & Fulton L., 2014. A Global High Shift Scenario: Impacts And Potential For More Public Transport, Walking, And Cycling With Lower Car Use. UC Institute for Transportation and Development Policy and University of California, Davis, September 2014. 35 p. [verkkodokumentti] Saatavilla: https://www.itdp.org/wp-content/uploads/2014/09/A-Global-High-Shift-Scenario_WEB.pdf. [Viitattu 20.10.2015]

Resnick P. & Zeckhauser R., 2002. Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. Kirjassa: Baye M.R. (toim.) The Economics of the Internet and E-Commerce. Volume 11 of Advances in Applied Microeconomics. Elsevier Science, Amsterdam. Pp. 127–157. [verkkodokumentti] Saatavilla: http://www.presnick.people.si.umich.edu/papers/ebayNBER/index.html. [Viitattu 22.10.2015]

Resnick P., Zeckhauser R., Friedman E. & Kuwabara K., 2000. Reputation Systems: Facilitating Trust in Internet Interactions. Communications of the ACM, Vol. 43, No. 12. [verkkodokumentti] Saatavilla: onemvweb.com/sources/sources/reputations.pdf [Viitattu 22.10.2015]

Rhee I., Shin M., Hong S., Lee K., Kim S. & Chong S., 2011. On the levy-walk nature of human mobility. IEEE/ACM Transactions on Networking (TON), Vol. 19, Issue 3, June 2011, pp. 630–643. [verkkodokumentti] Saatavilla: http://dl.acm.org/citation.cfm?id=2042974 [Viitattu 20.10.2015]

Rogers E., 1976. New Product Adoption and Diffusion. Journal of Consumer Research, 2 (March), pp. 290–301. [verkkodokumentti] Saatavilla: http://uts.cc.utexas.edu/~tecas/syllabi2/adv382jfall2002/readings/roger.pdf. [Viitattu 22.10.2015]

Rohunen A., Markkula J., Heikkila M. & Heikkila J., 2014. Open Traffic Data for Future Service Innovation – Addressing the Privacy Challenges of Driving Data. Journal of Theoretical and Applied Electronic Commerce Research, Vol. 9, Issue 3, September 2014, pp. 71–89. [verkkodokumentti] Saatavilla: http://www.scielo.cl/scielo.php?pid=S0718-18762014000300007&script=sci_arttext [viitattu 19.10.2015].

Rubinstein I. & Good N., 2013. Privacy by Design: A counterfactual Analysis of Google and Facebook Privacy Incidents. Berkeley Technology Law Journal, Vol. 28. pp. 1334–1414. [verkkodokumentti] Saatavilla:

http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2399105_code419245.pdf?abstractid=2128146&mirid=1&type=2 [Viitattu 20.10.2015]

Scafetta N., 2011. Understanding the complexity of the Levy-walk nature of human mobility with a multi-scale cast/benefit model. Chaos 21, 2011. 10 p.

Schoettle B. & Sivak M., 2014. The reasons for the recent decline in young driver licensing in the United States. Traffic Injury Prevention, Vol. 15, Issue 1. [verkkodokumentti] Saatavilla: http://www.tandfonline.com/doi/abs/10.1080/15389588.2013.839993#aHR0cDovL3d3dy50YW5kZm9ubGluZS5jb20vZG9pL3BkZi8xMC4xMDgwLzE1Mzg5NTg4LjIwMTMuODM5OTkzQEBAMA== [Viitattu 22.10.2015]

Shankar P., Ganapathy V. & Iftode L., 2009. Privately querying location-based services with SybilQuery. UbiComp '09 Proceedings of the 11th international conference on Ubiquitous computing. [verkkodokumentti] Saatavilla: http://dl.acm.org/ft_gateway.cfm?id=1620550&ftid=680942&dwn=1&CFID=722713708&CFTOKEN=69107582 [Viitattu 20.10.2015]

Shroff M., 2007. Privacy Impact Assessment Handbook. [verkkodokumentti] Saatavilla: https://privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/ [Viitattu 21.10.2015]

Sikow-Magny C., 2004. EU research and policy on road user charges, European Commission – Directorate General for Energy and Transport. [verkkodokumentti] Saatavilla: http://www.internationaltransportforum.org/IntOrg/ecmt/taxes/pdf/London04Sikow.pdf. [Viitattu 21.10.2015]

Simonite T., 2014. Facebook Creates Software That Matches Faces Almost as Well as You Do. MIT Technology Review, March 17. [verkkodokumentti] Saatavilla: http://www.technologyreview.com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/ [Viitattu 23.10.2015]

Sivak M. & Schoettle B., 2012. Update: Percentage of Young Persons With a Driver's License Continues to Drop. Traffic Injury Prevention, Vol. 13, Issue 4. [verkkodokumentti] Saatavilla: http://www.tandfonline.com/doi/abs/10.1080/15389588.2012.696755#aHR0cDovL3d3dy50YW5kZm9ubGluZS5jb20vZG9pL3BkZi8xMC4xMDgwLzE1Mzg5NTg4LjIwMTIuNjk2NzU1QEBAMA== [Viitattu 22.10.2015].

Sochor J., Strömberg H. & Karlsson M., 2014. The Added Value of a New, Innovative Travel Service: Insights from the UbiGo Field Operational Test in Gothenburg, Sweden. International Conference on Mobility and Smart Cities, Rome, October 27–28, 2014. [verkkodokumentti] Saatavilla:

http://publications.lib.chalmers.se/records/fulltext/204389/local_204389.pdf. [Viitattu 22.10.2015]

Solove D., 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, January 2006, No. 3. [verkkodokumentti] Saatavilla: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf. [viitattu 19.10.2015].

Song C., Qu Z., Blumm N. & Barabási A., 2010. Limits in Predictability in Human Mobility. Science 19, February 2010, Vol. 327, No. 5968, pp. 1018–1021. [verkkodokumentti] Saatavilla: https://www.sciencemag.org/content/327/5968/1018.full [Viitattu 20.10.2015]

Spiekermann S., 2012. The Challenges of Privacy by Design, Communications of the ACM, Vol. 55 No. 7, pp. 38–40. [verkkodokumentti] Saatavilla: http://cacm.acm.org/magazines/2012/7/151231-the-challenges-of-privacy-by-design/fulltext [Viitattu 20.10.2015]

Spitz S. & Tuchelmann Y., 2011. A Survey of Security Issues in Trust and Reputation Systems for E-Commerce. Kirjassa: J.M. Alcaraz Calero et al. (Eds.): ATC 2011, LNCS 6906, pp. 203–214. [verkkodokumentti] Saatavissa: http://link.springer.com/chapter/10.1007%2F978-3-642-23496-5_15 [Viitattu 22.10.2015]

Sprenger P., 1999. Sun on Privacy: 'Get Over It'. Wired 1999. [verkkodokumentti] Saatavilla: http://www.wired.com/politics/law/news/1999/01/17538. [viitattu 19.10.2015]

Steinbrecher S., 2011. The Need for Interoperable Reputation Systems. Teoksessa: J. Camenisch, V. Kisimov, andM. Dubovitskaya (Eds.): iNetSec 2010, LNCS 6555, pp. 159–169. [verkkodokumentti] Saatavilla: http://link.springer.com/content/pdf/10.1007%2F978-3-642-19228-9.pdf [Viitattu 22.10.2015]

Sun Y. & Yuhong Liu Y., 2012. Security of Online Reputation Systems. The evolution of attacks and defences. Signal Processing Magazine, IEEE, Vol. 29, Issue 2, pp. 87–97. [verkkodokumentti] Saatavissa: http://scripts.cac.psu.edu/users/y/u/yul38/My%20Paper/Security%20of%20Online%20Reputation%20Systems%20Evolution%20of%20Attacks%20and%20Defenses.pdf. [Viitattu 22.10.2015]

Tavakolifard M. & Almeroth K., 2012. A Taxonomy to Express Open Challenges in Trust and Reputation Systems. Journal of Communications, Vol. 7, No. 7, pp. 538–551. [verkkodokumentti] Saatavilla:

http://ojs.academypublisher.com/index.php/jcm/article/view/jcm0707538551. [Viitattu 22.10.2015]

Tay, 2015. Liikkuminen palveluna – esiselvitys. 8.5.2015. [verkkodokumentti] Saatavilla: http://www.hermiagroup.fi/@Bin/1800495/Liikkuminen%20palveluna%20-%20Loppuraportti%20-%20v2%20Final.pdf. [Viitattu 22.10.2015]

Tietosuojaryhmä, 2014. 0829/14/FI WP216 Lausunto 5/2014 anonymisointitekniikoista annettu 10. huhtikuuta 2014. [verkkodokumentti] Saatavilla: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf. [Viitattu 20.10.2015]

Tsai J., Kelley P., Cranor L. & Sadeh N., 2009. Location-Sharing Technologies: Privacy Risks and Controls [verkkodokumentti] Saatavissa: http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf. [Viitattu 19.10.2015]

Uber, 2015. Uber [verkkosivusto]. Saatavilla: https://www.uber.com/ [Viitattu 21.10.2015]

Urban G., Amyxb C. & Lorenzonc A., 2009. Online Trust: State of Art, New Frontiers, and Research Potential. Journal of Interactive Marketing, 23, pp. 179–190. [verkkodokumentti] Saatavilla: http://www.sciencedirect.com/science/article/pii/S1094996809000413/pdfft?md5=ff9bb226b847e822dc54d3bcab72963d&pid=1-s2.0-S1094996809000413-main.pdf [Viitattu 20.10.2105]

US DoJ, 1974. Privacy Act of 1974. [verkkodokumentti] Saatavilla: http://www.justice.gov/opcl/privacy-act-1974. [Viitattu 20.10.2015]

US DoJ, 1984. Electronic Communications Privacy Act of 1986 (P.L. 99-508) [verkkodokumentti] Saatavilla: http://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf [Viitattu 20.10.2015]

US DoJ, 1996. Telecommunications Act of 1996 [verkkodokumentti] Saatavilla: http://transition.fcc.gov/Reports/tcom1996.pdf [Viitattu 20.10.2015]

Varian H., 1996. Economic Aspects of Personal Privacy. [verkkodokumentti] Saatavilla: http://people.ischool.berkeley.edu/~hal/Papers/privacy/. [Viitattu 19.10.2015]

Vercouter L., Casare S., Sichman J. & Brandao A., 2007 An Experience on Reputation Models Interoperability based on a Functional Ontology. IJCAI'07 Proceedings of the 20th International Joint Conference on Artifical Intelli-

gence. Pp. 617–622. [Verkkodokumentti] Saatavilla: http://ijcai.org/papers07/Papers/IJCAI07-098.pdf. [Viitattu 22.01.2015]

Vodafone, 2006. Anders Betalen voor Mobiliteit – Market consultation phase 2. Final report, 04 August 2006. [verkkodokumentti] Saatavilla: http://www.m2c-solutions.com/documents/D4_Report_topic1_VODAFONE_ Final Report 070804_v2.0_tcm195-164308.pdf [Viitattu 21.10.2015]

Wang D. & Emurian H., 2004. An overview of online trust: Concepts, elements, and implications. Computers in Human Behaviour, 21, pp. 105–125. [verkkodokumentti] Saatavilla: http://www.sciencedirect.com/science/article/pii/S0747563203001092/pdfft?md5=8192668d564c8e23ad928eb433eb691f&pid=1-s2.0-S0747563203001092-main.pdf [Viitattu 20.10.2015]

Waris H. & Paloheimo H., 2015. Joukkoistetut kuljetukset – Esiselvitys. Taksipalvelut, kimppakyydit ja tavarakuljetukset. Trafin tutkimuksia 8/2015. Trafi, Helsinki. [verkkodokumentti] Saatavilla: http://www.trafi.fi/filebank/a/1430904363/19d60b16eec96575da2349c2e0cfc185/17526-Trafi_tutkimuksia__8-2015_-_Joukkoistetut_kuljetukset_-_esiselvitys.pdf. [Viitattu 22.10.2015]

Warren S. & Brandeis D., 1890. The Right to Privacy. Harvard Law Review, Vol. IV, December 15, No. 5. [verkkodokumentti] Saatavilla: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [Viitattu 19.10.2015]

WEF, 2011. Personal Data: The Emergence of a New Asset Class. An Initiative of the World Economic Forum January 2011. [verkkodokumentti] Saatavilla: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. [Viitattu 19.10.2015]

Weitzner D., 2012. Consumer Data Privacy in a networked world: A framework for protecting privacy and promoting innovation in the global Digital Economy. White House, February, 2012. [verkkodokumentti] Saatavilla: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [Viitattu 22.12.2015]

Westin A., 2003. Social and Political Dimensions of Privacy. Journal of Social Issues, Vol. 39, No. 2, pp. 431–453. [verkkodokumentti] Saatavilla: http://onlinelibrary.wiley.com/doi/10.1111/1540-4560.00072/epdf [Viitattu 19.10.2015]

Wikipedia, 2015. 2011 PlayStation Network outage. [verkkodokumentti] Saatavilla: https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage [Viitattu 20.10.2015]

Wright D. & Hert P., 2012. Introduction to Privacy Impact Assessment. Volume 6 of the series Law, Governance and Technology Series, pp. 3–32. [verkkodokumentti] Saatavissa: http://link.springer.com/content/pdf/10.1007%2F978-94-007-2543-0_1.pdf [Viitattu 20.10.2015]

Wyden R., 2013. Geolocation Privacy and Surveillance ("GPS") Act. [verkkodokumentti] Saatavilla: http://www.wyden.senate.gov/priorities/gps-act [Viitattu 20.10.2015]

Xu N., Zhu D., Liu H., He J., Du X. & Liu T., 2012. Combining Spatial Cloaking and Dummy Generation for Location Privacy Preserving. Kirjassa: Zhou S., Zhang S. & Karypis G. (toim.) ADMA 2012, LNAI 7713. Pp. 701–712. [verkkodokumentti] Saatavilla: http://link.springer.com/content/pdf/10.1007%2F978-3-642-35527-1.pdf [Viitattu 20.10.2015]

Zickuhr K., 2013. Location-Based Services. September 12, 2013. PewResearchCenter. 25 p. [verkkodokumentti] http://pewinternet.org/Reports/2013/Location.aspx. [Viitattu 19.10.2015]

Zijderhand F., Van Nifterick W. & Zwiers A., 2006. Accuracy and reliability of distance and position measurements by GNSS systems. ARS Traffic & Transport Technology bv The Hague (NL) September 2006. [verkkodokumentti] Saatavilla: https://zoek.officielebekendmakingen.nl/kst-30563-2-b8.pdf [Viitattu 21.10.2015]

Liite A: Älyliikenne (ITS) ja siihen liittyvät palvelut

Liikenteellä tarkoitetaan ihmisten, tavaroiden ja tiedon kuljettamista paikasta toiseen. Liikenne puolestaan hyödyntää liikennejärjestelmää, joka sisältää liikenneinfrastruktuurin, liikennetiedon, liikenteenhallinnan ja liikennepalvelut sekä edellisiä koskevat säädökset. Matka on Liikenneviraston määritelmän mukaan siirtymistä paikasta toiseen, esimerkiksi kotoa kauppaan tai työpaikalle. Meno ja paluu lasketaan erillisiksi matkoiksi.

Liikennekäyttäytymisen tutkimus pyrkii selvittämään, miten matkoja tehdään ja mitkä syyt ovat tämän liikkuvuuden taustalla. Yleinen olettamus liikennekäyttäytymisen tutkijoilla on, että ihmiset käyttäytyvät ennustettavasti toistaen niitä kuvioita, joihin he ovat tottuneet ja tyytyväisiä. Näkemys on jossain määrin yhdenmukainen jo aiemmin esitettyjen käytännön tutkimustulosten (luku 3.2) sekä hyödyn maksimoinnin teorian kanssa, jonka mukaan ihmiset toimivat mahdollisimman tehokkaasti. Toisaalta tutkimustulosten mukaan käyttäytyminen ei ole pitemmällä aikajänteellä täysin toistuvaa ja siten ennustettavaa, mutta lyhyemmällä tarkasteluvälillä käyttäytyminen ei juuri muutu, kun otetaan huomioon aika, maantieteelliset rajoitteet (esim. tieverkko) ja velvollisuudet, esim. työpaikalle meneminen viikolla.

Suomessa on tehty viimeisen kerran 2010–2011 laajempi liikennekäyttäytymisen tutkimus, jossa otoksena oli n. 12 000 henkilöä (LVM 2012). Tämän tutkimuksen mukaan iällä ja perhesuhteilla on huomattava vaikutus siihen, kuinka usein ja miten paljon ihmiset matkustavat. Ymmärrettävästi ne työssäkäyvät, joilla ei ole lapsia, tekevät matkoja eniten ja puolestaan vanhimmat ikäluokat vähiten. Myös maantieteellisellä sijainnilla on selkeä merkitys, sillä urbaaneilla alueilla kaikki aktiviteetit ovat saavutettavissa vähemmällä matkustamisella kuin harvemmin asutuilla alueilla.

Myös matkustamisen motivaatiotekijöitä kartoitettiin samassa tutkimuksessa ja osoittautui, että työmatkojen ja harrastuksiin liittyvien matkojen määrä on ollut pienenemässä, kun taas ostoksiin liittyvä matkustaminen on voimakkaassa (+30 %) kasvussa, mikä johtuu todennäköisesti kauppojen vapaammista aukioloajoista. Tulokset ovat yhdensuuntaisia muiden eurooppalaisten käyttäytymistutkimusten kanssa.

Liikennesuoritteiden määrä on siis yleisesti kasvussa. Urbanisoitumisen jatkuessa syntyy ongelmia, koska liikennejärjestelmissä keskeistä liikenneinfrastruktuuria, kuten tieverkkoa, ei voida enää juurikaan laajentaa. Etenkin yksityisautoilu aiheuttaa liikenneruuhkia ja paikoitusongelmia. Ruuhkat ovat erityinen ongelma alueilla, joissa on enemmän kuin miljoona asukasta. Toinen suuri ongelmaryhmä ovat liikenteen ympäristövaikutukset ja energiatehokkuus; saasteet ja melu vaikuttavat kaupunkialueiden väestön terveyteen, ja toisaalta etenkin yksityisautoilu on edelleen riippuvainen uusiutumattomista energialähteistä perinteisten polttoaineiden muodossa. Kun kehitys näissä on aikaa vievää ja kallista, liikennejärjestelmän tehokkuuden parantamisessa onkin suunnattu toiveita älyliikennejärjestelmiin (ITS,

Intelligent Traffic Systems) ja niiden tarjoamiin palveluihin, joilla voitaisiin ohjata käyttäjiä tekemään ”parempia” matkustamiseen liittyviä päätöksiä.

ITS on yhteinen nimitys kaikille niille tekniikoille ja järjestelmille, joilla voidaan tarjota innovatiivisia palveluita matkojen hallintaan. Tavoitteena on käyttää tieto- ja tietoliikenneteknologiaa liikennejärjestelmissä siten, että ne sujuvoittavat, tehostavat ja tekevät turvallisemmaksi liikenteen. Lähtökohtina ovat mm. seuraavat:

- Nykyisten resurssien käytön tehostamisen tarve. ITS-järjestelmien on arvioitu antavan paremman kustannus-hyötysuhteen liikennejärjestelmien kapasiteetin kasvattamiseen kuin investoinnit tieverkon rakentamiseen.
- Tieliikenteen turvallisuus. Vuosittain maailmassa kuolee liikenteessä 1,2 miljoonaa ihmistä (esim. Yhdysvalloissa 41 000, Euroopassa 43 000, Japanissa 6 300) ja 95 % näistä kuolemista aiheutuu inhimillisten virheiden seurauksena. Esimerkiksi yhteistoiminnallisten liikennejärjestelmien, joissa ajoneuvot ja infrastruktuuri kommunikoivat keskenään, on arvioitu pienentävän onnettomuuksien määrää.
- Ympäristövaikutusten pienentäminen. Ajoneuvot ovat suurin kasvihuonekaasujen lähde, ja CO_2- ja pienhiukkaspäästöjä sekä liikenneruuhkia voidaan vähentää, jos ajoneuvojen turhaa käyttöä voidaan vähentää järkevillä valinnoilla. Kalifornian yliopiston ja ITPD:n (Institute of Transportation and Development Policy) mukaan julkiseen ja kevyeen liikenteeseen (kävely, pyöräily) investointi säästäisi Yhdysvalloissa 100 triljoonaa dollaria vuoteen 2050 mennessä (Reploge & Fulton 2014).
- Matkustamisen mukavuuden parantaminen reaaliaikatietoja jakamalla, esim. ruuhka ja matka-aikatietoja, säätiedot, navigointi jne.
- Uusien liiketoimintamahdollisuuksien luominen, jolla tähdätään talouskasvun, tuottavuuden ja työllisyyden turvaamiseen.

Edellisiä päämääriä tukevat avoimet järjestelmät, jotka helpottavat liikennejärjestelmien yhteensopivuutta ja yhteistoimintaa (interoperability). Ympäristövaikutuksia pienentävät luotettavat ja reaaliaikaiset yhdistettyjen liikennemuotojen matkaketjut ja niiden hallinta sekä informaatiojärjestelmät, jotka tarjoavat mahdollisuuden yhdistettyjen matkaketjupalveluiden helppoon käyttöön. Jos kuluttajat kuitenkin päätyvät yksityisajoneuvojen käyttöön, sovellukset suosittelevat reittejä alhaisten ympäristövaikutusten ja polttoainetaloudellisuuden mukaan. Tieliikenteen turvallisuutta pyritään vastaavasti parantamaan ajoneuvojärjestelmillä ja autonomisella ajamisella.

ITS-tekniikan perustana ovat kaikkialle sijoitettavat sensorit, niistä tietoja välittävä langaton verkko sekä taustajärjestelmät, jotka prosessoivat ja jakavat tietoa. Sensoreina voidaan käyttää satelliittijärjestelmiä (ajoneuvopaikannus), matkapuhelimia, erilaisia tienpintaan tai tienvarteen liitettyjä antureita ja ajoneuvoon asetettavia antureita. Tiedonsiirtoverkkona hyödynnetään lyhyen kantaman teknologioita (DSRC, Dedicated Short Range Communication) ja 3G/4G/5G-matkaviestinjärjestelmiä. Taustajärjestelmät perustuvat jatkossa pilvipalveluiden hyödyntämiseen.

Ensimmäisen sukupolven ITS-palvelut ovat jo markkinoilla, ja niistä voidaan mainita kuluttajamarkkinoille suunnatut:

- Hätäpalvelut, kuten yhteiseurooppalainen eCall, jossa esim. turvatyynyn ja törmäyssensorin laukeaminen aiheuttaa sijaintitiedon välittymisen hätäkeskukseen. Kaupalliset toimijat tuottavat esim. ajoneuvojen vikapalvelua, jossa ajoneuvotiedot ja sijainti välittyvät apua tarjoavaan palvelukeskukseen.
- Vakuutuspalvelut, kuten erilaiset ajotapaan (IHYD, Insurance How You Drive) tai käyttötapaan (PAYD, Pay As You Drive) perustuvat vakuutusmallit.
- Parkkipaikkojen löytymiseen ja niiden maksamiseen liittyvät palvelut.
- Varkaudenesto- ja ajoneuvoseurantapalvelut varkaustapausten varalta.
- Logistiikkaan ja kuljetuksiin liittyvät palvelut ovat olleet jo pitkään käytössä käsittäen kuljetusten optimoinnin, etädiagnostiikan ja erilaiset opastuspalvelut, kuten navigoinnin, lepoalueiden sijainnin, raskaiden ajoneuvojen ajorajoitukset kaupunkien alueilla jne.

EU:n ITS-strategian pitkäaikaisempana tavoitteena on päästöjen vähentäminen ajoneuvojen optimoidulla käytöllä. Tähän voidaan vaikuttaa vähentämällä ajoneuvojen yleistä käyttöä ja vaikuttamalla ajotapoihin. Esimerkiksi yhdysvaltalainen Automic.com-yritys on tuonut markkinoille jo hyvin helppokäyttöisen ajotapaseurantalaitteiston, joka liitetään autoon OBD (On Board Diagnostics) -väylään ja jonka käyttö tapahtuu matkapuhelimen välityksellä.

EU:n päästövähennystavoitetta palvelevat myös erilaiset uudet liikkumisen palvelu- ja maksumallit, kuten ABvM (Alternative ways to pay Mobility) ja MaaS (Mobility as a Service). Göteborgissa Ruotsissa on ollut käynnissä Go:smart-kokeilu, jossa älypuhelinsovelluksen avulla voidaan kätevästi yhdistellä julkista liikennettä, autojen jakamista, vuokra-autopalvelua, taksia ja pyörällä liikkumista helposti paketoidulla ratkaisulla, jolla voidaan korvata kaupunkialueilla asuvien oman auton omistuksen tarve. Jokaisesta Go:smart-palvelulla tehdystä matkasta saa bonuspisteitä sen mukaan, kuinka paljon matka alentaa hiilidioksidipäästöjä yksityisautoon nähden. Bonuksia voi hyödyntää Go:smart-palveluiden käytössä. Suomessa on myös omaksuttu vastaavankaltainen MaaS-ajattelu.

Ilmaston lämpenemisen ja CO_2-päästöjen vähentämiseksi myös Euroopan autoteollisuus pyrkii eliminoimaan päästöt ja tuomaan markkinoille toimivia hybridi- ja sähköautoja seuraavien 5–10 vuoden aikana. Yhteistoiminnalliset tukiympäristöt sähköautojen lataamisen helpottamiseksi, älykäs sähkön syöttö ja varastointi (smart grid) sekä akkujen lataamisen nopeuttaminen ovat kehityksen keskiössä (EcoFeV2014).

Paljon huomiota saanut autonominen ajaminen, jossa itse ajosuoritus jätetään tietoteknisen järjestelmän vastuulle kaikissa olosuhteissa, on vielä pitkälle unelmaa, vaikka huomattavia edistysaskelia onkin tällä alalla otettu. Keskeinen elementti autonomisessa ajamisessa on luotettava ja tarkka paikannus. Satelliittipohjainen sijaintitieto ei yksinään pysty takaamaan luotettavaa paikannusta urbaanis-

sa ympäristössä, joissa on runsaasti satelliittisignaalien katvealueita. Satelliittitiedon lisäksi tarvitaan useita eri tekniikoita, kuten laser-keilausta ympäristön kolmiulotteisesta geometriasta, inertiasensoritietoja kiihtyvyydestä ja hidastuvuudesta jne., jotta sijaintitieto saataisiin tarkasti selville. Suurin haaste sisältyy kuitenkin sen älykkyyden kehittämiseen, jota tarvitaan liikenneympäristön ja -tilanteiden hahmottamisessa reaaliaikaisesti.

Energia- ja resurssitehokkaan liikkumisen keskeinen komponentti on sijaintitieto, joka auttaa matkustamisen optimoinnissa eli matkustustavan valinnassa ja reitinsuunnittelussa. Kun tätä tietoa tuotetaan ja toisaalta tarvitaan kasvavassa määrin, siihen liittyvät tietosuojaongelmat keruun, prosessoinnin, tallennuksen ja jakelun osalta vastaavasti lisääntyvät.

Liikenneministeriö on pyrkinyt osaltaan vastaamaan näihin haasteisiin käynnistämällä mm. Liikennelabra-pilottihankkeen (www.liikennelabra.fi). Siinä pyritään viranomaisten ja yksityisen sektorin yhteistyöllä nopeuttamaan älyliikennepalveluiden muodostumista. Tämän käynnissä olevan hankkeen tavoitteena on

- uusien sähköisten palveluiden ja toimintamallien kehittäminen tieliikenteen tarpeisiin tulevaisuudessa
- ITS-palveluiden tunnettavuuden edistäminen ja palveluiden vaikutusten arviointi
- osaamisen luonti uusien käyttäjälähtöisten palveluiden synnyttämiseksi sekä näiden palveluiden testaaminen käytännössä
- käyttäjätarpeiden ja käyttökokemusten kartoittaminen ja palveluiden tehokkuuden arviointi
- julkisen ja yksityisen sektorin yhteisen, liikkumispalveluiden tarjontaan sopivan palvelualustan kehittäminen ja siihen liittyvät tarpeelliset määrittelyt
- älyliikennepalveluiden markkinoiden tukeminen innovatiivisen hankintaprosessin kautta.

Liikennelabra aloitti työnsä 2014 ja alkuperäisenä ajatuksena oli ensimmäisten markkinademonstraatioiden toteuttaminen vuoden 2015 loppuun mennessä. Julkisen rahoituksen osuudella oli tarkoitus saada käsitystä liikenteen reaaliaikaisesta tilannekuvasta ja kokemuksia mahdollisesta satelliittiperustaisesta kilometriveroituksesta. Näiden tavoitteiden saavuttamiseksi julkinen sektori (liikenne- ja viestintäministeriö, Trafi ja Liikennevirasto) käytti uudentyyppistä hankintamallia, jossa liikenneviranomaiset keräävät liikenteen tilannekuvan muodostamiseen tarvittavaa tietoa suoraan yksittäisiltä ajoneuvoilta kaupallisten palvelualustojen (esim. kalustonhallintasovellusten) kautta.

Suomessa on viimeisen vuoden aikana noussut erääksi älyliikennepalveluiden keskeiseksi teemaksi ns. MaaS-ajattelu (Mobility as a Service, Heikkilä 2014), jolla tarkoitetaan eri liikkumisen muotoja (yksityisautoilu, julkinen liikenne) yhdistelevää palvelua, joilla voitaisiin joustavasti ja tehokkaasti vastata kuluttajien liikkumiseen liittyviin tarpeisiin palvelupaketteina. MaaS-ajattelun kehittymisen taustalla on useita eri trendejä, joista voidaan mainita mm. kaupungistuminen, kulutustottumusten muutokset nuoremmilla ikäluokilla, omistusauton heikko käyttöaste ja sen

ylläpidosta koituvat rasitteet (Tay 2015). Vaikka itse MaaS-käsite onkin Suomessa julkistettu, ajatus MaaS-tyyppisistä ratkaisuista ei ole aivan uusi, sillä Britanniassa tehtiin jo 2010 ensimmäinen kattavampi selvitys ”Transport as a ce” -konseptista (McLean 2010).

Kaupungistuminen johtaa kasvaviin liikennettä koskeviin ongelmiin, joita ei voida ratkaista enää perinteisin keinoin esim. tiekapasiteettia lisäämällä. Tiheästi rakennettujen kaupunkialueiden pysäköinti on muodostumassa myös kalliiksi, kun parkkitilojen maankäytön kustannukset aletaan huomioimaan tarkemmin. Koska kaupunkialueet tarjoavat tehokkaan joukkoliikenneinfrastruktuurin ja sitä kehitetään edelleen, nuoremman kaupungeissa asuvan sukupolven otaksutaan olevan aiempaa haluttomampi hankkimaan ajokorttia ja omistusautoa.

Useissa Euroopan maissa, kuten Ruotsissa, Saksassa ja Isossa-Britanniassa, ja jopa perinteisessä ”automaassa”, kuten Yhdysvalloissa, nuorten kuljettajien (alle 40-vuotiaiden ikäryhmässä) suhteellinen osuus ajokortin haltijoista onkin vähentynyt viimeisen 25 vuoden aikana (Sivak & Schoettle 2012). Samoin ajamisen määrä on vähentynyt. Suomessa sen sijaan kehitys on nuorison osalta ollut päinvastaista, esim. vuosina 1983–2008 ajokortillisten määrä 20–29-vuotiaiden ikäryhmän keskuudessa lisääntyi 51 %:sta 82 %:iin.

Muutosta ajokortin hankinnan vähenemiseen muualla on pyritty selittämään useilla eri tekijöillä, kuten viestintäteknologian kehittymisellä (etenkin internet), autoon liittyvän sosiaalisen statuksen pienenemisellä, sillä, että nuoret asuvat pitempään vanhempiensa luona, ja osittain myös kasvaneella nuorisotyöttömyydellä (Delbosc & Currie 2013, Aretun & Nordbakke 2014, Schoettle & Sivak 2014). Schottlen ja Sivakin vuonna 2013 Yhdysvalloissa suorittaman verkkohaastattelututkimuksen perusteella (N=4572, ikäryhmä 18–39 v.) kävi ilmi, että pääsyyt ajokortittomuuteen olivat

- ”liika kiire ajokortin ajamiseen” (37 % vastanneista)
- liian suuret auton omistamisen ja ylläpidon kustannukset (32 %)
- mahdollisuus saada kyyti muilta (31 %)
- pyöräilyn tai kävelyn suosiminen (22 %)
- julkisen liikenteen käyttö (17 %).

Huomionarvoinen piirre tutkimuksessa on se, että jonkinlaista alustavaa korrelaatiota löytyi koulutus- ja tulotason sekä ajokortittomuuden välillä siten, että huonommin toimeentulevat ja vähemmän koulutetut ajoivat harvemmin ajokortin. Vastaava havainto on tehty myös muissa tutkimuksissa (Delbosch & Currie 2013). Sivakin ja Schottlen (2012) tutkimuksen ongelma on se, ettei siitä käy ilmi vastaajan asuinpaikka (kaupunkialueet vs. harvemmin asutetut alueet), jolla on suuri merkitys ajokortin ja auton hankintatarpeeseen. Yhdysvaltain huonon julkisen liikenteen infrastruktuurin huomioiden vastaavan kyselyn tulokset Euroopassa saattaisivat olla hyvinkin erilaiset. Asiaa on kuitenkin tutkittu toistaiseksi vähän, joten kovin pitkälle meneviä johtopäätöksiä ajokortittomuuden ja autottomuuden lisääntymisen syistä ei voida vielä tehdä.

Suomessa ja muualla Euroopassa eräs potentiaalinen MaaS-palveluiden käyttäjäryhmä ovat ikääntyneet, joille oman auton käyttäminen liikennevälineenä ei ole enää mahdollista. Suomi on monen muun maan tapaan ikärakenteeltaan vanhenemassa, ja entistä useammat joutuvat luopumaan lääkärin määräyksestä ajokortistaan. Tällöin joustavat MaaS-tyyppiset joukkoliikenneperustaiset palvelut, kuten taksien ja julkisen liikenteen palveluiden yhdistelmät (ns. saumattomat ovelta-ovelle-matkaketjut), tulevat entistä merkityksellisemmiksi tälle kohderyhmälle.

MaaS-kokeiluja, esim. Go:smart-hankkeen UbiGO-palvelua Ruotsissa, on perusteltu osittain juuri omistusautosta luopumisella. UbiGO-hankkeessa Göteborgin alueella yli 80 perhettä testasi puoli vuotta julkista liikennettä, autonjakoa (car sharing), vuokra-autoja, taksia ja polkupyöräilyä yhdistävää MaaS-palvelua autonomistamisen sijaan (Sochor ym. 2014). UbiGo-palvelussa kotitaloudet ostivat ennakkoon kuukauden liikkumistarpeensa käyttöoikeudet ja tiliä veloitettiin julkisen liikenteen palveluiden tai autonvuokrauksen yhteydessä samaan tapaan kuin puhelinliittymien puheaikaa ja tekstiviestejä. Minimiennakkomaksu oli 1200 SeK, ja liikkumistarpeiden ylittäessä ko. maksurajan liikkumisoikeutta pystyttiin ostamaan helposti lisää ja laskutus tapahtui seuraavan kuukausimaksun yhteydessä.

Keskeinen elementti UbiGo-palvelussa oli käyttäjän älypuhelimessa toimiva sovellus, jolla kulkuneuvojen käyttöoikeuksia saatettiin aktivoida ja tehdä varauksia kulkuvälineisiin sekä osoittaa tarvittaessa liikkumisvälineen käyttöoikeus. Tämän lisäksi käyttäjät saivat älykortin, jonka avulla voitiin lainata pyöriä tai avata ennakolta varattujen vuokra-autojen ovia. Älykortti toimi lisäksi back-up-laitteena, mikäli älypuhelinsovelluksen kanssa olisi tullut ongelmia julkisessa liikenteessä.

Käyttäjäpalautteet UbiGo-palvelukokeilun aikana ja jälkeen olivat hyvin myönteiset. Varsinaisen puolen vuoden kokeilun aikana vain yksi talous 83:sta lopetti kokeilun kesken ja jälkihaastattelussa 79 % haasteluista olisi ollut kiinnostunut jatkamaan palvelun käyttöä, 18 % tietyin ehdoin ja vain 3 % olisi jättäytynyt pois, mikäli kokeilu käynnistettäisiin uudelleen. Luonnollisesti UbiGo-kokeiluun hakeutuneet olivat jollakin tavalla ns. varhaisia omaksujia (early adopters), sillä 63 % kokeiluun osallistuneista ilmoitti uteliaisuuden keskeisimmäksi motiiviksi osallistua kokeiluun (Sochor ym. 2014). Tämä käyttäjäryhmä saattaa antaa liian optimistisen kuvan MaaS-palveluiden omaksumisesta suuremmissa käyttäjäryhmissä, mutta toisaalta varhaisten omaksujien ryhmät luovat usein uusia suuntauksia ja toimivat mielipiteiden muokkaajina.

Onkin ilmeistä, että jos käyttäjille luodaan helppokäyttöisiä ja kustannustehokkaita MaaS-liikkumispalvelukonsepteja, niiden käyttöönotto suuremmassa mittakaavassa on todennäköisempää ja tällöin voidaan huomattavasti pienentää yksityisautoilun määrää (Sochor ym. 2014) ja siihen liittyviä ongelmia. Rogersin (1976) innovaatioiden diffuusioteorian termein ilmaistuna MaaS-konseptissa toteutuisivat ”suhteellisen hyödyn”, ”kokeiltavuuden” ja ”yhteensopivuuden” ehdot, jotka ovat perusedellytyksiä uuden asian omaksumisessa laajemmassa mittakaavassa.

Liite B: Julkisen liikenteen sääntely ja sen purkaminen

Julkisen liikenteen sanaston (LiVi 2013) mukaan julkisella liikenteellä tarkoitetaan kaikille avointa joukkoliikennettä, joka sisältää myös taksiliikenteen. Suomen joukkoliikenteellä puolestaan tarkoitetaan joukkoliikennelain mukaan yleisesti käytettävissä tai tilattavissa olevaa, useiden ihmisten kuljettamiseen tarkoitettua ammattimaista markkinaehtoisesti tai palvelusopimusasetuksen mukaisesti harjoitettua linja-autoliikennettä ja raideliikennettä.

Toimivaltaisella viranomaisella tarkoitetaan EU:n asetuksen N:o 1370/2007 mukaan jäsenvaltion tai jäsenvaltioiden viranomaista tai viranomaisten ryhmittymää, jolla on valtuudet toimia julkisen henkilöliikenteen alalla tietyllä maantieteellisellä alueella, tai muuta elintä, jolle on annettu tällaiset valtuudet. Toimivaltaisia viranomaisia esim. linja-autoliikenteessä ovat meillä elinkeino-, liikenne- ja ympäristökeskukset (ELY) ja muut joukkoliikennelaissa mainitut kunnalliset viranomaiset.

Lain (Joukkoliikennelaki 13.11.2009/869) mukaan viranomaiset ovat velvollisia määrittämään toimivalta-alueensa joukkoliikenteen palvelutason. Valtiolla ja kunnilla ei kuitenkaan ole velvollisuutta järjestää julkisia liikennepalveluita muutoin kuin lainsäädännössä erikseen määritellyille erityisryhmille. Jos palvelutasotavoitteen mukaiset joukkoliikennepalvelut saadaan aikaiseksi ilman julkista tukea vapaan kilpailun kautta, liikenne voidaan järjestää markkinaehtoisesti. Markkinaehtoisuudella tarkoitetaan vapaaseen kilpailuun perustuvaa menettelyä, jossa liikenne toimii kunkin liikenteenharjoittajan oman suunnittelun ja hinnoittelun pohjalta ilman julkista tukea.

Jos markkinaehtoisuus ei toteudu, on liikenne järjestettävä palvelusopimusasetuksen mukaisesti. EU:n palvelusopimusasetuksessa (PSA, EU 2007) määritellään, miten julkinen valta voi joukkoliikennepalveluiden määrän ja laadun turvaamiseksi puuttua markkinoihin. Asetus määrittelee mm. ne ehdot, joiden mukaisesti liikenteenharjoittajille voidaan myöntää yksinoikeuksia tai maksaa julkista tukea, jos toimivaltainen viranomainen päättää järjestää liikenteen markkinaehtoista liikennettä monilukuisempana, luotettavampana, korkealaatuisempana tai edullisempana.

PSA:n mukainen tuettu joukkoliikenne voidaan järjestää joko omana tuotantona tai se voidaan hankkia hankintalainsäädännön mukaisena kilpailutettuna ostosopimuksena (ns. bruttomalli) tai käyttöoikeussopimuksena (EU 2007). Näiden välinen ero liittyy lähinnä lipputuloriskin hallintaan: bruttomallissa viranomainen vastaa liikenteen suunnittelusta ja kantaa lipputuloriskin, kun taas käyttöoikeussopimuksessa tietyn reitin tai maantieteellisen alueen liikennöinnistä sopimuksella vastaava liikenteenharjoittaja kantaa lipputuloriskin.

Vuonna 2009 voimaan astuneet EU:n palvelusopimusasetus (PSA) ja kansallinen joukkoliikennelaki, joka kumosi entisen henkilöliikennelain (laki luvanvaraisesta henkilöliikenteestä tiellä 15.2.1991/343), ovat avanneet joukkoliikenteen markkinat vapaalle kilpailulle Suomessa. Vanhan henkilöliikennelain mukaiset linjaliikenneluvat muutettiin siirtymäajan liikennöintisopimuksiksi, ja näistä ensimmäiset

umpeutuivat kesäkuussa 2014, ja muut loppuvat asteittain vuoden 2019 loppuun mennessä. Siirtymäajan päättymisen jälkeen alkava liikenne on kilpailutettava hankintalainsäädännön ja joukkoliikennelainsäädännön mukaisesti, jos liikennepalveluihin käytetään julkista tukea.

Nykyinen taksiliikenne perustuu taksiliikennelaki 2.3.2007/217 -asetukseen, joka määrittää toimialan yleiset periaatteet. Taksiliikennelain mukaan ammattimainen henkilöiden kuljettaminen tiellä henkilöautolla edellyttää taksilupaa, joka oikeuttaa harjoittamaan tilaus- ja ostoliikennettä koko maassa Ahvenanmaata lukuun ottamatta. Taksiluvan haltija on velvollinen harjoittamaan liikennettä ensisijaisesti taksilupaan merkityllä asemapaikalla (paikka tai kunta), jolta liikennettä harjoitetaan ja jonne liikenteessä käytetty auto viedään ajon tai toimeksiannon jälkeen.

Taksiluvat myöntävät ELY-keskukset, jotka vahvistavat vuosittain taksilupien kuntakohtaiset enimmäismäärät. Päätöksessä määrätään myös, kuinka moneen lupaan sisällytetään kaluston esteettömyyttä koskevat vaatimukset. Taksilupa voidaan myöntää oikeustoimikelpoiselle, hyvämaineiselle ja taloudellisista velvoitteista vastaamaan kykenevälle henkilölle, joka on suorittanut Liikenteen turvallisuusviraston Trafin taksiliikenteen yrittäjäkokeen (laajuus 120 tuntia), tai hakijalle, jolla on jo ennestään taksilupa ja käytännön kokemusta taksiliikenteen harjoittamisesta.

Suomessa harjoitettavaa tavaraliikennettä puolestaan säätelevät EU:n liikenteenharjoittaja-asetus (EY) 1071/2009 (EU 2009a), EU:n tavaraliikennelupa-asetus (EY) 1072/2009 (EU 2009b) sekä kansallinen tavaraliikennelaki (laki kaupallisista tavarankuljetuksista tiellä 693/2006, Finlex 2006). Tavaraliikennelain mukaan tavaran kuljettaminen ajoneuvolla tiellä korvausta vastaan edellyttää joitakin poikkeuksia lukuun ottamatta tavaraliikennelupaa.

Tavaraliikennelupa voi olla kotimaan liikennelupa, liikennetraktorilupa tai yhteisölupa ja se on aina liikenteenharjoittajakohtainen, eikä sitä saa luovuttaa toisen käytettäväksi. Kotimaan liikenneluvalla ja liikennetraktoriluvalla voi harjoittaa tavaraliikennettä koko Suomen alueella Ahvenanmaata lukuun ottamatta. Yhteisöluvalla voi harjoittaa tavaraliikennettä sekä kotimaassa että ulkomailla. Yhteisöluvan haltijan on haettava kuljettajatodistus jokaiselle yhteisölupaa edellyttävässä tavaraliikenteessä toimivalle kuljettajalleen, joka ei ole jonkin EU-jäsenvaltion kansalainen.

Tavaraliikennelupa myönnetään viiden vuoden määräajaksi. Uusille hakijoille myönnetään yhteisölupia ja liikennetraktorilupia. Kotimaan liikennelupia myönnetään nykyisille luvanhaltijoille lupia uudistettaessa tai kalustoa lisättäessä. Kotimaan tavaraliikenneluvan, liikennetraktoriluvan, yhteisöluvan sekä kuljettajatodistuksen myöntää Etelä-Pohjanmaan ELY-keskus. Tavaraliikennelupaa koskevat taksiluvan kaltaiset henkilövaatimukset: hyvämaineinen, vakavarainen ja ammatillisesti pätevä. Vakavaraisuus edellyttää, että hakijalla/haltijalla tulee olla käytettävissään varoja vähintään 9 000 euroa ensimmäisen ajoneuvon osalta. Ammatillinen pätevyys puolestaan osoitetaan suorittamalla Trafin järjestämän tavaraliikenteen yrittäjäkurssin loppukoe hyväksytysti. Yrittäjäkursseja järjestävät esim. Suomen Kuljetus ja Logistiikka SKAL ry ja monet muut toimijat.

Kilpailu- ja kuluttajavirasto (KKV) teki huhtikuussa 2014 aloitteen liikenne- ja viestintäministeriölle (LVM), jotta ministeriö käynnistäisi selvityksen taksilainsäädännön uudistamiseksi. KKV:n mukaan tulisi ensisijaisesti luopua taksiliikennelain 19 §:n mukaisesta tarveharkintaan perustuvasta taksilupien enimmäismäärän sääntelystä. Lisäksi KKV:n mukaan olisi perusteltua arvioida uudelleen taksiliikenteen kuluttajahintojen sääntelyä koskevat periaatteet. Perusteina näille vaatimuksille KKV (2014) esitti seuraavaa:

- Sääntelyn avulla ei ole mahdollista riittävällä tavalla määrittää taksilupien oikeaa määrää. Määräsääntelyn purkamisen jälkeen taksien määrä on merkittävästi kasvanut niissä maissa, joissa taksien määräsääntelystä on luovuttu. Tarjonnan rajoittaminen vähentää kannusteita myös muiden kilpailukeinojen, kuten hinta- ja laatukilpailun, käyttöön.
- Eduskunnan perustuslakivaliokunta on todennut, että määrällisiä säännöksiä ei voida pitää välttämättöminä valvonnallisiin, matkustajaturvallisuuden takaamiseen sekä rikollisuuden ja sosiaalisten haittojen torjumiseen liittyvien syiden vuoksi.
- KKV:ssä ja aluehallintovirastoissa on tutkittu useita epäiltyjä taksiyrittäjien kartelleja nimenomaan kuntien järjestämissä tarjouskilpailuissa. Valtion ja kuntien kokonaisrahoitusosuus taksiliikenteestä on yli 400 miljoonaa euroa taksiliikenteen miljardin euron kokonaisliikevaihdosta, mikä sekin puoltaa alan sääntelyn uudelleenarviointia julkisten menojen säästämiseksi.
- Virastolle on tullut useita toimenpidepyyntöjä taksien tilausvälitystä hoitavien yritysten poissulkevista ja syrjivistä menettelytavoista. Taksinvälityskeskukset ovat tyypillisesti paikallisten taksiyrittäjien ja taksiyhdistysten omistamia.

Taksiyritystoiminnan kilpailun vapauttaminen on herättänyt voimakasta vastustusta erityisesti aluepolitiikkojen ja taksiyrittäjien keskuudessa. Säätelyn purkamisen huolina ovat taksiliikenteen alueellinen ja ajallinen saatavuus, taksiyrittäjien tulojen pienentyminen ja kuluttajahintojen nouseminen sekä matkustamisen turvallisuus. Sääntelyn jatkamista puolustellaan mm. seuraavin väittämin:

- Taksien saatavuus haja-asutusalueilla ja tiettyinä kellonaikoina (esim. arkiöinä) heikkenee. Nykyisin taksin saa myös syrjäseudulla ja yöaikaan, koska laki velvoittaa päivystyksen järjestämiseen. Ympärivuorokautinen päivystys täysin sääntelemättömillä markkinoilla ei ole kenenkään velvoite.
- Hinnat nousevat pitkällä aikavälillä, kun kuljettaja voi määritellä, millä hinnalla ajaa asiakkaan. Halvemmat taksat eivät ole mahdollisia nykyisillä taksiliikenteen kustannuksilla; taksielinkeinon harjoittaminen vaatii nykyisilläkin taksoilla auton pitämistä ajossa jatkuvasti. Taksiliikenteen vapauttaminen toisi säätelyn vapauttamista vastustavien mukaan ”Ruotsin kaltaisen ryöstöhinnoittelun” myös Suomeen.

- Kuljettajien ammattitaito ja kokemus heikentyvät. Uusia kokemattomia kuljettajia tulisi alalle runsaasti, jolloin paikkatuntemus olisi heikompi. Navigaattoriin ei voi aina luottaa, eikä matkustaja osaa aina ohjastaa oikeaan paikkaan.
- Matkustajien turvallisuus ja yhdenvertaisuus heikentyisivät. Suomessa kuljettajien tekemät rikokset ovat erittäin harvinaisia, mutta ne lisääntyisivät, jos alalle pääsisi liian helposti.

Kilpailuttamisen seurauksena olisi se, että jos taksiala ei ole säädelty ja valvottu, epärehellisimmät pärjäisivät parhaiten. Säätelyn kannattajien mukaan huono palvelu ei vähennä yksittäisen kuljettajien asiakkaita eikä hyvä tuo niitä lisää. Epärehelliset saavat siis yhtä paljon asiakkaita, mutta veloittavat heiltä enemmän. Rehelliset karsiutuvat pikkuhiljaa alalta (vrt. aiempi ”market of lemons” -tilanne).

OECD:n kilpailukomiteassa tehty taksialan selvitys (OECD 2007) arvioi taksien määrän rajoittamisen olevan taloudellisesti perusteetonta ja johtavan tulonsiirtoon kuluttajilta palvelujen tuottajille. Selvityksen mukaan määräsääntelystä ei seuraa saatavuuden tai taksien toiminnan kannattavuuden paranemista. Yritysten lukumäärä sekä kysynnän ja tarjonnan tasapaino voivat määräytyä optimaalisesti vain vapaasti toimivilla markkinoilla. Kokemukset määräsääntelyä purkaneista OECD-maista osoittavat, että taksien saatavuus on parantunut, odotusajat ovat lyhentyneet, kuluttajien tyytyväisyys on lisääntynyt ja hinnat ovat laskeneet. Ruotsissa, jota Suomessa käytetään mielellään huonona esimerkkinä taksiliikenteestä, vapautettiin samanaikaisesti sekä määrä- että hintasääntely.

LVM on myös selvityttänyt liikenteen sääntelyn vapauttamista Tempo Economics Oy:llä teettämässään tutkimuksessa 2014 (LVM 2014). Tämän tutkimuksen johtopäätökset ovat samankaltaiset kuin OECD:n – yhteiskunnan kannalta säätelyn vapauttaminen olisi hyödyllistä. Taksimarkkinoiden avautuminen kilpailulle lisäisi henkilöliikennemarkkinoiden tehokkuutta, ja tätä kautta muutosten vaikutus kansantalouden tuottavuuteen olisi positiivinen.

Erityisesti on huomioitava, että KKV:n aloitteessa on esitetty toistaiseksi vain määräsääntelyn purkamista. Hintasääntelyyn on ottanut kantaa mm. kuluttaja-asiamies, joka katsoo, että sääntelyn purkaminen enimmäishinnoittelu säilyttäen on kuluttajan kannalta tässä vaiheessa turvallisin ratkaisu. Perusteluina on mm. se, että enimmäishinnoittelusta luopuminen saattaisi aiheuttaa taloudellista turvattomuutta tilanteissa, joissa tarjonta on vähäistä tai olosuhteet muutoin ovat hankalat kuluttajan valintojen tekemisen kannalta.

Julkaisun sarja ja numero

VTT Technology 256

Nimeke	**Yksityisyyden suoja ja luottamus liikkumisen sähköisissä palveluissa**
Tekijä(t)	Immo Heino
Tiivistelmä	Raportissa käsitellään yksityisyyden suojaan liittyviä kysymyksiä erityisesti liikkumiseen liittyvien palveluiden kannalta. Liikkumisen palvelut perustuvat pitkälti paikkatiedon hyväksikäyttöön, joten tarkastelussa painotetaan paikkatiedon yksityisyyden suojaan liittyviä teemoja. Palveluiden personointi helppokäyttöisiksi ja kuluttajien tavoitteita tukeviksi riippuu pitkälti yritysten ja yhteisöjen mahdollisuudesta käyttää kuluttajiin yhdistettyä tietoa (personal data). Erilaisilla tietoteknisillä menetelmillä voidaan kerätystä aineistosta ennustaa käyttäjien käyttäytymistä ja mieltymyksiä, mikä puolestaan helpottaa palveluiden asiakaskohtaista räätälöintiä asiakaskokemuksen parantamiseksi. Toistaiseksi yritykset ovat perustaneet toimintansa käyttäjien huolettomuuteen henkilöihin liitetyn tiedon kaupallistamisessa, mutta suunta voi muuttua tulevaisuudessa. Erityisesti henkilökohtaisen paikkatiedon jakeluun näyttää jo muodostuneen käyttäjien varaumia. Raportissa tarkastellaan erilaisia lähestymistapoja yksityisyyden suojaamiseen ja käyttäjien luottamuksen kasvattamiseen niin sääntelyn kuin teknologisten menetelmien avulla. Keskeistä on jo ennakolta arvioida yksityisyyden suojaan liittyvät riskitekijät ja niiden vaikutukset (PIA, Privacy Impact Assessment) sekä antaa käyttäjille merkittävä rooli itseään koskevan tiedon käytön valtuuttamisessa (ns. MyData-lähestymistapa). Näin menetellen voidaan tasapainoilla lainsäännön vaatimusten (EU:n kiristyvän yksityisyyden suojan, ns. General Data Protection Regulation) ja kaupallisen palvelutarjonnan kehittämisen välillä. Suomessa julkisiin liikennepalveluihin, kuten joukkoliikenteeseen ja taksijärjestelmään, liittyvä luottamus on ollut korkea. Näitä koskevaa sääntelyä ollaan asteettain purkaminen ja raportissa tarkastellaan tietoteknisten menetelmien (luottamusjärjestelmien) tarjoamia mahdollisuuksia pyrkiä ylläpitämään ja kasvattamaan käyttäjien luottamusta mm. sääntelystä vapaaseen taksi- ja tavaraliikennejärjestelmään.
ISBN, ISSN, URN	ISBN 978-951-38-8409-3 (URL: http://www.vtt.fi/julkaisut) ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) http://urn.fi/URN:ISBN:978-951-38-8409-3
Julkaisuaika	Maaliskuu 2016
Kieli	Suomi, englanninkielinen tiivistelmä
Sivumäärä	97 s. + liitt. 10 s.
Projektin nimi	Liikenteen sähköiset palvelut -tutkimus
Rahoittajat	Tekes, Liikennevirasto, Trafi, LVM
Avainsanat	yksityisyys, luottamus, älyliikenne
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111

Series title and number

VTT Technology 256

Title	**Privacy and trust in mobility services**
Author(s)	Immo Heino
Abstract	This report examines privacy issues concerning mobility services. These services are based on extensive use of positioning information; accordingly, the main emphasis of this study is on location privacy. Mobility service personalization is dependent on the ability of companies to acquire and process end-users' personal information and customers' willingness to share this data. Advanced data mining tools have been developed to find patterns in large collections of personal data, identify individuals' habits, and attempt to predict their interests and preferences. This provides a better user experience by adding value and convenience to daily life; it may also change the way people carry on their business or organize their work activities and free time in the future. On the other hand, location based information can expose sensitive information about users and cause embarrassment or even physical danger and financial loss. Until now, companies have relied on users' unconcerned attitudes towards the handling of personal data, but the rapid commercialization of this data is weakening their confidence and raising concerns over the misuse of personal information. In particular, accurate location information and continuous tracking are considered one of the main candidates for increasing strain among users. The report examines privacy safeguarding methods from two perspectives—protection trough legislation and organizational privacy policies, and protection trough technology. As a result of this study, the use of Privacy Impact Assessment (PIA) frameworks and applying user-centric control of personal data (the so-called MyData approach) are suggested. These principles may help resolve conflicting interests between commercial service offerings and ever tightening EU legislation (General Data Protection Regulation). Public trust in Finnish public transportation services has been high, but there are some concerns that deregulation of taxi and freight services might reduce the confidence related to these services. The report discusses these issues and examines whether ICT technology solutions like trust and reputation systems are applicable for retaining or even increasing public trust in transportation services.
ISBN, ISSN, URN	ISBN 978-951-38-8409-3 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-1211 ISSN 2242-122X (Online) http://urn.fi/URN:ISBN:978-951-38-8409-3
Date	March 2016
Language	Finnish, English abstract
Pages	97 p. + app. 10 p.
Name of the project	Liikenteen sähköiset palvelut -tutkimus
Commissioned by	Tekes, FTA, Trafi, MinTC
Keywords	privacy, trust, privacy protection, intelligent transportation systems
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

Yksityisyyden suoja ja luottamus liikkumisen sähköisissä palveluissa

Raportin tarkoituksena on tutkia yksityisyyden suojaan liittyviä kysymyksiä erityisesti liikkumiseen liittyvien palveluiden kannalta. Liikkumisen palvelut perustuvat pitkälti paikkatiedon hyväksikäyttöön, joten tarkastelussa painotetaan paikkatiedon yksityisyyden suojaan liittyviä teemoja.

Palveluiden personointi helppokäyttöisiksi ja kuluttajien tavoitteita palveleviksi riippuu pitkälti yritysten ja yhteisöjen mahdollisuudesta käyttää kuluttajiin yhdistettyä tietoa (personal data). Erilaisilla tietoteknisillä menetelmillä voidaan kerätystä aineistosta ennustaa käyttäjien käyttäytymistä ja mieltymyksiä, mikä puolestaan helpottaa palveluiden asiakaskohtaista räätälöintiä asiakaskokemuksen parantamiseksi.

Toistaiseksi yritykset ovat perustaneet toimintansa käyttäjien huolettomuuteen henkilöihin liitetyn tiedon kaupallistamisessa, mutta suunta voi muuttua tulevaisuudessa. Erityisesti henkilökohtaisen paikkatiedon jakeluun näyttää jo muodostuneen käyttäjien varaumia. Raportissa tarkastellaan erilaisia lähestymistapoja yksityisyyden suojaamiseen ja käyttäjien luottamuksen kasvattamiseen niin sääntelyn kuin teknologisten menetelmien avulla.

ISBN 978-951-38-8409-3 (URL: http://www.vtt.fi/julkaisut)
ISSN-L 2242-1211
ISSN 2242-122X (Verkkojulkaisu)
http://urn.fi/URN:ISBN:978-951-38-8409-3