hyväksymispäivä arvosana

arvostelija

Ympäristöpalvelut ja yksityisyys

Riia Nurmi

Helsinki 23.10.2000
Seminaari: Ubicomp -tulevaisuudenkuvako?
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Ympäristöpalvelut ja yksityisyys

Riia Nurmi

Seminaariesitelmä
Tietojenkäsittelytieteen laitos
Helsingin Yliopisto
23.10.2000

Tiivistelmä:
Kirjoituksessa tarkastellaan yksityisyyden käsitettä suhteessa ympäristöpalveluihin ja henkilökohtaisen verkon sovelluksiin. Ongelmaksi nousee miten ihminen pystyy hallitsemaan eri toimintoja ja tiedonvälitystä, kun hän ei välttämättä edes näe koneita. Kun tietoa kulkee käyttäjän huomaamatta eri sovellusten ja laitteiden välillä, käyttäjän yksityisyyttä ei aina pystytä säilyttämään tarpeeksi hyvin. Käyttäjien tyytyväisyyden ja sitä kautta myös palveluntarjoajien menestyksen takaamiseksi yksityisyys olisi kuitenkin otettava huomioon jo aikaisessa vaiheessa ja yksityisyyden suojelemista tulisi tukea.

Avainsanat: yksityisyys, ympäristöpalvelut, henkilökohtainen verkko

Sisältö

1 Johdanto

Yksityisyys on osa ihmisten jokapäiväistä elämää ja tarvetta yksityisyyteen esiintyy siis kaikkialla, missä ollaan ihmisten kanssa tekemisissä. Tässä esityksessä tarkastellaan yksityisyyden suhdetta ympäristöpalveluihin (ubiquitous computing). Ympäristöpalvelut jakautuu kahteen osa-alueeseen: ympäristöön upotettuihin sovelluksiin ja henkilökohtaisen verkon (wearable computing) sovelluksiin. Sovelluksia voidaan myös luonnollisesti yhdistää niin, että käyttäjän mukanaan kantamat laitteet kommunikoivat ympäristöön upotettujen laitteiden kanssa.

Uusien tekniikoiden (esimerkiksi Bluetooth) avulla voidaan tietokoneita piilottaa mitä mielikuvituksellisimpiin paikkoihin. Tietokoneen ei tarvitse olla enää järkäle toimiston pöydällä, vaan se voi kulkea ihmisen mukana vaikkapa vaatteisiin piilotettuna tai olla upotettuna huoneen seiniin. Ympäristöpalveluiden tavoitteena onkin siirtää tietokoneet osaksi arkiteknologiaa, kaikkialla läsnä oleviksi palveluiksi. Monia toimintoja voidaan helpottaa kätkemällä pieniä tietokoneita eri puolille ympäristöämme. Ongelmaksi nousee se, miten ihminen pystyy hallitsemaan eri toimintoja ja tiedonvälitystä, kun hän ei välttämättä edes näe koneita. Kun tietoa kulkee käyttäjän huomaamatta eri sovellusten ja laitteiden välillä, käyttäjän yksityisyyttä ei aina pystytä säilyttämään tarpeeksi hyvin.

Tässä esityksessä on tarkoitus keskittyä seuraaviin kysymyksiin:

- Mitä ihmiselle tarkoittaa yksityisyys ja milloin sitä koetaan loukatun?
- Millaisia tarpeita yksityisyyden säilyttämiseksi on ympäristöpalveluiden ja henkilökohtaisen verkon sovelluksissa ja mitä ongelmia tässä on?
- Mitä pitäisi ja mitä voitaisiin tehdä yksityisyyden parantamiseksi näillä sovellusalueilla?

Aluksi luvussa 2 esitellään käsitteet ympäristöpalvelut ja henkilökohtainen verkko ja annetaan muutamia sovellusesimerkkejä. Luvussa kolme määritellään tarkemmin, mitä

tietoja käyttäjästä paljastuu hänen käyttäessään sovelluksia ja mihin näitä tietoja tarvitaan. Luvussa 4 hahmotellaan käsitettä yksityisyys ja mitä sen rikkominen merkitsee. Luvussa 5 esitellään yksityisyyttä suojaavia lakeja ja luvussa 6 esitellään joitain keinoja, joilla voitaisiin parantaa yksityisyyden suojaa. Luku 7 sisältää yhteenvedon.

2 Ympäristöpalvelut

Ympäristöpalveluilla tarkoitetaan uuden ajan teknologiaa, jonka tarkoituksena on tuoda teknologia näkymättömäksi lisäksi jokapäiväiseen elämään. Ympäristöpalvelun sovellusten on tarkoitus helpottaa ihmisen työntekoa ilman, että ihmisen täytyy keskittyä tietokoneen käyttämiseen. Tällä hetkellä ympäristöpalveluiden sovellukset ovat keskittyneet lähinnä kokouksien tukemiseen sekä opiskeluympäristön parantamiseen [AbM00] ja useimmat testiympäristöt sijaitsevatkin tutkimuslaboratorioissa ja yliopistoilla. Tämä johtunee siitä, että ympäristöpalvelut ovat pitkälti vielä kehitysasteella ja kehittäjät tekevät palveluita, joista he itse hyötyvät ja joita he voivat testata omassa ympäristössään.

Jonkin verran vastaavia palveluita kuin ympäristöpalvelut tarjoavat muun muassa kannettavat tietokoneet, PDA-laitteet, matkapuhelimet ja taskulaskimet. Näiden laitteiden kohdalla käyttäjä joutuu kuitenkin keskeyttämään toimintansa siirtyäkseen käyttämään jotain tiettyä laitetta. Nämä laitteet eivät ole myöskään läpinäkyviä käyttäjälle eivätkä kommunikoi automaattisesti keskenään, joten ne eivät ole varsinaisia ympäristöpalveluita [Man96].

Eräs esimerkki ympäristöpalveluista on aktiiviset merkit (active badges), joiden avulla voidaan tarkkailla ihmisten liikkumista tietyssä tilassa [Wan92]. Sovelluksessa ihmiset kantavat mukanaan merkkejä, jotka lähettävät signaalia sijainnistaan. Ympäristöön

upotetut sensorit välittävät tiedon henkilöiden sijainnista keskitetysti paikallistamissovellukselle, joka vuorostaan välittää tiedon sitä tarvitseville.

2.1 Henkilökohtaisen verkon sovellukset

Pelkästään ympäristöön sijoitetut laitteet eivät riitä kattamaan ihmisten tarpeita. Ensinnäkin tuntuu epätodennäköiseltä, että kaikki ympäristöt sisältäisivät suuren määrän erilaisia laitteita ja toisaalta yleiskäyttöiset laitteet eivät pysty tarjoamaan yksilöllisiä palveluja kaikille [Man96]. Henkilökohtainen verkko sijoittaa puhtaimmillaan kaikki toiminnot käyttäjää itseensä [RMW99], jolloin palvelut liikkuvat käyttäjän mukana kaikkialle, mihin tämä menee ja tarjoavat yksilöllisiä palveluja juuri kyseiselle käyttäjälle.

Osittain henkilökohtaisen verkon sovellukset voivat toimia aivan omillaan, kommunikoimatta muun maailman kanssa. Esimerkiksi käyttäjän mukana olevat laitteet voivat tarkkailla tämän ruumiintoimintoja, kuten sydämen sykettä sekä liikkumista vaikkapa kenkiin kiinnitettyjen sensorien avulla [Man96]. Kyseisiä tietoja voidaan käyttää terveydentilan tarkkailuun tai liikunnan yhteydessä sykemittarin tavoin.

Monilla ihmisillä on vaikeuksia muistaa muiden henkilöiden nimiä. Tähän ongelmaan on kehitelty automaattista kasvojen tunnistajaa [Man96]. Tunnistus tapahtuu siten, että käyttäjään kiinnitetty kamera ottaa kuvan käyttäjän tapaamasta henkilöstä ja sovellus vertaa kuvaa paikallisesti mukana kannettavassa tietokannassa oleviin kuviin. Jos tunnistaminen tapahtuu, sovellus voi kertoa käyttäjälle paitsi toisen nimen myös kaiken muun tästä talletetun tiedon, kuten missä käyttäjä on tavannut kyseisen henkilön aiemmin.

Usein on kuitenkin hyödyllistä saada tietoja ulkopuolelta tai välittää omia tietoja sinne. Esimerkiksi ihmisen ruumiintoiminnoista kertovat tiedot voitaisiin välittää käyttäjän henkilökohtaiselle lääkärille diagnoosia varten. Ilmoitus voidaan tehdä myös poliisille,

jos havaitaan, että henkilön sydämensyke on erittäin korkea eikä henkilö kuitenkaan ole liikkeessä, mikä voisi kertoa esimerkiksi siitä, että henkilöä ryöstetään juuri [Man96]. Samoin automaattisen kasvojen tunnistajan kohdalla voitaisiin käyttää ulkopuolista tietokantaa vertailuun [Man96].

Henkilökohtaisen verkon sovelluksien on myös vaikea selviytyä paikkaan sidotun tiedon, paikkaan sidotun kontrollin sekä resurssien hallitsemisesta yksin. Esimerkiksi vammaisille tarjottavaa palvelua, jonka avulla kontrolloidaan eri toimintoja huoneessa [RMW99], ei voida käyttää hallitsematta huoneen resursseja. Palvelu voisi toimia niin, että käyttäjän saapuessa uuteen huoneeseen, hänen mukanaan kuljettamansa laite lähettää käyttäjän henkilökohtaisen profiilin huonetta hallitsevalle laitteelle. Profiilin perusteella huoneen hallitsija voi muuttaa valaistusta ja lämpötilaa tai vaikka käynnistää muita sovelluksia, jotka säätävät pöytätasojen ja kynnyksien korkeuksia.

Henkilökohtaisen verkon sovelluksissa löytyy myös useita esimerkkejä, joissa tarjotaan paikkasidonnaista tietoa, esimerkkinä opaskierrokset. Tällaisissa järjestelmissä tieto paikasta havaitaan ulkotiloissa GPS-järjestelmän avulla ja sisätiloissa paikkamerkkien (location beacons) avulla [RMW99]. Paikkamerkit ovat periaatteessa sama asia kuin mukana kannettavat aktiiviset merkit, joita käytetään ympäristöpalveluiden yhteydessä, mutta paikkamerkkien yhteydessä ei ihminen kannakaan laitetta, joka lähettää tietoa ihmisestä vaan paikkaan on piilotettu merkkejä, jotka lähettävät tietoa paikasta [RMW99].

2.2 Hive

Ympäristöön upotettujen laitteiden ja henkilökohtaisen verkon sovelluksia yhdistävää Hiveä on ehdotettu ratkaisuksi, jossa olisi molempien mallien hyvät puolet, mutta ei huonoja [RMW99]. Ehdotuksen mukaan siis ympäristöön upotettujen laitteiden ongelmat yksilöllisten palveluiden tarjoamisen kanssa ja henkilökohtaisen verkon

sovelluksien ongelmat paikkaan sidotun tiedon, paikkaan sidotun kontrollin ja resurssien hallinnan kanssa ratkeaisivat.

Hive on hajautettu agenttialusta (distributed agents platform) eli hajautettu järjestelmä, jonka avulla voidaan rakentaa sovelluksia verkottamalla paikallisia resursseja. Esimerkkejä sovelluksista, joissa on käytetty Hiveä ovat teemamusiikin esittäminen (Theme music) ja "Where's Brad?" agentti [RMW99].

Teemamusiikki –sovelluksessa henkilökohtaisen verkon omaavan henkilön astuessa huoneeseen, yrittää agentti löytää DJ-agentin, joka hoitaa huoneessa olevaa stereolaitteistoa. Jos agentti löytää DJ:n, eikä huoneessa soi musiikki sillä hetkellä, agentti lähettää DJ:lle sellaisen MP3:n osoitteen, jossa on käyttäjän henkilökohtainen teemamusiikki ja DJ laittaa musiikin soimaan [RMW99]. Tämä agentti siis kommunikoi paikallisten resurssien kanssa. Työnjako on sellainen, että henkilön yhteydessä oleva sovellus pitää yllä tietoa käyttäjän paikasta ja teemamusiikista ja DJ agentti pitää yllä resurssitietoja, kuten soiko tällä hetkellä jokin musiikki vai ei.

Useimmat agentit tarjoavat palveluita vain omalle käyttäjälleen, mutta "Where's Brad?" agentti näyttää, että arkkitehtuuri mahdollistaa myös tiedon tarjoamisen muille [RMW99]. Agentti voi toimia missä tahansa laboratoriossa ja se tuottaa kartan, joka näyttää henkilökohtaisen verkon omaavien käyttäjien sijainnin. Agentti käyttää toiminnassaan resurssinhaku työkaluja niin, että se etsii agentteja, jotka ovat yhteydessä tiettyyn henkilöön. Näkyvyyden määrää säädellään henkilökohtaisen verkon omaavan käyttäjän puolelta. Käyttäjä voi määrätä mitkä agentit saavat tietää hänen sijaintinsa ja myös sen kenelle tietoa voidaan jakaa. Esimerkiksi samassa työryhmässä olevat ihmiset saavat tietää tarkan sijainnin kun käyttäjä on työpaikalla, mutta eivät mitään tietoa talon ulkopuolelta [RMW99].

3 Käyttäjästä talletettava tieto

Käytettäessä ympäristöön upotettuja palveluja tai henkilökohtaisen verkon sovelluksia, jotka kommunikoivat ympäristön kanssa, välitetään käyttäjästä erilaisia tietoja tietoverkon välityksellä. Esimerkiksi edellisessä kappaleessa esitellyissä sovelluksissa välitetään tietoa käyttäjän sijainnista, terveydentilasta, profiilista ja mielimusiikista.

Tietoverkossa toimivasta käyttäjästä voi jäädä paljon muitakin jälkiä, kuten verkko-osoite, käyttäjätunnus, henkilön nimi, hakupalveluissa käytetyt hakusanat, yleisissä keskusteluryhmissä esitetyt mielipiteet, verkkokaupankäynnissä fyysinen toimitusosoite, henkilötunnus, pankkitilin numero ja luottokortin numero [Lam97]. Huomattavaa on myös se, että vaikka palvelu sinänsä ei vaatisikaan käyttäjätunnusta vaan sallisi käyttäjän anonyymin toiminnan, jää verkkoliikenteestä kuitenkin aina tietoja kuten sähköposti- tai muu tunnus, IP-osoite, puhelinnumero tai muu verkko-osoite, proxy-palvelimen osoite tai yrityksen palomuuri-koneen osoite [Lam97].

Käyttäjää määrittäviä sähköisiä jälkiä jää muun muassa operaattoreille, vastaanottajille, palveluntarjoajille, yritysten sisäisille palvelimille sekä julkisiin keskusteluryhmiin [Lam97]. Koska jälkiä jää useaan paikkaan eikä kaikkialla tietoturvan taso ole riittävä, on olemassa suuri riski, että kuka tahansa voi saada tietoja tietoverkkoja käyttävistä henkilöistä. Keräämällä tarpeeksi tietoa eri lähteistä ja yhdistelemällä niitä voidaan saada selville mitä palveluita käyttäjä käyttää, mitä hän ostaa ja kenelle hän lähettää viestejä.

Käyttäjästä kerättyjä tietoja voidaan käyttää käyttäjäprofiilin luomiseen. Profiilia puolestaan voidaan käyttää paitsi yksilöllisten palvelujen tuottamiseen, myös henkilön tarkkailemiseen tai jopa vakoilemiseen työnantajan tai valtion taholta. Suuri markkina-alue käyttäjäprofiileille ovat myös erilaiset palveluyritykset, jotka profiilien avulla voivat suunnata mainontaansa juuri tietylle kohderyhmälle.

3.1 Profiilien tarve

Tänä päivänä palveluiden tuottajien on tarjottava yksilöityjä palveluita tyydyttääkseen erilaisten kuluttajien tarpeet [Lan92].

Jos ihmisille halutaan tarjota yksilöllisiä palveluja käyttäjästä tarvitsee kerätä mahdollisimman paljon tietoa. Käyttäjä paljastaa tietäen tai tietämättään itsestään henkilökohtaisia mieltymyksiä ja joutuu usein automaattisen profiloinnin kohteeksi käyttäessään palveluja. Paikkasidonnaisten palvelujen kohdalla käyttäjä joutuu samalla myös paikallistetuksi.

Yksi tapa hoitaa käyttäjille yksilöllisiä palveluita on se, että jokainen käyttäjä täyttää seikkaperäisen lomakkeen kertoen omista mieltymyksistään. Käyttäjät eivät kuitenkaan ole yleensä kovin innokkaita täyttämään pitkiä lomakkeita, mieltymykset muuttuvat ajan myötä eivätkä käyttäjät aina osaa eritellä tarkoitusperiään. Suuri ongelma on myös se, että sovellukset eivät välttämättä osaa kysyä oikeita kysymyksiä. Näistä seikoista johtuen yksilöllisiä käyttöliittymiä tehtäessä saadaan parempia tuloksia käyttäen oppivia menetelmiä, kuten mukautuvia käyttöliittymiä [Lan92]. Mukautuvia käyttöliittymiä käyttävät palvelut yhdistävät käyttäjän itse antamia tietoja siihen kokemukseen mitä niillä on käyttäjistä. Käyttäjät voidaan jakaa karkeasti luokkiin mieltymystensä perusteella tai jokaiselle käyttäjälle voidaan tehdä aivan oma yksilöity profiili, jonka kautta hänelle suodatetaan tietoa.

Profiilin luominen on hyvä asia, jos käyttäjä on siitä tietoinen ja hyväksyy sen, eikä kukaan kenelle käyttäjä ei halua tietojaan näyttää näe niitä.

4 Ympäristöpalvelut ja yksityisyys

Yksityisyyden määritelmä vaihtelee riippuen tilanteesta. Kun kyseessä on uusi teknologia kuten ympäristöpalvelut, uudet käyttäytymismallit ja sosiaaliset normit kehittyvät sen mukana [BeS93]. Hyväksyttävänä pidettävä käytös muuttuu koko ajan. Lisäksi ihmiset hyväksyvät uuden teknologian helpommin, vaikka se sisältäisikin mahdollisuuden yksityisyyden loukkauksiin, jos he pitävät siitä saatavia hyötyjä riskejä suurempina [BeS93]. Yksityisyys on siis kunkin henkilökohtainen käsitys yksityisyydestä muokattuna kulttuurisilla odotuksilla ja havainnoilla omasta ympäristöstä [BeS93]. Toinen määritelmä yksityisyydelle on "yksilön mahdollisuus kontrolloida itseensä liittyviä tietoja" [Mil95].

Yksityisyyden loukkaukset suhteutetaan yleensä tilanteeseen, jossa loukkaus tapahtuu. On eri asia, jos oma perheenjäsen näkee vahingossa henkilökohtaisia papereita kuin jos esimies seuraa työntekijäänsä kaikkialle minne tämä menee, tai jos ihmisen henkilökohtaisia asioita paljastetaan lehdistölle. Oleellisia ovat kysymykset: mitä tietoja ihmisestä paljastuu, missä kontekstissa tietoja paljastuu, milloin paljastuminen tapahtuu, miksi tietoja paljastuu tai miksi niitä ylipäätään on kerätty ja erityisesti kenelle tiedot paljastuvat.

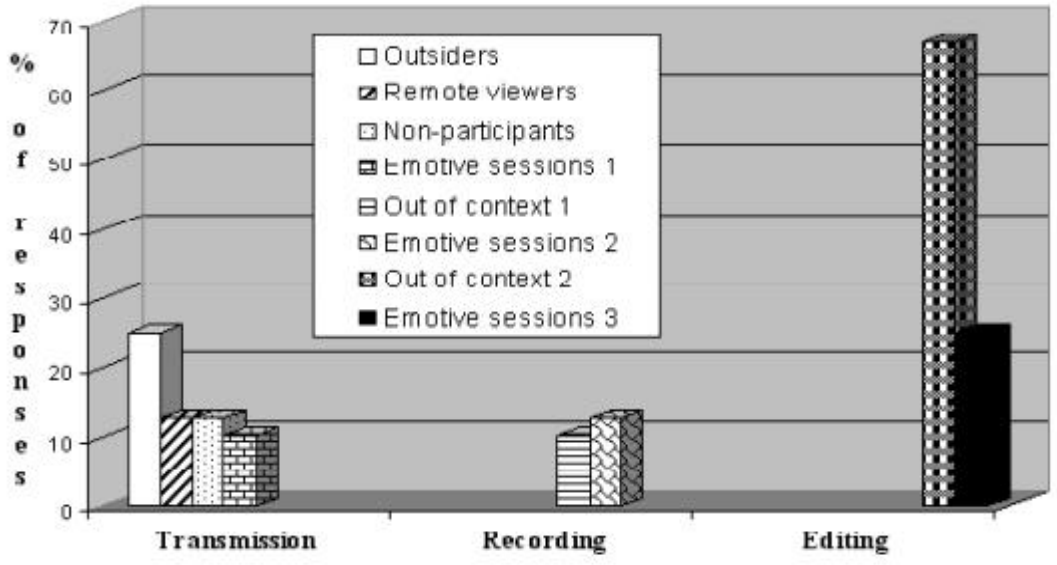
Yleistäen voidaan sanoa, että ihmiset eivät pidä siitä, että heistä kerätään tietoja. Ironista kyllä ihmiset ovat usein innokkaita tutkimaan toisten yksityisiä tietoja [Vol00] ja saamaan yksilöityjä palveluja.

IETF:n (Internet Engeneering Task Force) jäsenten keskuudessa tehtiin tutkimus, jonka tavoitteena oli selvittää asiantuntijoiden näkemyksiä yksityisyyttä koskeviin riskeihin liittyen tiedon välittämiseen Internetin avulla [AdS99]. Kaikkia erääseen IETF:n kokouksessa esiintyneitä haastateltiin. Haastatteluissa pyrittiin kattamaan kolme osa-aluetta: lähetettyjen esiintymisten vastaanottajat, lähetyksen arkaluontoisuus ja

materiaalin jälleenkäyttö (information receiver, information sensitivity, information usage) [AdS99].

Esiintymisten lähettämiseen liittyen haastatellut näkivät joko nykyisinä tai mahdollisina ongelmina ulkopuolisten mukanaolon, kaukaiset lähetyksen seuraajat, jotka todennäköisesti näkevät vain osan esityksestä, esitystä seuraamattomien (esimerkiksi nukahtaneiden tai lehteä lukevien) paljastumisen ja tunnepitoisten esiintymisten lähettämisen. Tallentamiseen liittyvinä ongelmina nähtiin nauhoituksen joutuminen pois asiayhteydestään (esimerkiksi esiintymisen aika ja paikka tulisi aina kertoa) ja tunnepitoisten esiintymisten tallettaminen. Talletetun materiaalin uudelleenkäsittelyyn liittyvinä ongelmina mainittiin tallenteen joutuminen pois asiayhteydestä ja tunnepitoisten esiintymisten käsittely. Tutkimuksessa havaittiin, että valta-osa (67%) vastaajista piti materiaalin mahdollista jälleenkäyttöä toisessa asiayhteydessä suurimpana uhkana yksityisyydelleen (kuva 1).

Useimmat haastatelluista eivät pitäneet tallennettujen esiintymisten uudelleenkäyttöä huonona asiana, mutta olisivat halunneet itse vaikuttaa siihen missä ja miten materiaalia käytetään. Jos talletetun materiaalin käyttö on vapaata, johtaa se usein siihen, että materiaalista käytetään vain osa ilman alkuperäistä kontekstiaan, jolloin väärinymmärrysten vaara on suuri [AdS99].



Kuva 1: Käyttäjien nimeämät ongelmat [AdS99].

4.1 Ongelmia yksityisyyden säilymisessä

Yksityisyys on kenties suurin ongelma ympäristöön upotettujen laitteiden kohdalla [RMW99]. Järjestelmät tarkkailevat käyttäjää tallettaen tietoa tämän tekemisistä ja mieltymyksistä ilman, että käyttäjällä on mitään suoranaista kontrollia siihen, mitä talletetaan ja mihin talletetaan. Henkilökohtaisen verkon sovellukset ratkaisevat ainakin osan ongelmasta pitämällä tiedot käyttäjän itsensä lähellä.

Ympäristöpalvelut tarvitsevat tietoa käyttäjän profiilista, jotta ne pystyisivät tarjoamaan yksilöityjä palveluita käyttäjille. Ongelmia tulee kuitenkin silloin, jos käyttäjä ei pysty estämään profiilinsa lataamista eri järjestelmiin. Esimerkiksi jos yhtiön edustaja menee neuvottelemaan sopimuksesta toisen yhtiön konttoriin, ei hän todennäköisesti halua oman profiilinsa tulevan vastaneuvottelijoiden tietoon, sillä siitä voi olla haittaa neuvotteluissa.

Yksityisyyden rikkoutuminen on erityisen suuri ongelma, jos tiedot joutuvat "vääriin käsiin" eli tietotekniikkaa käytetään epäeettisiin tarkoituksiin [BeS93]. Kaikki

tietojärjestelmät, ja erikoisesti hajautetut tietojärjestelmät, sisältävät mahdollisuuden tietovuotoihin. Sovellukset voivat säilyttää yksityisyyden hyvin teoriassa mutta harvoin käytännössä [Mul89].

Ihmisten paikallistaminen hyvin tarkasti on eräs piirre, joka uudella teknologialla saavutetaan helposti. Kriittisessä tilassa olevat potilaat haluavat varmasti erikoislääkärin olevan helposti saavutettavissa ja tulipalon sattuessa palomiesten on hyvä olla lähellä [Doh94]. Toisaalta esimerkiksi työntekijä ei halua työnantajan tietävän meneekö hän lounastauolla työpaikan ruokalaan vai tapaamaan tuttuja paikalliseen pubiin. Paikallistettavuuden tarpeen on oltava erittäin hyvin perusteltua ja paikallistajan on se pystyttävä perustelemaan. Ihmisiä ei pidä pakottaa perustelemaan miksi he eivät halua olla paikallistettavissa vaan heillä on oikeus kysyä, miksi joku haluaa paikallistaa heidät [Doh94].

Palvelun tarjoajien tulisi ottaa yksityisyyteen liittyvät seikat vakavasti ja hoitaa niitä ennaltaehkäisevästi, sillä käyttäjät luottavat yleensä johonkin yhtiöön ja tätä kautta myös kyseisen yhtiön tuotteisiin. Jos käyttäjät itse löytävät aukon tietojensa turvaamisessa, menettävät he yleensä uskon tuotteen tarjonneeseen yhtiöön eivätkä kyseessä olleeseen teknologiaan [AdS99].

Ongelma on se, että teknologia ja sovellukset ovat vielä niin uusia ja niissä ei ole vielä keskitytty yksityisyyden säilyttämiseen. Kokeiluja ympäristöpalveluiden sovelluksilla tehdään usein yritysten tai yhdistysten omissa laboratorioissa ja kokeilun kohteena ovat itse palveluiden kehittäjät. Tällöin luottamus palveluntarjoajaan on suuri [AdS99, BeS93], mikä ei kuitenkaan vastaa tilannetta todellisessa käytössä. Toisaalta myöskään tarkkoja lakeja ja säännöksiä koskien uutta teknologiaa ei ole olemassa, joten käytäntö hieman vaihtelee riippuen palveluntarjoajasta.

5 Yksityisyyttä suojaavat lait

Uusien lakien hyväksyminen on verrattain hidas prosessi, joten tietotekniikan sovelluksissa voidaan joutua tilanteisiin, joissa ei ole selkeää lakipykälää, jota noudattaa. Useimmiten voidaan kuitenkin soveltaa jo olemassa olevia lakeja.

Suomessa yksityishenkilöä suojaavat useat lait ja oikeus yksityiselämän suojaan on perusoikeus. Henkilötietojen käsittelyssä on noudatettava henkilötietolakia, julkisuuslakia ja tapauskohtaisesti soveltuvaa erityslainsäädäntöä [Lai00]. Henkilötietolakia sovelletaan henkilötietojen automaattiseen käsittelyyn sekä muuhun käsittelyyn, kun henkilötiedot muodostavat henkilörekisterin [Lai00]. Henkilötietolaissa on kielletty arkaluonteisen tiedon kerääminen ilman henkilön nimenomaista suostumusta. Arkaluonteisella tiedolla tarkoitetaan muun muassa henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai etnistä alkuperää kuvaavia tietoja.

Ympäristöpalveluissa ja henkilökohtaisen verkon sovelluksissa liikkuvaa tietoa säätelee teletoiminnan tietosuojalaki. Teletoiminnan tietosuojalakia sovelletaan perinteisten telepalveluiden ohella sähköpostiin ja televiestintään Internetin välityksellä. Lain avulla rajoitetaan yritysten oikeutta käsitellä viestinnässä saatavia tunnistetietoja. Esimerkiksi erilaisten profiilien laatiminen on rajoitusten piirissä [Lai00].

Eräs erityispiirre tietotekniikassa ja erityisesti Internetissä on sen maailmanlaajuisuus. Suomen lakien lisäksi vaikuttavat kansainväliset normit ja ohjeet, kuten Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä [Lai00].

Mielenkiintoiseksi asia tulee, kun maan ja koko Euroopan unionin rajat ylitetään. Mitä lakeja silloin noudatetaan? Henkilökohtaisen verkon tapauksessa ihmisellä voi olla mukanaan pienoistietokoneita, jotka kommunikoivat ympäristön kanssa. Mitä tapahtuu kun suomalainen henkilö menee vaikkapa Kuubaan ja hänen mukanaan olevat laitteet kommunikoivat paikallisten laitteiden kanssa?

6 Keinoja yksityisyyden suojan parantamiseksi

Yksityisyyden suojaa ympäristöpalveluiden kohdalla voidaan parantaa erilaisilla keinoilla, kuten tarjoamalla mahdollisuus anonyyminä esiintymiseen ja ottamalla jo suunnitteluvaiheessa huomioon avoimuus.

6.1 Mahdollisuus anonyymiyteen

Käyttäjällä tulee olla mahdollisuus anonyymiyteen tilanteissa, joissa käyttäjän todentaminen ei ole välttämätöntä [Lam97]. Anonyymiys voidaan toteuttaa joko niin, että käyttäjän henkilöllisyys ei paljastu missään olosuhteissa tai siten, että käyttäjä on tarvittaessa jäljitettävissä esimerkiksi operaattorin ylläpitämien lokitietojen kautta.

Käyttäjälle voidaan tarjota anonyymipalveluja, jotka poistamalla käyttäjän tunnistamistiedot mahdollistavat nimettömänä tai pelkällä nimimerkillä toimimisen. Myös tunnistetietojen salaaminen kryptografiaan perustuvilla ratkaisuilla suojaa käyttäjän yksityisyyttä [Lam97].

6.2 Avoimuus

Käyttäjän profiilien suunnittelussa ja muussa tiedon keruussa on erittäin tärkeää kertoa käyttäjälle tiedon keruun syyt, mitä tietoa talletetaan, kuka sitä saattaa päästä

katsomaan ja missä sitä voidaan myöhemmin käyttää. Käyttäjiä huolettaa kuka näihin tallennettuihin tietoihin pääsee käsiksi. Tietokoneiden ollessa kyseessä useimmat ihmiset eivät tiedä mitä ne tekevät. Tiedon puute aiheuttaa pelon, että jotain tehdään "selän takana" [AbM00].

EuroPARC:in tutkimuslaboratorioon pystytetty mediatila (media space), RAVE ympäristö, on yksi esimerkki ympäristöpalveluiden käytännön tutkimuksesta [BeS93]. RAVE:ssa jokaiseen toimistoon, auloihin ja kokoushuoneisiin on sijoitettu kameroita, monitoreita, mikrofoneja ja kaiuttimia. RAVE -ympäristön kanssa tehdyt tutkimukset ovat vahvistaneet, että yksityisyyden parantamiseksi voitaisiin tehdä paljon ottamalla palautteen ja kontrollin antaminen käyttäjälle huomioon jo suunnitteluvaiheessa [BeS93].

Tutkimuksessa havaittiin, että on tärkeää antaa käyttäjälle palautetta seuraavista asioista: mitä tietoa käyttäjästä kerätään, mitä tiedolle tapahtuu sen siirtyessä järjestelmään, kuka pääsee tietoon käsiksi ja mitä varten tietoja halutaan [BeS93]. Käyttäjälle on tärkeää antaa myös keinot kontrolloida vastaavia asioita, mistä hänelle annetaan palautetta. Yksityisyyden suojelemisessa on tärkeintä tietää, mitä tietoja järjestelmä saa tietää käyttäjästä [BeS93]. Aina ei ole mahdollista selvittää, mihin tietoja halutaan käyttää, vaan käyttäjän on pääteltävä tietojen luonteesta ja siitä kuka pääsee tietoja katsomaan, voiko hän luovuttaa kyseiset tiedot.

Tutkimuksen tarkoituksena oli kehittää ympäristöpalveluiden suunnittelua helpottava suunnittelukehys. Yleisiä suunnitteluperiaatteita ovat suunnittelun halpa hinta, opittavuus, tarkoituksenmukaisuus sekä helppous ja se, että käyttäjän tulee suoriutua tehtävistään mahdollisimman vähällä vaivalla. Lisäksi listattiin seitsemän kohtaa, jotka ovat erityisen tärkeitä yksityisyyden suojelemisessa. Nämä olivat luotettavuus, palautteen oikea ajoitus, palautteen näkyvyys, häiritsemättömyys, muiden yksityisyyden suojeleminen, turvallisuus ja joustavuus [BeS93].

Palautteen antaminen voi kuormittaa palvelua, jos vaaditaan, että kaikesta on annettava täysimittainen selvitys käyttäjälle. Tämä voidaan ratkaista niin, että tietoa on saatavissa jos käyttäjä niin haluaa, mutta ei oletusarvoisesti. Tai käyttäjälle voidaan antaa kaikki tieto oletusarvoisesti kunnes käyttäjä itse määrittelee, että hän ei halua enää nähdä tietoa (käyttäjä luottaa palvelun tarjoajaan). Tällaisessa tapauksessa käyttäjän tulisi voida siirtyä ensiksi mainittuun tapaan, jossa hän saa tiedot kuitenkin esiin niin halutessaan.

7 Yhteenveto

Yksityisyys on erittäin tärkeä osa-alue kehitettäessä ympäristöpalveluja. Ottamalla yksityisyys huomioon tärkeänä osa-alueena jo suunnitteluvaiheessa voidaan yksityisyyden takaamiseksi tehdä paljon. Ihmisille on tärkeää tuntea hallitsevansa itseään koskevia tietoja ja tämä hallintaoikeus tulisi käyttäjällä säilyttää ellei käyttäjä itse siitä tietoisesti luovu. Käyttäjän tiedoista tulisi säilyttää vain tarpeellinen ja tietoa tulisi tallentaa mahdollisimman vähän eri paikkoihin. Lisäksi talletuspaikan tulisi olla turvallinen, parhaimmillaan se olisi käyttäjän itsensä hallittavissa.

Lähteet

RMW99 Rhodes, B. J., Minar, N., Weaver, J., Wearable Computing Meets Ubiquitous Computing: Reaping the best of both worlds. *Proc. The Third International Symposium on Wearable Computers (ISWC '99)*, San Francisco, CA, October 18-19 1999, pp. 141-149.

BeS93 Bellotti, V., Sellen, A., Design for Privacy in Ubiquitous Computing Environments. *G. de Michelis, C. Simone & K. Schmidt (eds.), Proceedings of ECSCW?93*, Milano, Italy, Sept 1993, Kluwer (Academic Press), 77-92.

AdS99 Adams, A., Sasse, M. A., Taiming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications. *Proceedings of ACM Multimedia'99.*

Mul89 Mullender, S., Protection in S. Mullender (ed.) Distributed Systems. *Addision Wesley*, 1989

Doh94 Stephane Doheny-Farina, S., The Last Link's article on Ubiquitous Computing. *Computer-Mediated Communication Magazine*, Volume 1, Number 6, October 1, 1994, Page 18.

Lan92 Langley, P., User modeling in adaptive interfaces. *Proceedings of the Seventh International Conference on User Modeling*. Banff, Alberta: Springer. 1992

AbM00 Abowd, G., D., Mynatt, E., D., Charting Past, Present, and Future Research in Ubiquitous Computing. *ACM Trans. Comput.- Hum. Interact.* 7, 1 (Mar. 2000) 29-58

Fin96 Finger, S., *et al*. Rapid Design and Manufacture of Wearable Computers. *Commun. ACM 39*, 2 (Feb 1996), 63-70

Vol00 Volokh, E., Deep issues: personalization and privacy. Comm. ACM 43, 8 (Aug 2000), 84-88

Mil95 Milberg, S., J., *et al.* Values, privacy, personal information and regulatory approaches. *Commun. ACM 38*, 12 (Dec. 1995), 65-74

Man96 Mann, S., Smart clothing: Wearable multimedia computing and personal imaging to restore the technological balance between people and their environments. *Proceedings of the fourth ACM international conference on Multimedia*, 1996, 163-174

Wan92 Want, R., *et al*. The Active Badge Location System. *ACM Trans. Inf. Syst. 10*, 1 (Jan 1992), 91-102

Lam97 Lamberg, A., *et al*. Yksityisyys ja sananvapaus tietoverkoissa, Tietotekniikan kehittämiskeskus ry (Tieke) (http://www.tieke.fi/arkisto/tiveke/Fin96ortit/yksislyh.htm)

Lai00 Lainsäädäntö, Tietosuojavaltuutetun toimisto (http://www.tietosuoja.fi/1556.htm)