# Loppuraportti

Yksilönsuoja langattomassa viestinnässä: esineiden internet
1.6.2012–31.5.2014

Johanna Virkki
Tampereen teknillinen yliopisto, Elektroniikan ja tietoliikennetekniikan laitos

## 1. Tutkimuksen lähtökohta

Internet liittää yhteen miljardeja tietokoneiden ja mobiililaitteiden käyttäjiä. Yksi keskeisimpiä ilmiöitä tulevassa kehityksessä on asteittainen siirtyminen esineiden internetiin (Internet of Things), jossa myös esineet ja laitteet viestivät ja toimivat ihmisten kanssa ja keskenään. Esimerkiksi autot, lääkepakkaukset, rakennukset ja kodin elektroniikkalaitteet osallistuvat aktiivisesti tapahtumiin ja tiedonsiirtoon. Onkin kiinnostavaa nähdä, mitkä esineiden internetin sovellukset tulevat saavuttamaan paikan jokapäiväisessä elämässämme. Vaikka esineiden internet auttaakin ratkaisemaan monia ongelmia ja helpottaa elämää aivan uusilla tavoilla, se tuo tullessaan myös uudenlaisia haasteita. Yksi tärkeimmistä haasteista on yksilönsuojan säilyminen. Suuri vaikutus esineiden internetin käyttöönottoon, leviämiseen ja mahdollisuuksiin tulee olemaan sillä, uskovatko käyttäjät yksilönsuojaan esineiden internetissä. On myös kiinnostavaa seurata, miten tällainen kaikkialla läsnä oleva viestintäverkosto tulee vaikuttamaan yksityisyyden käsitteeseen. Muutos entiseen on jo tapahtunut, kiitos tietokoneiden, mobiililaitteiden ja internetin sosiaalisten verkkoviestintäyhteisöjen. Tässä tutkimuksessa keskityttiin selvittämään, mikä on yksilönsuojan merkitys esineiden internetin ja internetin verkkoviestintäyhteisöjen nykyisille ja tulevaisuuden potentiaalisille käyttäjille.

## 2. Tutkimuksen kulku

Aluksi tutkimuksessa selvitettiin haastattelujen avulla suomalaisten ajatuksia nykyhetken ja tulevaisuuden langattomasta viestinnästä ja erityisesti heidän asenteitaan tulevaisuuden kaikkialla läsnä olevaa verkkoympäristöä kohtaan. Tavallisten suomalaisten ihmisten lisäksi haastateltiin langattoman viestinnän ja esineiden internetin kanssa työskenteleviä ihmisiä eri yliopistoista ja yrityksistä Suomessa ja Kiinassa. Suomessa tutustuttiin Tampereen teknillisessä yliopistossa useiden tutkimusryhmien tutkimusaiheisiin ja keskusteltiin tutkijoiden kanssa. Erityisesti keskityttiin heidän ajatuksiinsa yksilönsuojasta erilaisissa esineiden internetin sovelluksissa. Lisäksi tutkimuksen ensimmäiseen vuoteen sisältyi tutkijavierailu Nanjingiin, Kiinaan (Research Center of Wireless Communication and Information Security, Southeast University, Kiina, 23.9.2012–5.11.2012). Tutkijavierailun tarkoituksena oli tutustua kiinalaisten tutkimusryhmien työhön kyseisessä tutkimuskeskuksessa ja keskustella tutkijoiden kanssa yksilönsuojasta tulevaisuuden langattomassa viestinnässä ja esineiden internetissä. Tutkijavierailun aikana toteutettiin myös haastatteluja, joita tehtiin Southeast Universityn tutkimuskeskuksen lisäksi kiinalaisten alan tutkijoiden ja toimijoiden keskuudessa konferenssissa Wuxissa (International Conference on the Internet of Things, 24.10.2012–26.10.2012). Tästä aiheesta on julkaistu kaksi artikkelia:

- *J. Virkki, Finnish Perspectives for the IOT, American Journal of Networks and Communications, Volume 2, Issue 2, 2013, pp. 23–27.*
  Artikkelissa esitellään tuloksia Suomessa tehdyistä tavallisten ihmisten (11 haastateltavaa) ja langattoman viestinnän kanssa työskentelevien ihmisten (11 haastateltavaa) haastatteluista.
- *J. Virkki and L. Chen, Personal Perspectives: Individual Privacy in the IOT, Advances in Internet of Things, Volume 3, Issue 2, 2013, pp. 21–26.*
  Artikkelissa esitellään tuloksia Suomessa (11 haastateltavaa) ja Kiinassa (11 haastateltavaa) tehdyistä langattoman viestinnän kanssa työskentelevien ihmisten haastatteluista.
- Tutkimuksessa saatujen tulosten mukaan suurin osa haastatelluista ihmisistä uskoi esineiden internetin tulevan osaksi jokapäiväistä elämäämme ja monet esineiden internetin sovellukset

nähtiin houkuttelevina. Toisaalta vastauksissa kyseenalaistettiin se, onko kaikille esineiden internetin sovelluksille todellista tarvetta. Ihmiset, joiden työ liittyi langattoman viestinnän tai esineiden internetin kehitykseen, olivat tavallisia ihmisiä kriittisempiä esineiden internetiä kohtaan ja huolestuneempia yksilönsuojasta siinä. Lisäksi kiinalaiset vastaajat olivat yleisesti enemmän huolissaan yksilönsuojasta kuin suomalaiset vastaajat. Ongelmat turvallisuuden ja yksityisyydensuojan kanssa ja mahdottomuus itse kontrolloida sovellusten käyttöä nousivat esiin tulevaisuuden haasteina. Lisäksi esiin nousi jo olemassa olevia ongelmia yksilönsuojaan liittyen.

Seuraavaksi keskityttiin tarkemmin esineiden internetin muutamaan esimerkkisovellukseen. Puettava elektroniikka on tärkeä osa tulevaisuuden kaikkialla läsnä olevaa verkkoympäristöä, ja sillä on valtava määrä mahdollisia sovelluksia. Aluksi tutkimuksessa selvitettiin suomalaisten ajatuksia puettavan elektroniikan käytöstä terveydenhuolto- ja lastenhoitosovelluksissa, erityisesti yksilönsuojan näkökulmasta. Tämä osio toteutettiin seuraamalla asiasta käytävää internetkeskustelua (keskusteluja myös aloitettiin itse useilla keskustelufoorumeilla) ja tekemällä haastatteluja. Tutkimuksessa tehtiin yhteistyötä Aston Universityn tutkijan Rebecca Aggarwalin kanssa (Aston University, Iso-Britannia). Hän teki haastatteluja Isossa-Britanniassa, ja näin tutkimuksessa pystyttiin vertaamaan haastattelujen tuloksia näissä kahdessa maassa. Tästä aiheesta on julkaistu kaksi artikkelia:

- *J. Virkki and P. Raumonen, Perspectives for Wearable Electronics in Healthcare and Childcare, E-Health Telecommunication Systems and Networks, Volume 2, Issue 3, 2013, pp. 58–63.*
  Artikkelissa esitellään tuloksia suomalaisten ihmisten haastatteluista (24 haastateltavaa) ja seuratuista internetkeskusteluista.
- *J. Virkki and R. Aggarwal, Privacy of Wearable Electronics in the Healthcare and Childcare Sectors: A Survey of Personal Perspectives from Finland and the United Kingdom, Journal of Information Security, Volume 5, Issue 2, 2014, pp. 46–55.*
  Artikkelissa esitellään ja vertaillaan tuloksia suomalaisten (24 haastateltavaa) ja isobritannialaisten (21 haastateltavaa) ihmisten haastatteluista.
- Tutkimuksen tulosten mukaan suurin osa ihmisistä Suomessa ja Isossa-Britanniassa koki puettavan elektroniikan käytön terveydenhuolto- ja lastenhoitosovelluksissa positiivisesti. Ajatukset Isossa-Britanniassa olivat hieman positiivisempia kuin Suomessa. Mitä enemmän puettaviin sovelluksiin lisättiin tietoa langattomasti luettavaksi, sitä negatiivisemmiksi asenteet tulivat molemmissa maissa. Tutkimuksessa nousi esiin monenlaisia huomioita, jotka liittyivät esimerkiksi lasten turvallisuuteen, yksilönsuojaan, mahdollisuuteen jättäytyä näiden sovellusten ulkopuolelle ja nykyisten teknologioiden mahdollisuuksiin. Puettavan elektroniikan käyttöönotto terveydenhuolto- ja lastenhoitosovelluksissa tarjoaa valtavasti mahdollisuuksia mutta vaatii monialaista tutkimus- ja kehitystyötä.

Seuraaviksi esimerkkisovelluksiksi valittiin älykodit ja älykkäät autot, jotka molemmat ovat olleet paljon esillä mediassa esineiden internetin yhteydessä. Kesällä 2014 kaksi kiinalaista opiskelijaa, Yu Zhai ja Yan Liu (City University of Hong Kong, Kiina), suoritti kansainvälisen harjoittelunsa Tampereen teknillisessä yliopistossa ja työskenteli tässä tutkimusprojektissa kesän ajan. He keskittyivät työssään älykoteihin ja älykkäisiin autoihin. Opiskelijat haastattelivat eurooppalaisia ja aasialaisia ihmisiä henkilökohtaisten haastattelujen ja internetkyselyn avulla ja keräsivät heidän mielipiteitään näistä sovelluksista ja yksilönsuojan merkityksestä niissä. Tästä aiheesta on julkaistu kaksi artikkelia:

- *Y. Liu, Y. Zhai, M. Yang, F. Long, and J. Virkki, Personal Perspectives for Smart Vehicles and Driving, Journal of Emerging Trends in Computing and Information Sciences, Volume 5, Issue 9, 2014, pp. 682–689.*
  Artikkelissa esitellään haastattelujen (95 haastateltavaa) ja internetkyselyn (153 vastaajaa) tuloksia liittyen älykkäisiin autoihin.
- *Y. Zhai, Y. Liu, M. Yang, F. Long, and J. Virkki, A Survey Study of the Usefulness and Concerns about Smart Home Applications from the Human Perspective, Accepted to be published in Open Journal of Social Sciences, Volume 2, Issue 11, 2014.*
  Artikkelissa esitellään haastattelujen (95 haastateltavaa) ja internetkyselyn (153 vastaajaa) tuloksia liittyen älykoteihin.
- Saaduista tuloksista huomattiin ensimmäiseksi, että ihmisillä on hyvin erilaisia ajatuksia siitä, mitä termeillä ”älykoti” ja ”älykäs auto” tarkoitetaan ja millaisia vaikutuksia niillä voisi olla jokapäiväiseen elämään. Suurin osa vastaajista oli halukkaita asumaan älykodissa ja ajamaan älykkäällä autolla. Hinta ja luotettavuus nousivat päällimmäisiksi huolenaiheiksi, ja aasialaiset vastaajat olivat yleisesti enemmän huolissaan kuin eurooppalaiset vastaajat. Yksilönsuoja älykodeissa ja älykkäissä autoissa huolestutti sekä eurooppalaisia että aasialaisia vastaajia.

Tutkimusprojektin viimeinen pääteema liittyi yksilönsuojaan sosiaalisessa mediassa. Aluksi tutkimuksessa tutustuttiin aiheesta käytävään keskusteluun internetin keskustelupalstoilla ja keskusteluja aiheesta aloitettiin myös itse. Kesällä 2013 kiinalainen opiskelija Chi Kin Chan (City University of Hong Kong, Kiina) suoritti kansainvälisen harjoittelunsa Tampereen teknillisessä yliopistossa ja työskenteli kesän ajan tässä tutkimusprojektissa. Hän keskittyi tutkimaan tiedon jakamista ja yksilönsuojaa sosiaalisessa mediassa ja keräsi kiinalaisten ja suomalaisten ihmisten ajatuksia aiheista. Tutkimuksensa hän teki henkilökohtaisia haastatteluja ja internetkyselyä käyttäen. Tästä aiheesta on julkaistu kaksi artikkelia:

- *C.K. Chan and J. Virkki, Perspectives for Sharing Personal Information on Online Social Networks, Social Networking, Volume 3, Issue 1, 2014, pp. 41–49.*
  Artikkelissa esitellään haastattelujen ja internetkyselyn (yhteensä 50 vastaajaa) avulla kerättyjä tuloksia omien ja muiden ihmisten henkilökohtaisten tietojen jakamisesta sosiaalisessa mediassa.
- *J. Virkki and C.K. Chan, Perspectives for Sharing Photos of Children Online, Journal of Social Sciences, Volume 3, Issue 2, 2014, pp. 357–366.*
  Artikkelissa esitellään internetin keskustelupalstoilla esiin tulleita mielipiteitä ja haastattelujen ja internetkyselyn (yhteensä 50 vastaajaa) avulla kerättyjä tuloksia lasten kuvien jakamisesta sosiaalisessa mediassa.
- Saatujen tuloksien mukaan suurin osa vastaajista käyttää sosiaalista mediaa päivittäin ja jakaa henkilökohtaisia tietojaan internetissä. Puolet vastaajista jakaa tietoa myös muista ihmisistä. Tulosten mukaan naispuoliset vastaajat jakavat aktiivisemmin tietoa muista ihmisistä kuin miespuoliset vastaajat, myös kysymättä siihen tietojen omistajan lupaa. Vastauksien perusteella vain pieni osa ihmisistä käyttää sosiaalista mediaa saadakseen uusia ystäviä. Sen sijaan tärkein syy näiden verkkoviestintäyhteisöjen käyttämiseen on se, että nykyiset ystävät käyttävät niitä. Vastauksista selvisi myös, että monet ihmiset näkevät internetin olennaisena osana nykymaailmaa ja kokevat, että se yksityisyyden taso, joka heillä on internetissä, on sama yksityisyyden taso, joka heillä on muutenkin elämässään.

## 3. Rahoituksen käyttö ja tulokset

Helsingin Sanomain Säätiön apuraha käytettiin pääasiassa henkilökohtaisena palkkana, artikkelien julkaisukustannuksiin ja tutkijavierailun kustannuksiin. Tutkimus eteni hyvin, esiin nousi mielenkiintoisia näkökulmia, ja saadut tulokset antavat erittäin hyvän pohjan jatkotutkimukselle. Saavutetut tulokset ovat erityisesti esineiden internetin ja sen sovellusten kehityksen kanssa työskentelevien hyödynnettävissä. Tuloksia on hyödynnetty myös opetuksessa Tampereen teknillisessä yliopistossa. Tämä loppuraportti tutkimuksesta julkaistuine vertaisarvioituine artikkeleineen toimitettiin Helsingin Sanomain Säätiölle marraskuussa 2014.

**American Journal of Networks and Communications**
2013; 2(2) : 23-27
Published online April 2, 2013 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20130202.11

SciencePG
Science Publishing Group

# Finnish perspectives for the IOT

**Johanna Virkki**

Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland

**Email address:**
johanna.virkki@tut.fi (J. Virkki)

**To cite this article:**
Johanna Virkki. Finnish Perspectives for the IOT, *American Journal of Networks and Communications.* Vol. 2, No. 2, 2013, pp. 23-27. doi: 10.11648/j.ajnc.20130202.11

**Abstract:** The Internet of Things (IOT) means connecting people, things, and devices in order to create an omnipresent computing world. One of the most important challenges in convincing users to adopt this kind of all-around network is the protection of security and privacy in different applications. This paper presents the results of interviews conducted in a Finnish study during 8/2012-2/2013. In this research, 11 Finnish people working with different aspects of IOT development and 11 ordinary Finnish people were interviewed. The goal was to investigate their feelings on the IOT and its applications, as well as personal opinions on security and individual privacy in the IOT. Most of the answerers in this study believed that we are heading towards the IOT in the future and many IOT applications were seen tempting. However, security and privacy issues, the lack of control, and the actual need for versatile IOT applications were questioned. The people working with the IOT were found to be more critical towards the IOT than the ordinary people. An introduction of the IOT, examples of potential applications, the conducted interviews and collected answers, as well as highlights of the collected free comments are presented in this paper.

**Keywords:** Finland, Individual Privacy, Internet Of Things, Interviews, Security

## 1. Introduction

The Internet of Things (IOT) is a conceptual vision to connect things (everyday things from school buildings to coffee cups) and devices (from laptops to ovens), in order to create a ubiquitous computing world. Things will exchange data and information about the environment, while reacting autonomously to different events, influencing the environment, and creating services. This all can happen with or without human intervention. The IOT is thus the extension of the Internet to the next level, i.e., bringing the Internet to the real physical world of things. Potential examples of the versatile applications of the IOT are presented next.

Given that a growing number of people have chronic diseases and inconveniences, health-related applications of the IOT are gathering more and more attention. Potential applications include e.g. assistance and monitoring of conditions of patients inside hospitals and at home, and accident victim’s medical journals that are automatically made available to the caregivers to ensure that optimal treatment can be provided. Electronic tags can be used in drugs and drug boxes can carry information on adverse effects and optimal dosage, monitor the use, inform the pharmacist when new supply is needed, know incompatible drugs, and prevent overdoses. The IOT also offers many applications to home-environment, for example automatic energy and water supply consumption, control of temperature gauges, remotely armed home security system, switching appliances on and off, etc. Possible retail applications include e.g. payment processing based on location or duration and allowing customers to pay in department stores only by walking out with the products. Customers can also receive advices in the point of sale according to customer habits, preferences, presence of allergic components, or expiring dates. Also smart cities are examples of the potential future IOT applications; for example, the citizens can monitor the pollution concentration and can receive automatic alarms when the radiation level reaches too high level, rubbish bins can send an alarm to garbage collector when they are close to being full, etc. The IOT also has many potential applications in catastrophic prevention, for example detection and warning of forest fires and earthquake, and monitoring of vibrations and material conditions in buildings and bridges [1-6].

A number of countries or districts have realized the importance of the IOT in the recovery of economic growth and sustainability. Amongst them the European Union (EU), the United States, and China are prominent examples. Thus, companies, universities, and research institutions currently take an active part in IOT development worldwide [7].

One of the most important challenges in convincing users to adopt this kind of all-around network is the protection of security. And it is not only security, but privacy too. Concerns over security and privacy can spread wide, particularly as wireless systems can track users' personal information, actions, behaviour and ongoing preferences. Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data. The huge volumes of data that the IOT generates will have to be routed, captured, analysed, and acted upon in timely relevant ways. Working out how to do this will be no easy task. One important issue related to these different applications is the data aggregation (combining seemingly non-sensitive separate small bits of information may reveal additional, possibly sensitive information) [8]. Similar effect can occur when the data collected for one purpose is used for a different purpose, and this is done without the person's approval. As the devices and things within the IOT collect seemingly inconsequential fragments of data for their service, it should also be considered what happens when all that information is brought together, correlated, and reviewed. The sheer scale and capacity of the new technologies will magnify this problem and source suspect. Thus, security and privacy of the IOT are currently active and important research topics [2-7, 9-14].

Interesting point of view are the differences and similarities in personal thoughts of people who work with the development of the IOT and of those people, who are not yet so familiar with the concept, but are potential end users of the IOT (henceforth referred to as "ordinary people"). In this research, 22 people were interviewed in Finland during a period of 7 months, 8/2012-2/2013, in order to investigate their thoughts and feelings on the Internet and individual privacy, as well as their opinions on the IOT and its applications.

This paper is organized as follows: The introduction section introduces the concept of the IOT and gives examples of potential applications. Section 2 presents the performed interviews, including the information on the answerers and presented questions. The collected answers and examples from free comments are presented and discussed in section 3. The last section summarizes the results and presents the conclusions of this paper.

## 2. Interviews

For this research, 11 people working with different aspects of the IOT, e.g. radiofrequency identification, wireless networks, and wireless communication were interviewed. These answerers were chosen from different organizations (from researchers of different universities in Finland and from workers of companies on the field). Also, 11 ordinary people, working in very different areas, were interviewed. The idea of this research study is not only to compare the answers from these two different groups but to gather more versatile answers by interviewing people with different backgrounds. Thus, people of different age and people of both gender were chosen (the genders and ages of the answerers can be seen in Table 1). The personal interviews were conducted by an associate of the researcher, and they took place either at the answerers working facility, home, or at a neutral, public place. Some of the interviews were done by private e-mails between the researcher and the answerer. All these interviews thus had more flexibility than only a paper survey, as both the researcher and the answerer were able to ask for clarification. This survey had 5 questions and a possibility for free comments. Questions are listed next.

***Table 1.*** *Genders and ages of the answerers.*

| | Ordinary people | People working with the IOT |
|---|---|---|
| **N of female** | 5 | 6 |
| **N of male** | 6 | 5 |
| **N total** | 11 | 11 |
| **Min. age** | 19 | 20 |
| **Average age** | 32 | 32 |
| **Max. Age** | 56 | 48 |

Question 1: Are you currently using social media and/or do you share pictures or personal information on yourself in the Internet?

·Yes, many times in a week

·Yes, sometimes

·No

Question 2: How much do you think a person can currently affect his/her own individual privacy in the Internet? Scale = 1-5, where

·1= A person can completely control his/her own individual privacy

·5= A person has no control over his/her own individual privacy

Question 3: What kinds of IOT applications do you see potential in your own life? What kinds of IOT applications you would not want into your own life?

Question 4: Do you believe that current Internet will grow into IOT and this kind of all-around network will come to use? What will be the schedule?

·In the near future

·During following 10 years

·During following 20 years

·Longer than 20 years

·Never

Question 5: How much do you think a person can affect his/her own individual privacy in the Internet/IOT after 10 years from now? Scale = 1-5, where

·1= A person can completely control his/her own individual privacy

·5= A person has no control over his/her own individual privacy

## 3. Results and Discussion

This section introduces and discusses the collected answers. All the examples of the achieved free comments are presented as direct quotes and their text is italicized.

### *3.1. Question 1*

Social media refers to the means of interactions among people in which they create, share, and exchange information in virtual communities and networks. It allows users to share their lives in many different ways, via updates, images, voice, etc. Social media is more and more becoming a platform for the public to voice their opinion and present them to a huge audience in the Internet. Many people have chosen to make their life, at least partly, public. In Question 1, it was asked if the answerers are currently using social media and/or share pictures or personal information of themselves in the Internet. The answers to this question (shown in Fig. 1) show that 73 % of all the answers were “many times a week” or “sometimes”, and 27 % of all the answers were “no”. There were significantly more “no” answers among the people that work with the IOT: 91 % of the ordinary people answered “many times a week” or “sometimes”, whereas among the people working with the IOT, 55 % answered “many times a week” or “sometimes”. Also, in their free comments, people working with the IOT were more critical towards the use of social media.

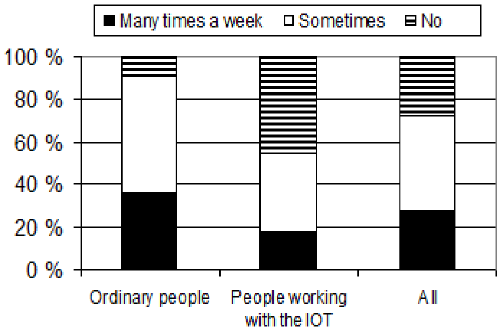

***Figure 1.*** *Results from Question 1; Are you currently using social media and/or do you share pictures or personal information on yourself in the Internet?*

“I have not opened a Facebook or Google account, neither I am using any online photo storages or backup services, while there are benefits also. In these cases I see privacy concerns and legal complications more substantial than benefits.”

“There really is no information available about what kinds of security methods they’re using in many of the social media applications. Why would I want to use (with my own personal information!) something that I have no idea of?”

### *3.2. Questions 2 and 5*

Questions 2 and 5 dealt with the feelings on how much people can currently/after 10 years affect their own individual privacy in the Internet (results can be seen in Fig. 2 and Fig. 3, respectively). According to these answers, people believe that the possibility of moving from the traditional Internet towards the IOT during the following 10 years will not significantly affect how much they can control their individual privacy in the Internet. However, some answerers from both groups do believe for a negative change, which can be seen from the differences between Fig 2 and Fig 3. The average value of all the answers to Question 2 was 2,64 and the average value of all the answers to Question 5 was 3,18. Thus, according to these results, people already feel that there is a lack of control related to the individual privacy in the Internet. This was also pointed out in the free comments. A lot of work is currently done to maintain and improve the security and privacy in the Internet, which was also mentioned.

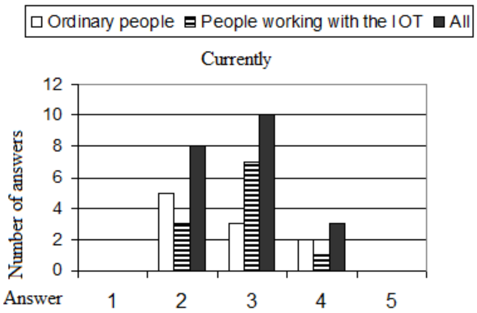

***Figure 2.*** *Results from Question 2; How much do you think a person can currently affect his/her own individual privacy in the Internet?*

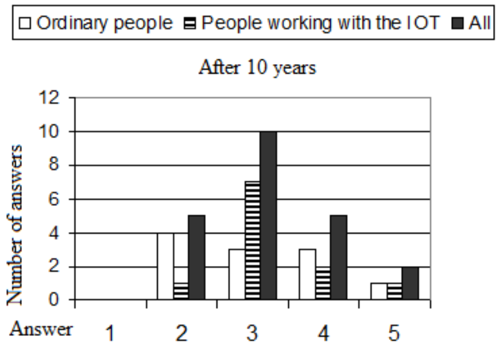

***Figure 3****. Results from Question 5; How much do you think a person can affect his/her own individual privacy in the Internet after 10 years?*

“Everything you share can come public information but that is the case with old fashion communication also.“

“I find the individuals privacy quite poor and therefore wish a lot higher security before IOT is everywhere more than it already is.”

“Nowadays there are a lot of problems with the security. I know that they are working to improve it. I just hope that they succeed..”

“I do not want to use applications that have security risks or applications that mean I may lose my privacy. I will not want to use them in the future either, no matter how great things anyone promises.”

### *3.3. Question 3*

As was described in the first section of this paper, the range and diversity of IOT applications permeates practically through all aspects of the everyday life. Question 3 was about the IOT applications that the answerers see potential in their own life in the future, and those they would not want into their life. The most wanted applications among these answerers seem to be those related to healthcare, e.g. automatic health-monitoring. This seems reasonable, since the adjustment of the healthcare systems to the increasing number of elderly and patients with chronic diseases is one of the biggest challenges to the EU, including Finland, and the future of the public healthcare is currently a hot topic in the Finnish media.

"Monitoring of my own health and the health of those close to me"

"From personal and professional point of view, elderly people more often benefit of staying at their own home as long as possible, where this kind of monitoring can be useful."

Also, versatile applications to be used at home were seen tempting. These applications also probably are the ones most commonly mentioned with the IOT. Thus, they may be the applications that the people are the most familiar with. In general, very different kinds of applications were mentioned to be considered helpful in everyday life.

"Energy and water supplies consumption monitoring. It helps to save money."

"Cloud storage of media so that it can be accessed and used anytime and anywhere"

"Remote control of home applications"

"IOT brings lot of new possibilities for social life and business."

The lack of control was seen as the main reason why some applications were not considered desirable. It was also questioned if the cost of using different applications will be suitable. Again, negative perspectives and feelings were mentioned more often in the answers collected from the people that work with the IOT.

"Those that will help, but not cause substantial privacy concerns or other risks. This is a matter of balance, meaning that if benefits are substantial then more risks can be accepted. E.g. I am using sometimes navigation applications on the phone while knowing that the data can be tracked."

"Controlling things, like photo based recognition, or something what will happen without my knowledge."

"Systems that I cannot control or modify myself"

"I also do not want that the systems carry permanent individual information without a possibility to erase."

"I would not feel comfortable with a home alarm or smart home system connected or controllable through the Internet. Such case is especially if the authentication is not strong, e.g. based just on password and user name. Also the potential damage is essential. For example, if you can turn the heating completely off during the winter time, I would not use such application. Also you should be able to bypass locally the Internet application in case of misuse or other problems."

### *3.4. Question 4*

In Question 4, it was inquired what people think will be the possible schedule for the current Internet to grow into the IOT and this kind of all-around network to come to use, if it will come to use. The answers to this question can be seen in Fig. 4. According to these results, 18 % of the answerers felt that this will happen during the following 10 years, 18 % during the following 20 years, and 14 % of the answerers felt that it will take longer than 20 years. In addition, two of the answerers (both working with the IOT) felt that this growing into the IOT will never happen. There was also one answerer from the group of ordinary people who felt that this will happen in the near future.

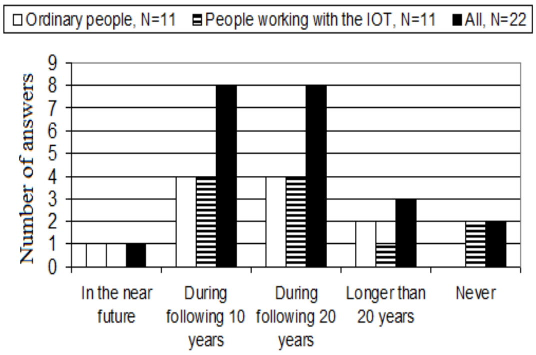

***Figure 4.*** *Results from Question 3; Opinions on the possible schedule for current Internet to grow into IOT and this kind of all-around network to come to use.*

"It is quite hard to know the schedule. There already are applications that I think are part of the IOT. On the other hand, it seems something that will happen in the far away future. For example, now everybody has a computer and a cellular phone in Finland. This was not the case 25 years ago. I do not think they would have predicted this"

In the free comments, the IOT was seen tempting, in principle, but the necessity of the versatile applications was also questioned:

"All in all, I expect much more positive consequences than negative ones. Life becomes easier and IOT is continuously learning more and more on us, our habits, preferences and the environment we live in. However, it may also be bad for individual decision making, since IOT may decide options or make the final decision. We may trust too much on the guidance of IOT. Therefore strict personal profiles for the applications of IOT are needed. Therefore, we must be active users not lazy followers."

"Nowadays people believe that they need loads of stuff. In reality we could survive with a lot less."

In addition, it was questioned (both by the ordinary people and the people working with the IOT) if people are aware of the potential problems that may occur.

"It's scary how few people are preparing for the IOT."

“Orwell's 1984 is here.”

## 4. Conclusion

In this research, 22 people were interviewed about the IOT in Finland. Out of the 22 answerers, 11 were working with the IOT and 11 were ordinary people, who were not yet so familiar with the concept. This paper presents the collected answers to 5 questions and highlights of the free comments. Most of the answerers believed that we are heading towards the IOT in the future. According to these answers, many future IOT applications were seen tempting, but the necessity of the huge amount of new applications was also questioned. In addition, the security risks and losing control your own individual privacy were seen as the main barriers, as was expected. The most desired applications seem to be those related to health-monitoring and applications used at home. In general, the people working with the IOT were found to be more critical towards it.

## Acknowledgements

Johanna Virkki would like to thank the Helsingin Sanomat Foundation.

## References

[1] Libelium, “50 Internet of Things applications”, 2012. Available at: http://www.libelium.com/top_50_iot_sensor_applications_ranking (accessed 20 February 2013).

[2] The Internet of Things 2012 - New Horizons -Cluster Book 2012. Available at: http://www.Internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf (accessed 20 February 2013).

[3] Commission of the European Communities, Internet of Things — An Action Plan for Europe, 2009. Available at: http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf (accessed 19 February 2013).

[4] Internet of Things - Pan European Research and Innovation Vision-IERC 2011. Available at: http://www.Internet-of-things-research.eu/pdf/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011_web.pdf (accessed 20 February 2013).

[5] European Commission, Information Society and Media, Internet of Things in 2020 Roadmap for the Future, 2008. Available at: http://www.iot-visitthefuture.eu/fileadmin/documents/researchforeurope/270808_IoT_in_2020_Workshop_Report_V1-1.pdf (accessed 12 February 2013).

[6] The 2nd Annual Internet of Things Europe 2010: A Roadmap for Europe' Conference Report, 2010. Available at: http://ec.europa.eu/information_society/policy/rfid/documents/iotconferencereport2010.pdf (accessed 15 January 2013).

[7] The Strategic Centre for Science, Technology and Innovation in the Field of ICT, Internet of Things Strategic Research Agenda http://www.Internetofthings.fi/

[8] D.J. Solove, "'I've got nothing to hide' and other misunderstandings of privacy” San Diego Law Review, Vol. 44, 2007, GWU Law School Public Law Research Paper No. 289.

[9] Futuretech Alert. Technology Convergence Leading To the Internet of Things, Frost & Sullivan, 2012.

[10] L. Wu and P. Shao, “Research on the protection algorithm and model of personal privacy information in internet of thing”, International Conference on E -Business and E -Government, 2011.

[11] H. Feng and W. Fu, “Study of recent development about privacy and security of the Internet of Things, International Conference on Web Information Systems and Mining, 2010.

[12] D. Gessner, A. Olivereau, A.S. Segura, A. Serbanati, “Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things”, International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[13] V. Oleshchuk “Internet of things and privacy preserving technologies”, International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009.

[14] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future Internet of Things," Advances in Internet of Things, Vol. 2 No. 1, 2012, pp. 1-7. doi: 10.4236/ait.2012.21001.

# Personal Perspectives: Individual Privacy in the IOT

**Johanna Virkki[1], Liquan Chen[2]**
[1]Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
[2]School of Information Science and Engineering, Southeast University, Nanjing, China
Email: johanna.virkki@tut.fi, lqchen@seu.edu.cn

Received February 7, 2013; revised March 11, 2013; accepted March 22, 2013

## ABSTRACT

The Internet of Things (IOT) is the extension of the Internet to the next level, *i.e.*, bringing the Internet to the real physical world of things. In this research, 22 people working with different aspects of IOT development were interviewed in Finland and in China, in order to investigate their thoughts and personal opinions on the IOT and the individual privacy in the IOT. This paper presents the background of the IOT, interviews and collected answers, as well as highlights of collected free comments.

**Keywords:** China; Finland; Individual Privacy; Internet of Things; Interviews

## 1. Introduction

The Internet of Things (IOT) means connecting things and devices in order to create an omnipresent computing world. Things will exchange data and information about the environment, while reacting autonomously to different events, influencing the environment, and creating services with or without human intervention. The IOT is thus the extension of the Internet to the next level, *i.e.*, bringing the Internet to the real physical world of things. Possible applications of the IOT are versatile and some examples are presented next.

Health-related applications include e.g. assistance and monitoring of conditions of patients inside hospitals and old people at home. For example, a tiny, wearable device that can detect a person's vital signs and send an alert to a healthcare professional if a certain threshold is reached or if a person has fallen down. Also, when an accident occurs, the victim's medical journals are automatically made available to the ambulances to ensure that optimal treatment can be provided. Electronic tags can be used in drugs and drug boxes can carry information on adverse effects and optimal dosage, monitor the use, inform the pharmacist when new supply is needed, know incompatible drugs, and prevent overdoses. The IOT also offers many applications to home-environment, for example energy and water supply consumption monitoring in houses to save cost and resources, remotely armed home security system, control of temperature gauges, switching appliances on and off, controlling lightning, etc. Possible retail applications including e.g. payment processing based on location or duration in public transport allow customers to pay in department stores without using a cash desk, only by walking out with the products that have electronic tags, and advices in the point of sale according to customer habits, preferences, presence of allergic components, or expiring dates. The IOT has many potential applications in catastrophic prevention, for example, detection and warning of forest fires and earthquake and monitoring of vibrations and material conditions in buildings and bridges. In addition, smart cities and intelligent transportation are examples of potential future IOT applications [1].

The term "Internet of Things" was coined by Kevin Ashton, executive director of the Auto-ID Center, in 1999. Different definitions for the IOT have appeared and the term was evolving as the technology and implementation of the ideas move forward. A number of countries or districts have realized the importance of the IOT in the recovery of economic growth and sustainability. Amongst them, the European Union (EU), the United States, and China are prominent examples. Academia has a relatively long history of IOT research. The IOT research in China has a strong support from the government. Several research institutes have been, and currently are, involved in far-reaching, government-supported, projects. In Europe, the academic research work in the IOT has been largely performed in different EU-funded seventh Programme Framework (FP7) projects. To better utilize the research achievements and to provide a place to share expertise, in 2009, the European Research Cluster on the Internet of Things was founded. The industrial activities in the IOT started around the same time as the academia, though the corresponding products were very sparse the first several years [2]. Thus, a wide range of research and application projects have been set up in different application areas, the technical aspects of the future Internet are widely studied, and a lot of development work is done [2-5].

One of the most important challenges in convincing users to adopt this kind of all-around network is the protection of privacy [6-9]. Concerns over privacy can spread wide, particularly as wireless systems can track users' actions, behaviour and ongoing preferences. Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data. The sheer scale and capacity of the new technologies will magnify this problem and source suspect [10]. Privacy problems, nevertheless, are not caused by the technology alone, but primary through activities of people, businesses, and the government [11].

Several interesting survey studies have already been conducted. The results from an empirical study with 92 subjects indicated that the acceptance of IOT services is influenced by various contradicting factors, such as perceived privacy risks and personal interests. It was also assumed that legislation, data security and transparency of information influence the adoption behavior [12]. Also, a survey with 475 subjects, focusing on the activities and habits that people do at home that they would not want to be recorded, was conducted, and bedroom was found to be the most private place [13]. A study that investigated American, Chinese, and Indian social networking site users' privacy attitudes and practices, based on 924 responses, found the American respondents to be the most privacy concerned, followed by the Chinese and Indians, respectively [14].

While our work shares many similar objects to the work above, we focus only on the personal perspectives of the people who are working with different aspects of the development of the IOT, in two very different countries, in different parts of the world. In this research, people working with IOT research and development were interviewed in Finland (EU member) and in China, in order to investigate their personal feelings about the Internet and the individual privacy in the Internet today and in the future. In this study, the individual privacy refers to the evolving relationship between the technology and the legal right to, or public expectation of, privacy in the collection and sharing of data about one's self. This definition is used for both the Internet and the IOT.

## 2. Interviews

For this research, 22 people working with the research and development of the IOT, e.g. with wireless components/devices, wireless systems, Internet protocols, and mobile communications were interviewed. People of different age (the average age of the answerers was 28, the youngest answerer was 20 years old and the oldest answerer was 48 years old), of both gender (genders of the answerers can be seen in **Table 1**), and from different organizations (researchers of different universities in Finland and China, workers of companies on the field, and participants of an international conference) were chosen from Finland (11 people) and from China (11 people).

Personal interviews were conducted by an associate of the researcher, and they took place either at the answerers working facility or at a neutral, public place. Some of the interviews were done by private e-mails between the researcher and the answerer. All these interviews thus had more flexibility than only an anonymous paper survey as both the researcher and the answerer were able to ask for clarification. This study had 5 questions and a possibility for free comments. The idea of this research was not only to compare the answers from China and from Finland, but also to gather more versatile answers by making interviews in two very different countries. Questions are listed next.

Question 1: How much do you think a person can currently affect his/her own individual privacy in the Internet? Scale = 1 - 5, where

1 = A person can completely control his/her individual privacy;

5 = A person has no control over his/her individual privacy.

Question 2: How worried are you about individual privacy in the following Internet/IOT applications?

Scale = 1 - 5, where 1 = Not worried at all, 5 = Very worried.

- Personal health-related applications (e.g. your medical conditions, drugs, treatments);
- Personal finances-related applications (e.g. your account and credit information);
- Personal purchases-related applications (e.g. what did you buy, from where, how much did you spend);
- Personal communication-related applications (e.g. what did you communicate, when, with whom);

**Table 1. Gender and nationality of the answerers.**

| | China | Finland | All |
|---|---|---|---|
| **Female** | 7 | 6 | 13 |
| **Male** | 4 | 5 | 9 |
| **All** | 11 | 11 | 22 |

- Personal tracking-related applications (e.g. where are/were you).

Question 3: Do you believe that the current Internet will grow into the IOT and this kind of all-around network will come to use? What will be the schedule?

- In the near future;
- During the following 10 years;
- During the following 20 years;
- Longer than 20 years;
- Never.

Question 4: If you think that the current Internet will grow into the IOT in the future, do you feel that the use of at least some IOT applications will be mandatory so that it is very hard to stay out?

- Yes;
- No;
- I don't know.

Question 5: How much do you think a person can affect his/her own individual privacy in the Internet/IOT after 10 years from now? Scale = 1 - 5, where 1 = A person can completely control his/her individual privacy, 5 = A person has no control over his/her individual privacy.

## 3. Results and Discussion

Questions 1 and 5 dealt with the opinions and feelings on how much people can currently and after 10 years affect their own individual privacy in the Internet. Results can be seen in **Figures 1** and **2**, respectively. As can be seen, the answerers from Finland are currently less worried about the individual privacy in the Internet than the answerers from China. This is an unexpected result, since traditionally Finland is more of an individualistic society and thus values individual privacy, where as China is more of a collective society. Since the explanation to this result cannot be found from this survey, more research is definitely needed. According to these answers, people from both countries believe that moving from the traditional Internet towards the IOT during the following 10 years will not significantly affect how they can control their individual privacy in the Internet. Some answerers from Finland believe for a negative change, whereas some of the answerers from China believe that they might have even better control of their privacy in the Internet after 10 years. This is probably because a lot of work is currently done to improve the individual privacy in the Internet and also the awareness of people is rising. This was also seen in free comments from both countries:

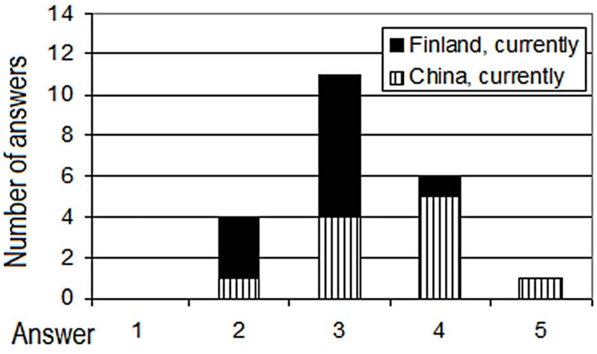

**Figure 1. Results from Question 1. Opinions on how much people can currently affect their individual privacy in the Internet.**

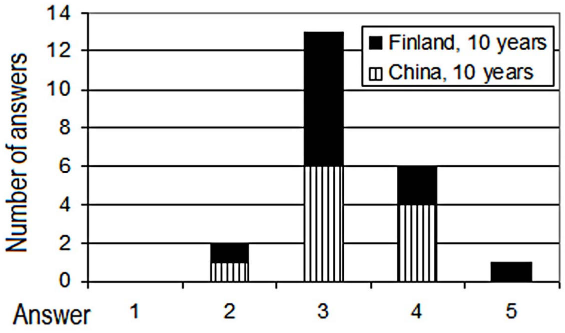

**Figure 2. Results from Question 5. Opinions on how much people can affect their individual privacy in the Internet after 10 years.**

"*New technology must strengthen, rather than undermine, the privacy of people.*"

"*Users should be able to monitor and control the security and privacy settings of all the devices that they own, some services should be accessible in an anonymous way, while others should require an explicit authentication or authorization of the user.*"

It is also probable that achieving this kind of high level individual privacy may first require some bad experiences:

"*Nowadays alertness of privacy issues and identity theft possibilities are increasing, regrettably, for the most part, by bad practice.*"

"*If we want to make good use of it (the IOT), we must make some strict policy to manage the use of it.*"

Question 2 inquired how worried the answerers are about individual privacy in different Internet/IOT applications. The application areas were chosen to be versatile areas from everyday life. Results from China and Finland can be seen in **Figures 3** and **4**, respectively. In China, personal finances related applications were clearly the ones that the answerers were most worried about. Salary and other aspects of personal finances are seen very private information in China and the future Internet applications must not affect this. Applications related to personal health were the least worrying ones and also the one and only lowest level of concern (1 = not worried at all) answer was nominated for this question. According to free comments from China, many applications were seen tempting, but safety must first be ensured. Also, it was questioned if the cost of applications in many areas

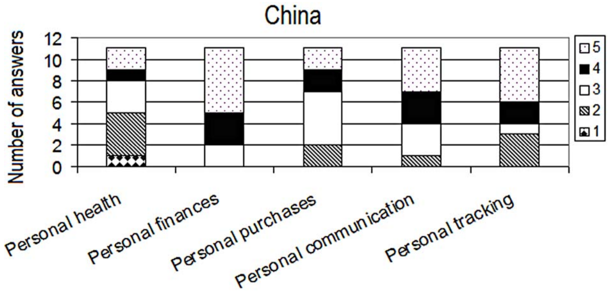

**Figure 3. Results from Question 2. Opinions on individual privacy in different Internet/IOT applications in China.**

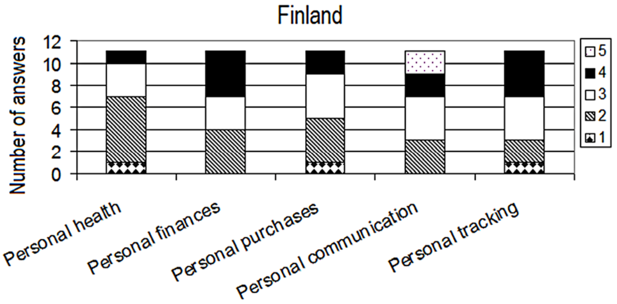

**Figure 4. Results from Question 2. Opinions on individual privacy in different Internet/IOT applications in Finland.**

will be too high.

"*Insuring the individual privacy is obviously the key point of popularizing the IOT*."

"*Seeing it as a possibility for new applications but also a lot of work must be done to safely implement them*."

"*Until the devices and services will become both cheap and safe*, *I will not let this kind of applications* (*home automation*) *enter my life*."

Again, unexpected results were achieved in this part, when the answerers from Finland were significantly less worried than the answerers from China. For example, in China, there were more than one nominations for the highest concern (5 = very worried) for all applications, whereas in Finland there were only two nominations for the highest concern at all, both in personal communication related applications. As in China, applications related to personal health were the least worrying ones also in Finland. It was stated in free comments that in healthcare, the most important thing is that all the vital information is available when needed. The future of the public healthcare is currently a hot topic in the Finnish media and thus also opposite opinions, pointing important issues, were presented in free comments. For example, in one comment from Finland, it was stated that there already are individual privacy problems related to personal health.

"*There is not enough control*, *who can truly view your healthy records as the cases of misuse in publicity indicate*."

"*I want all my information to be available to anyone who needs it when they take care of me*. *I also think future applications can improve the privacy in the healthcare*."

Thus, the effects of carefully designed and secured IOT applications to individual privacy in the future can also be positive. One important issue related to these different applications is the data aggregation (combining seemingly non-sensitive separate bits of information may well reveal additional, possibly sensitive, information) [15]. Similar effect can occur when data collected for one purpose is used for a different purpose without the person's approval. This was also made known in free comments:

"*Giving a small piece of information there and something small somewhere else does not seem bad*, *but what if somebody combines all information*? *And will I even know about that*?"

In Question 3, it was inquired what the answerers think will be the possible schedule for the current Internet to grow into the IOT and this kind of all-around network to come to use, if it will come to use. The answers to this question can be seen in **Figure 5**. According to these results, 41% of the answerers felt that this will happen during the following 10 years, 36% during the following 20 years, and 14% that it will take longer than 20 years. In addition, 9% of the answerers (all from Finland) felt that this growing into IOT will never happen. None of the answerers felt that this will happen in the near future. In free comments, the IOT was seen tempting but challenging. Also the necessity of versatile IOT applications was questioned in free comments.

"*I am interested in living in world with IOT*."

"*It is useful*, *but it is difficult*."

"*Are ordinary people willing to pay for all these great applications that are invented*?"

In Question 4, it was asked if the answerers feel that the use of at least some IOT applications will be mandatory in the future, so that it is very hard to stay out. The answers from China and Finland can be seen in **Figure 6**.

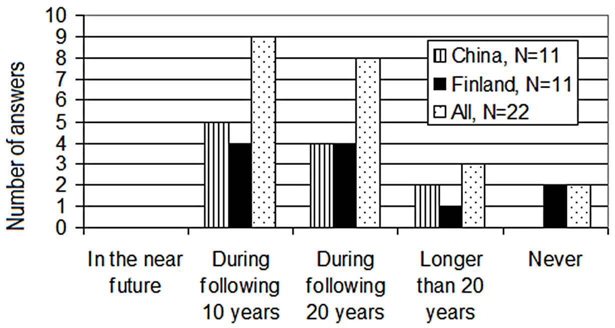

**Figure 5. Results from Question 3. Opinions on the possible schedule for the current Internet to grow into IOT and this kind of all-around network to come to use.**

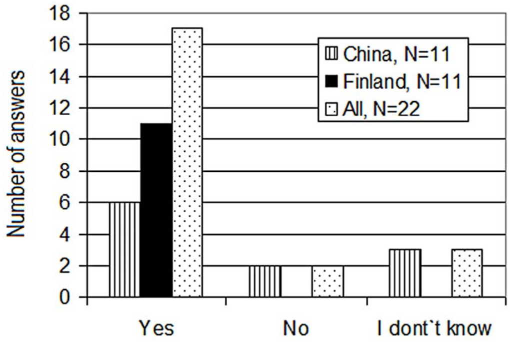

**Figure 6. Results from Question 4. Opinions on if the use of at least some IOT applications will be mandatory in the future.**

In China, 55% of the answerers felt that the IOT will be mandatory in some way. People in Finland were more concerted and all 11 answerers felt that the IOT will be mandatory in some way. It was also mentioned that the use of the Internet is already mandatory when living in Finland and thus this will also be the case in the future with the IOT. Also some feeling of helplessness was seen in free comments. Thus, unlike the people in Finland, some people in China feel that it is still possible to live without the Internet in China and this may also be possible in the future.

"*Living without Internet is already impossible in Finland*!"

"*It is also a matter of control. For example, I am not comfortable that anyone can track my personal contact details from my car's license number and I cannot do much about it*." (in Finland)

## 4. Conclusion

In this study, 22 people working with different aspects of research and development of the IOT were interviewed in Finland and in China, related to the IOT and the individual privacy in the IOT. This paper presents and discusses the collected answers and highlights of free comments. We feel that this research study brings a new perspective to this interesting research area. Most of the answerers believed that we were heading towards the IOT and in the future it would be mandatory to be part of it somehow. According to answers, many future applications were seen tempting, but they contained great risks and thus individual privacy must first be ensured. Also individual privacy problems today were stated. In general, the answerers from Finland were less worried about the individual privacy in the IOT than the answerers from China. This was an unexpected result and the reasons for this definitely required more research work. Next step is also to compare these answers with answers collected from normal people. This future research also has to involve significantly more answerers in order to achieve more meaningful results.

## 5. Acknowledgements

J. Virkki would like to thank the Helsingin Sanomat Foundation.

## REFERENCES

[1] Libelium, "50 Internet of Things Applications," 2012. http://www.libelium.com/top_50_iot_sensor_applications_ranking

[2] The Strategic Centre for Science, "Technology and Innovation in the Field of ICT, Internet of Things Strategic Research Agenda." http://www.Internetofthings.fi/

[3] Futuretech Alert, "Technology Convergence Leading to the Internet of Things," Frost & Sullivan, Mountain View, 2012.

[4] "The Internet of Things 2012—New Horizons-Cluster Book," 2012. http://www.Internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf

[5] European Commission, Information Society and Media, "Internet of Things in 2020 Roadmap for the Future," 2008. http://www.iot-visitthefuture.eu/fileadmin/documents/researchforeurope/270808_IoT_in_2020_Workshop_Report_V1-1.pdf

[6] L. Wu and P. Shao, "Research on the Protection Algorithm and Model of Personal Privacy Information in Internet of Thing," *International Conference on E-Business and E-Government*, Guiyang, 6-8 May 2011, pp. 1-4.

[7] H. Feng and W. Fu, "Study of Recent Development about Privacy and Security of the Internet of Things," *International Conference on Web Information Systems and Mining*, Beijing, 23-24 October 2010, pp. 91-95.

[8] D. Gessner, A. Olivereau, A. S. Segura and A. Serbanati, "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things," *International Conference on Trust, Security and Privacy in Computing and Communications*, Heidelberg, 25-27 June 2012, pp. 998-1003.

[9] V. Oleshchuk, "Internet of Things and Privacy Preserving Technologies," *International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, Grimstad, 17-20 May 2009, pp. 336-340.

[10] International Telecommunication Union, "The Internet of Things, Executive Summary." http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

[11] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, No. 3, 2006, p. 477. doi:10.2307/40041279

[12] T. Kowatsch and W. Maass, "Privacy Concerns and Acceptance of IoT Services," *Internet of Things Intitiative*, 2012, pp. 176-187.

[13] E. K. Choe, S. Consolvo, J. Jung, B. Harrison and J. A.

Kientz, "Living in a Glass House: A Survey of Private Moments in the Home," *Proceedings of the* 13*th International Conference on Ubiquitous Computing*, Beijing, 17-21 September 2011, pp. 41-44.

[14] Y. Wang, G. Norcie and L. F. Cranor "Who Is Concerned about What? A Study of American, Chinese and Indian Users Privacy Concerns on Social Network Sites," *International Conference on Trust & Trustworthy Computing*, Vol. 6740, 2011, pp. 146-153.

[15] D. J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review*, Vol. 44, 2007, p. 745.

*E-Health Telecommunication Systems and Networks*, **2013, 2, 58-63**
http://dx.doi.org/10.4236/etsn.2013.23008 Published Online September 2013 (http://www.scirp.org/journal/etsn)

# Perspectives for Wearable Electronics in Healthcare and Childcare

**Johanna Virkki[1], Pasi Raumonen[2]**
[1]Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
[2]Department of Mathematics, Tampere University of Technology, Tampere, Finland
Email: johanna.virkki@tut.fi

Received June 3, 2013; revised July 8, 2013; accepted July 31, 2013

## ABSTRACT

This paper starts with a literature survey that introduces the possibilities of wearable electronics (WE) in different health-care and childcare applications. Next, 24 personal interviews and an Internet forum survey were conducted in Finland about the use of WE in the applications mentioned above. According to the results, most of the people feel positive about clothes used for wireless identification purposes in healthcare and childcare, but when more information about the person is added that can be wirelessly read, the feelings become more negative. Several important points to consider before implementation of WE for healthcare and childcare environments were brought up.

**Keywords:** Childcare; Finland; Healthcare; Individual Privacy; Wearable Electronics

## 1. Introduction

One important part of the development of the future living environment is the development of wearable electronics (WE) [1,2]. Recently, many innovative products have appeared and expectations about the potential of WE are high. The history of WE is summarized in [3]. Important application areas can be found e.g. from healthcare [4,5] and childcare.

This study focuses on WE used in healthcare and childcare environments. It includes a literature survey, personal interviews in Finland, and an Internet forum survey in Finnish Internet forums. After this introduction to the literature survey, the second section introduces the interviews and the Internet forum survey. The results are presented and discussed in the third section. The last section summarizes the results and presents the conclusions of this paper.

### 1.1. WE in Healthcare

In healthcare applications, WE can be used e.g. in patient monitoring, positioning, and identification in hospitals [6]. For example, a wireless sensor network (WSN)-based indoor location system to support the nursing staff [7], a radiofrequency identification (RFID) system to track and identify patients in a children's critical care ward [8], body-worn tags for the continuous tracking of human movements in a conventional room [9], and a system to detect life-threatening changes of daily activeties of older people [10] have been presented. In the future, the importance of telemedicine and home-nursing is expected to grow. The adjustment of the healthcare systems to the increasing number of elderly and patients with chronic diseases is one of the biggest challenges to the European Union, including Finland, where this survey was done, and the future of the public healthcare is currently a hot topic in the Finnish media. There are many opportunities to help elders live alone in their homes with the help of WE. For example, a system has been proposed that is installed in footwear for location tracking and in gloves for activity monitoring [11], as well as an RFID-based fall detection monitoring system that includes a dual-band RFID module, placed into a pair of slippers [12]. WE allows the body status to be monitored by devices that measure heart or brain activity, blood pressure, body temperature, or other body functions [13]. For example, the realization of wireless oxygen saturation and heart rate system for patient monitoring [14], a scheme for monitoring the patient's temperature, heartbeat, and pressure [15], and a wearable health system for non-invasive and wireless monitoring of physiological signals [16] have been introduced. Freedom of movement achieved by WE is especially important in home nursing [17]. Thus, another application for WE is in the recovery of patients after an operation; instead of being hospitalized for recovery monitoring, the patients can be discharged to return home sooner. In addition to reducing the cost of the operation, home-nursing can increase the patient's physical activity, and thus also speed up recovery.

### 1.2. WE in Childcare

In childcare applications, WE could automate the children security and safety and thus provide help to nurses [18]. A single cloth can keep the information of a child (e.g. name, age, kindergarten group, allergies, etc.) easily achieved for the nurses. In one proposed system, RFID tags were embedded in the children uniforms in order to automate the children security supervision and to provide integration with the current security management system for the kindergarten [19]. Another study proposed a system solution based on RFID to be deployed in schools. The system registers arrival and departure times of pupils and sends that information to parents via SMS and/or e-mail [20]. In Finland, all children under seven years old have the right to have daycare organized by municipalities either on a full-time or part-time basis. Compulsory education starts in the year when a child becomes seven years of age and in the previous year the child can participate in pre-primary education in a pre-primary school.

### 1.3. Individual Privacy and WE

One of the most important challenges in convincing users to adopt WE is the protection of privacy. Informational privacy is the right of an individual to exercise control over the collection, use, disclosure, and retention of his or her personal information. Concerns over privacy can spread wide, particularly as wireless systems can track users' actions, behavior, and on-going preferences [21, 22]. It makes the adoption of a ubiquitous healthcare or childcare system deterred [23,24]. It has been stated, however, that privacy problems are not caused by the technology alone, but primary through activities of people, businesses, and governments [25].

Several interesting surveys have already been conducted. According to one study, using an iPod jacket as the test item, the most important adoption factors are convenience and compatibility, and the least important are perceived social prestige and observability [26]. It was mentioned, that this finding might not be intuitive, considering that potential consumers of this kind of WE are thought to be greatly influenced by external forces such as peer pressure, trends, and perceived social prestige. In a survey focusing on the activities and habits that people do at home, which they would not want to be recorded, the bedroom was found to be the most private place [27]. The willingness of older adults to share health or activity data with one's doctor or family members and concerns about privacy or security of monitoring has also been measured [28]. A high proportion (over 72%) of participants reported acceptance of in-home and computer monitoring and willingness to have data shared with their doctor or family members. However, a majority (60%) reported concerns related to privacy or security; these concerns increased after one year of participation. Findings suggest that involvement in this unobtrusive in-home monitoring study may have raised awareness about the potential privacy risks of technology. Elderly individuals, who were still living independently, were asked to discuss their perceptions and concerns towards the likelihood of using a WSN-based healthcare system in their home [29]. The findings in this study indicate that independence is highly valued by elderly people and hence any system or technology that can prolong that independence tends to be highly regarded. Thus, for example the privacy of WSN health data might not be as important as typically considered. Also, according to the participants in a similar study, the results suggested strong acceptance of the concept of home health monitoring and the devices to make the system work [30]. In a study, where opinions on individual privacy were collected from China and Finland, the Internet of Things applications related to personal health were the least worrying ones among all applications [31]. It was stated, that in healthcare, the most important thing is that all the vital information is available when needed. This work shares some similar objects to the studies above. The goal is to gather information on ordinary people's thoughts about WE in healthcare and childcare in Finland.

## 2. Interviews and Internet Forum Survey

### 2.1. Interviews

In this work, 24 Finnish people of different age were interviewed (genders and ages of the answerers can be seen in **Table 1**). The personal interviews were conducted by an associate of the researcher, and they took place either at the answerers working facility, home, or at a neutral, public place. Some of the interviews were done by private (e-)mails between the researcher and the answerers. All these interviews thus had more flexibility than only a paper survey as both the researcher and the answerer were able to ask for clarification. In this study, the individual privacy refers to the evolving relationship between the technology and the legal right to, or public expectation of, privacy in the collection and sharing of data about one's self. The interview had the following questions and a chance for free comments.

1) Would you be willing to wear hospital clothes that.

**Table 1. Genders and ages of the interviewees.**

| | female | male |
|---|---|---|
| **minimum age** | 29 | 28 |
| **average age** | 36 | 38 |
| **maximum age** | 52 | 61 |
| **number of interviewees** | 12 | 12 |

1A) Would allow wireless reading of your name and patient number for those taking part into your care? (Yes/No)

1B) In addition to wireless reading of your name and patient number, would allow wireless reading of your medical and medication records for those taking part into your care? (Yes/No)

2) How worried would you be about your individual privacy in situations 1A and 1B? (Scale = 1 - 5, where 1 = not worried at all, 5 = very worried)

3) Would you be willing to let your child wear clothes in kindergarten that.

3A) would allow the nurses to wirelessly read the child's name and kindergarten group? (Yes/No)

3B) In addition to the child's name and kindergarten group, would allow the nurses to wirelessly read other information, such as age, allergies, legal guardian, or contact information of guardians? (Yes/No)

4) How worried would you be about your child's individual privacy in situations 3A and 3B? (Scale = 1 - 5, where 1 = not worried at all, 5 = very worried)

## 2.2. Internet Forum Survey

The second part of this work was a survey of discussions on different Internet forums. Discussions on WE were started in May 2013, on 7 Finnish Internet forums, where people are able to discuss anonymously. Three of the forums were focused on discussions on parenthood and children, two of the forums were science forums, one was a forum concentrated on electronics, and one for media and information technology. In the message starting the discussion, the potential of WE in healthcare and childcare was introduced and thoughts of such topic were asked. The goal was to collect a general idea of feelings and highlight some of the presented thoughts.

# 3. Results and Discussion

## 3.1. Results from Interviews

The results (percentages for answers "yes" and "no") from the questions 1A, 1B, 3A, and 3B can be seen in **Table 2**. The results for how worried would the interviewees be about the individual privacy in these different situations can be seen in **Table 3** and **Figure 1**.

**Table 2. The results (percentages for answers "yes" and "no") from the situations 1A, 1B, 3A, and 3B.**

| | yes/no | 1A | 1B | 3A | 3B |
|---|---|---|---|---|---|
| **female (%)** | Yes | 75<br>(N = 9) | 50<br>(N = 6) | 83<br>(N = 10) | 8<br>(N = 1) |
| | No | 25<br>(N = 3) | 50<br>(N = 6) | 17<br>(N = 2) | 92<br>(N = 11) |
| **male (%)** | Yes | 83<br>(N = 10) | 33<br>(N = 4) | 83<br>(N = 10) | 50<br>(N = 6) |
| | No | 17<br>(N = 2) | 67<br>(N = 8) | 17<br>(N = 2) | 50<br>(N = 6) |
| **all (%)** | Yes | 79<br>(N = 19) | 42<br>(N = 10) | 83<br>(N = 20) | 29<br>(N = 7) |
| | No | 21<br>(N = 5) | 58<br>(N = 14) | 17<br>(N = 4) | 71<br>(N = 17) |

**Table 3. The average values of results how worried would the interviewees be about the individual privacy in situations 1A, 1B, 3A, and 3B, scale 1 - 5.**

| | 1A | 1B | 3A | 3B |
|---|---|---|---|---|
| **average value** | 2.25 | 3.38 | 1.67 | 3.42 |

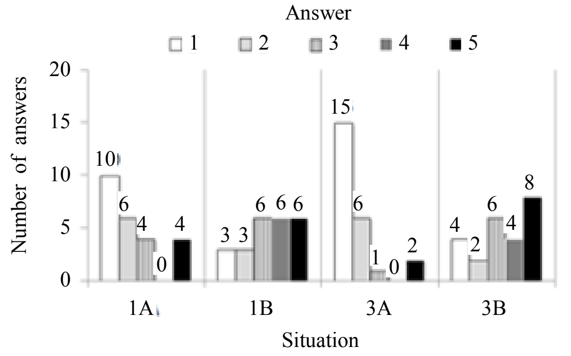

**Figure 1. The results how worried would the interviewees be about the individual privacy in situations 1A, 1B, 3A, and 3B, scale 1 - 5.**

According to our results, 79% of the interviewees would be willing to wear hospital clothes that would allow wireless reading of their name and patient number (Situation 1A). If, in addition of wireless reading of the name and patient number, the hospital clothes would allow wireless reading of medical and medication records (Situation 1B), only 42% would be willing to wear the clothes. In free comments, WE in hospitals were mostly considered useful, especially in hospitals with a lot of patients and a great turnover, as such clothes may prevent mix-ups of patients. However, it was strongly pointed out that the use of this kind of clothes should be voluntary or there would have to be a good reason for it. It was specified that availability of medical records is good but they cannot be available for inappropriate people, not even for those working in that hospital.

As can be seen in **Table 3**, on scale 1 - 5, the average values for the worry about individual privacy in situations 1A and 1B were 2.25 and 3.38, respectively. Thus, as natural, when more information on the user of the clothes is available, the worry about the individual privacy is stronger. However, in neither situation, the worry cannot be considered extremely strong (scale 1 - 5).

It is shown in **Table 2**, that 83% of the interviewees would be willing to let their child wear clothes in kindergarten that would allow the nurses to wirelessly read the child's name and kindergarten group (Situation 3A). If, in addition to the child's name and kindergarten group, the clothes would allow the nurses to wirelessly read other information, such as age, allergies, legal guardian, contact information of guardians (Situation 3B), only 29% would be willing to let their child wear the clothes. In situation 3B, there was a notable difference between women and men; only 8% of the answers from women were positive, compared to 50% from men. The suitability of WE for children was questioned in many ways in free comments. It was mentioned, that if children are able to rip an electronic component from the clothes, they may eat it, which may cause a serious danger. It was also pointed out, that with children, it is essential that the caregivers should know all children in person. Since this is not always possible, this kind of wearable safety was seen to be one kind of solution.

As can be seen in **Table 3**, on scale 1 - 5, the average numbers for the worry about individual privacy in situations 3A and 3B were 1.67 and 3.42, respectively. Thus, WE that allow the name and kindergarten group to be wirelessly read were not found to be a threat for individual privacy of the child. There were no free comments related to individual privacy of WE in kindergartens, but according to the result 3.42 (on scale 1 - 5) from situation 3B, at least some worrying issues were considered when more information was available for wireless reading.

Due to the small amount of the interviewees, this survey does not offer statistical data for conclusions. However, this paper gives a starting point for research on this important topic by gathering different perspectives for WE in healthcare and childcare. Future research will involve significantly more answerers in order to achieve more meaningful results.

### 3.2. Results from Internet Forum Survey

The first thing that was noticed when starting conversations on different Internet forums was that it is hard to start conversation on WE, as the topic did not enjoy a great interest. 2 of the 7 started conversations got no answers at all. However, in 5 of them, interesting thoughts were presented.

In most of the started conversations, the idea of using WE in hospitals and kindergartens, as long as it is done with the person's own permission, was seen promising. It was also brought up that such applications already exist; particularly tracers for children were mentioned. On the contrary, in one conversation it was stated that WE will never become a part of everyday life. Reasons for this were, e.g., the fact that people want to change clothes all the time and all clothes would need to have the same information stored in them. Also, it was stated that no electronic component can monitor who actually eats the delivered drugs. In addition, WE in healthcare were found to be the sad future direction mainly because there is not enough staff working in hospitals.

Also, the mixing of clothes (e.g. of patients in the same room) must be prevented, as it was mentioned in one conversation. This may also cause care in a kindergarten, where clothes get easily mixed-up. Thus, instead of preventing mix-ups, WE could cause them. The effects of continuous washing and bending on electronics were considered. This is reasonable, since the reliability of wearable components, e.g. in hospitals, is essential.

It was also discussed that some people may not be willing to wear clothes with electronics, as is currently the case with safety wristbands. It was also pointed out that clothes could be taken off. Thus, for example a lockable band was considered to be more suitable if monitoring is mandatory for some reason. In addition, the problems with drawing the limits were mentioned; at what point we can start to monitor a demented person without him/her knowing and how young/old child can decide if not to wear clothes with electronics. In one conversation, the use of current electronic devices, e.g. mobile phones, to be utilized in such healthcare applications was also considered. Current mobile devices already have many of the needed features. In many cases, existing mobile devices could be used instead of WE.

## 4. Conclusions

Many innovative applications of WE have appeared recently and expectations about the possibilities are great. WE have an important application area in the healthcare industry and also a great potential for applications in kindergarten and primary school environments. This paper offers information on ordinary people's thoughts to those developing wearable electronic applications and those working with the individual privacy in the future wireless world. It introduces a literature survey about the possibilities of WE in healthcare and childcare. In addition, 24 personal interviews and an Internet forum survey were conducted about these applications in Finland.

According to the results, most of the people feel positive about clothes used for wireless identification purposes. However, when more information is added which can be wirelessly read, the feelings become more negative. In general, the use of WE in hospitals and kindergartens, as long as it is done with person's own permission, was seen promising. Several important points to consider were brought up in free comments and in the Internet forum survey, e.g., related to the safety of children, individual privacy of people, practical issues to consider when embedding electronics to clothes, and usability of already existing mobile devices for such future applications.

## REFERENCES

[1] T. Löher, R. Vieroth, M. Seckel, A. Ostmann and H. Reichl, "Stretchable Electronic Systems for Wearable and Textile Applications," *IEEE VLSI Packaging Workshop of Japan*, Kyoto, 1-2 December 2008, pp. 9-12.

[2] M. Swan, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0.," *Journal of Sensor and Actuator Networks*, Vol. 3, No. 1, 2012, pp. 217-253. doi:10.3390/jsan1030217

[3] H.-J. Yoo, "Your Heart on Your Sleeve: Advances in Textile-Based Electronics Are Weaving Computers Right into the Clothes We Wear," *IEEE Solid-State Circuits Magazine*, Vol. 5, No. 1, 2013, pp. 59-70. doi:10.1109/MSSC.2012.2232781

[4] L. Yang, R. Vyas, A. Rida, J. Pan and M. M. Tentzeris, "Wearable RFID-Enabled Sensor Nodes for Biomedical Applications," *Electronic Components and Technology Conference*, Lake Buena Vista, 27-30 May 2008, pp. 2156-2159.

[5] H. Alemdar and C. Ersoy, "Wireless Sensor Networks for Healthcare: A Survey," *Computer Networks*, Vol. 54, No. 15, 2010, pp. 2688-2710. doi:10.1016/j.comnet.2010.05.003

[6] S.-W. Wang, W.-H. Chen, C.-S. Ong, L. Liu and Y.-W. Chuang. "RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital," *International Conference on System Sciences*, Vol. 8, 4-7 January 2006, 10 p. doi:10.1109/HICSS.2006.422

[7] C. C. Hsiao, Y-J. Sung, S.-J. Lau; C.-H. Chen, F.-H. Hsiao, H.-H. Chu and P. Huang, "Towards Long-Term Mobility Tracking in NTU Hospital's Elder Care Center," *IEEE International Conference on Pervasive Computing and Communications Workshops*, Seattle, 21-25 March 2011, pp. 649-654.

[8] E. Iadanza and F. Dori, "Custom Active RFID Solution for Children Tracking and Identifying in a Resuscitation Ward," *IEEE International Conference, Engineering in Medicine and Biology*, Minneapolis, 3-6 September 2009, pp. 5223-5236.

[9] C. Occhiuzzi, S. Cippitelli and G. Marrocco, "Modeling, Design and Experimentation of Wearable RFID Sensor Tag," *IEEE Transactions on Antennas and Propagation*, Vol. 58, No. 8, 2010, pp. 2490-2498. doi:10.1109/TAP.2010.2050435

[10] A. A. Safavi, A. Keshavarz-Haddad, S. Khoubani, S. Mosharraf-Dehkordi, A. Dehghani-Pilehvarani and F. S. Tabei, "A Remote Elderly Monitoring System with Localizing Based on Wireless Sensor Network," *International Conference on Computer Design and Applications*, Qinhuangdao, 25-27June 2010, pp. V2-553-V2-557.

[11] K. K. Jung, D. S. Son and K. H. Eom, "RFID Footwear and Floor System," *World Congress on Computer Science and Information Engineering*, Los Angeles, 31 March-2 April 2009, pp. 72-75.

[12] Y.-C. Chen and Y.-W. Lin, "Indoor RFID Gait Monitoring System for Fall Detection," *International Symposium on Aware Computing*, Tainan, 1-4 November 2010, pp. 207-212.

[13] Z. Pang, Q. Chen, L. Zheng and E. Dubrova, "An In-Home Medication Management Solution Based on Intelligent Packaging and Ubiquitous Sensing," *International Conference on Advanced Communication Technology*, PyeongChang, 27-30 January 2013, pp. 545-550.

[14] C. Rotariu and V. Manta, "Wireless System for Remote Monitoring of Oxygen Saturation and Heart Rate," *Federated Conference on Computer Science and Information Systems*, Wroclaw, 9-12 September 2012, pp. 193-196.

[15] B. Vijayalakshmi and C. Ram Kumar, "Patient Monitoring System using Wireless Sensor based Mesh Network," *International Conference on Computing Communication & Networking Technologies*, Coimbatore, 26-28 Junly 2012, pp. 1-6.

[16] R. G. Haahr, S. Duun, E. V. Thomsen, K. Hoppe and J. Branebjerg, "A Wearable 'Electronic Patch' for Wireless Continuous Monitoring of Chronically Diseased Patients," *International Summer School and Symposium on Medical Devices and Biosensor*s, Hong Kong, 1-3 June 2008, pp. 66-70.

[17] T. Kellomäki, W. G. Whittow, J. Heikkinen and L. Kettunen, "2.4 GHz Plaster Antennas for Health Monitoring," *European Conference on Antennas and Propagation*, Berlin, 23-27 March 2009, pp. 211-215.

[18] C.-J. Lin, T.-L. Lee, S.-L. Syu and B.-W. Chen, "Application of Intelligent Agent and RFID Technology for Indoor Position: Safety of Kindergarten as Example," *International Conference on Machine Learning and Cybernetics*, Qingdao, 11-14 July 2010, pp. 2571-2576.

[19] Z. Fang, L. Wei, W. Chen and Y. He, "A RFID-Based Kindergarten Intelligence Security System," *IEEE International Conference on e-Business Engineering*, Hangzhou, 9-11September 2012, pp. 321-326.

[20] M. Krsmanovic, G. Muric and N. Gospic, "Improvement of Children Safety by using RFID Based Service," *Telecommunications Forum*, Belgrade, 22-24 November 2011, pp. 130-133.

[21] H. Feng and W. Fu, "Study of Recent Development about Privacy and Security of the Internet of Things," *International Conference on Web Information Systems and Mining*, Sanya, 23-24 October 2010, pp. 91-95.

[22] S. Kurkovsky, E. Syta and B. Casano, "Continuous RFID-Enabled Authentication: Privacy Implications," *IEEE Technology and Society Magazine*, Vol. 30, No. 3, 2011, pp. 34-41. doi:10.1109/MTS.2011.942306

[23] W. J. Song, S. H. Son, M. Choi and M. Kang, "Privacy and Security Control Architecture for Ubiquitous RFID Healthcare System in Wireless Sensor Networks," *Inter-*

*national Conference on Consumer Electronics*, Las Vegas, 7-11 January 2006, pp. 239-240.

[24] S. S. Choi, M. K. Choi, W. J. Song and S. H. Son, "Ubiquitous RFID Healthcare Systems Analysis on PhysioNet Grid Portal Services Using Petri Nets," *International Conference on Information, Communications and Signal Processing*, Bangkok, 6-9 December 2005, pp. 1254-1258.

[25] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, No. 3, 2006, GWU Law School Public Law Research Paper No. 129.

[26] G. Anderson and G. Lee, "Why Consumers (Don't) Adopt Smart WE," *IEEE Pervasive Computing*, Vol. 7, No. 3, 2008, pp. 10-12. doi:10.1109/MPRV.2008.64

[27] E. K. Choe, S. Consolvo, J. Jung, B. Harrison and J. A. Kientz, "Living in a Glass House: A Survey of Private Moments in the Home," *International Conference on Ubiquitous Computing*, Beijing, 17-21 Sseptember 2011, pp. 41-45.

[28] L. Boise, K. Wild, N. Mattek, M. Ruhl, H. H. Dodge and J. Kaye, "Willingness of Older Adults to Share Data and Privacy Concerns after Exposure to Unobtrusive In-Home Monitoring," *Gerontechnology*, Vol. 11, No. 3, 2013, pp. 428-435.

[29] R. Steele, A. Lo, C. Secombe and Y. K. Wong, "Elderly Persons' Perception and Acceptance of Using Wireless Sensor Networks to Assist Healthcare," *International Journal of Medical Informatics*, Vol. 78, No. 12, 2009, pp. 788-801. doi:10.1016/j.ijmedinf.2009.08.001

[30] W. C. Mann, T. Marchant, M. Tomita, L. Fraas and K. Stanton, "Elder Acceptance of Health Monitoring Devices in the Home," *Care Management Journals*, Vol. 3, No. 2, 2002, pp. 91-98.

[31] J. Virkki and L. Chen, "Personal Perspectives: Individual Privacy in the IOT," *Advances in Internet of Things*, Vol. 3, No. 2, 2013, pp. 21-26. doi:10.4236/ait.2013.32003

Journal of Information Security, 2014, 5, 46-55
Published Online April 2014 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2014.52005

# Privacy of Wearable Electronics in the Healthcare and Childcare Sectors: A Survey of Personal Perspectives from Finland and the United Kingdom

**Johanna Virkki[1], Rebecca Aggarwal[2]**

[1]Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
[2]School of Engineering Systems and Management, Aston University, Birmingham, UK
Email: johanna.virkki@tut.fi, r.aggarwal3@aston.ac.uk

Received 7 January 2014; revised 7 February 2014; accepted 14 February 2014

## Abstract

**The innovative development of Wearable Electronics (WE) is creating exciting opportunities for application across many industries. Two sectors with high potential are healthcare and childcare. However, it is in these two sectors where the challenges of privacy are presumed to be of the highest. In order to ascertain the personal views of people about potential privacy problems in WE application in these two sectors, interviews with questionnaires were conducted in two different countries: Finland and the United Kingdom (UK). The results indicated that the majority of people in both countries are positive about the use of WE in healthcare and childcare environments. However, when more information is added to be read wirelessly, the attitudes become more negative. In general, the application of WE is more favorable in the UK and the reason as to the difference will make for interesting further research. Several interesting viewpoints and concerns were presented in the interviews. It can be concluded that the implementation of WE in these two sectors will require the collaboration of work on several areas and the development of versatile user studies.**

## Keywords

**Childcare; Healthcare; Privacy; Wearable Electronics**

## 1. Introduction

Given the importance of addressing ways to provide efficient care for the elderly, children, and people with

**How to cite this paper:** Virkki, J. and Aggarwal, R. (2014) Privacy of Wearable Electronics in the Healthcare and Childcare Sectors: A Survey of Personal Perspectives from Finland and the United Kingdom. *Journal of Information Security*, **5**, 46-55. http://dx.doi.org/10.4236/jis.2014.52005

chronic diseases, researchers have started to explore technological solutions to enhance healthcare and social care provision whilst complementing existing services [1]. Within the childcare sector, there is a need to implement systems that monitor the children and automate the safety and security procedures. However, within the healthcare sector, there is a requirement to develop systems which go beyond the identification and monitoring of patients and also include the collection of important data in order to implement preventive care, allow prompt diagnosis of acute complications, and promote understanding of how (pharmacological) therapy is improving patients' parameters [2].

To address the growing needs of the healthcare and childcare sectors, a new generation of clothing and other wearables are being developed, which are able to sense, communicate data, and harvest energy in a nonintrusive way [3] [4]. These innovations fall under the area of Wearable Electronics (WE). The characteristic of ubiquitous monitoring and the wide range of versatile manufacturing methods (screen printing [5] [6], sewing machine and embroidery [7]-[9], copper meshes, conducting textiles, and ribbons [2] [10]-[13], and spraying using conductive paint [12]) has led to high expectations in regard to the potential of WE applications.

Although there are significant benefits in WE applications, the area also has challenges, as illustrated in **Table 1**. One area that is not addressed, and is of vast importance, is the perception of the people who the technology will be applied. There have been a lot of concerns from the public in regard to wireless sensor technologies but there has not been an investigation into the perceptions of people in regard to WE, particularly in important sectors such as the healthcare and childcare sectors.

This paper explores the personal perspectives of people in reference to WE application in the healthcare and childcare sectors. The research is conducted in both Finland and the UK in order to explore if there is a difference between the two countries. The paper is set out as follows. In section 2, there is a literature review of WE with a focus of its application in the healthcare and childcare sectors. Section 3 explores the main issue of WE (privacy) by exploring the challenges and concerns. It is asserted that further research is required into the perceptions of individuals in regard to WE in healthcare and childcare, and their views of privacy. Section 4 introduces the methodology to investigate this research problem, which is through questionnaires and interviews. In order to gather versatile data and investigate if there are any differences in views, the interviews are carried out in the UK and Finland. The results are presented and discussed in Section 5 and finally the paper concludes with Section 6, the conclusions.

## 2. Wearable Electronics (WE)

### 2.1. The Definition of WE

Wearable electronics and wearable computers appeared in the mid-1990s, when the computer was regarded as

**Table 1.** List of challenges in WE applications [1].

| Challenge | |
|---|---|
| **Hardware** | |
| | Unobtrusiveness |
| | Sensitivity and calibration |
| | Energy |
| | Data acquisition efficiency |
| **Physical** | |
| | Error resilience and reliability |
| | Interoperability |
| | Bandwidth |
| **Application** | |
| | Security |
| | Privacy |
| | User-friendliness |
| | Ease of deployment and scalability |
| | Mobility |

the ultimate equipment for information processing and thus before tablet computers and smart phones [14]. The concept of wearables, something you're wearing, e.g., clothing, glasses, or watches, is nothing new. However, today's wearables can sense and communicate. In reference [15], WE is defined as "apparel with unobtrusively built-in electronic functions" whereas in reference [16] it is defined as "intelligent assistance that augments memory, intellect, creativity, communication and physical senses". WE in this study is defined by adding electronics in anything wearable. Therefore, the focus in this study is on e-clothes, *i.e.*, clothes with added electronics, and more specifically, an exploration of people's perceptions and not so much in the e-cloth technology itself.

## 2.2. WE in Healthcare

The healthcare sector is very large all across the globe and high costs and large quantity of errors make the industry very challenging [17]. Also, population structures are changing and an increase in the aging population creates a higher demand for healthcare services. The increasing number of patients (many elderly) with chronic diseases (such as heart failures, dementia, and strokes) and the healthcare system adjustment required to cope with the changes have been highlighted as one of biggest challenges by the European Union (EU). Therefore, this research focuses on two member states within the EU; Finland and the UK.

Potential healthcare sector applications of WE can be found, e.g., in patient monitoring, positioning, and identification [18]. In addition, a wireless sensor network (WSN)-based indoor location system to support the nursing staff [19], a radiofrequency identification (RFID) system to track and identify patients in a children's critical care ward [20], body-worn tags for the continuous tracking of human movements in a conventional room [21], and a wearable RFID-enabled sensor node for continuous biomedical monitoring [22] have been introduced.

WE can also offer opportunities to help old people live alone in their homes and systems to detect life-threatening changes of daily activities of older people have been presented [23]. For example, imagine a system installed in footwear for location tracking and in gloves for activity monitoring [24], as well as an RFID-based fall detection monitoring system, placed into a pair of slippers [25]. WE can monitor the body status by devices that measure heart or brain activity, blood pressure, body temperature, and other body functions [26]. Just to present a couple of examples; the realization of wireless oxygen saturation and heart rate system for patient monitoring [27], a scheme for monitoring the patient's temperature, heartbeat, and pressure [28], and a wearable health system for non-invasive and wireless monitoring of physiological signals [29] have been introduced, which opens up a realm of possibilities when addressing the issues within the healthcare sector for coping with chronic diseases and an aging population.

In addition to reducing the cost of the operation by replacing the time being hospitalized for recovery monitoring with WE and home-nursing, it is also possible to increase the patient's physical activity, and thus also speed up recovery. In the future, the importance of home-nursing is expected to grow in general, and the freedom of movement achieved by WE is especially significant in home nursing [30].

## 2.3. WE in Childcare

In childcare applications, WE could automate the children security and safety and thus provide help to nurses. For example, in emergency situations, use of WE can ensure everyone is safely evacuated and it can provide accurate child and nurse counts for daily management. A single cloth can keep the data of a child (e.g. name of the child and parents, age, kindergarten group, allergies, etc.), allowing the nurses easy access to vital information.

Interesting studies have already been conducted. In one proposed system, RFID tags were embedded in the costumes of the children in order to automate the security supervision and to provide integration with the current security management system for the kindergarten [31]. Another study proposed a system solution based on RFID to be deployed in schools. The system registers arrival and departure times of pupils, and sends that information to parents via mobile phone and/or e-mail [32]. RFID technology was also deployed in a kindergarten environment for indoor positioning to provide a helping hand to nurses [33]. In Finland, all children under seven years old have the right to have daycare organized by municipalities either on a full-time or part-time basis. Compulsory education starts in the year when a child becomes seven years of age and in the previous year the child will participate in pre-primary education in a pre-primary school. In the UK, full-time education is compulsory for all children aged between five and seventeen with a child beginning primary education during the school year he or she turns five.

## 3. WE and Privacy

Information privacy is the right of an individual to exercise control over the collection, use, disclosure, and retention of his or her personal information. One of the most important challenges in adopting, and most of all, convincing the actual users to adopt WE in healthcare and childcare environments, is the protection of privacy. The fact that wireless systems can track users' actions, behaviors, and on-going preferences, creates a deterrent to the adoption of a ubiquitous healthcare or childcare system [34]-[37].

One study asserts that during a test of the iPod jacket, the most important adoption factors were convenience and compatibility, and the least important ones were perceived social prestige and observability [38]. It was mentioned that this finding might not be intuitive considering that potential consumers of this kind of WE are thought to be greatly influenced by external forces, such as peer pressure, trends, and perceived social prestige. When moving in personal spaces, such as at home, the bedroom was found to be the most private place that people would not want to be monitored [39]. Therefore, there is an imaginary line as to what is deemed acceptable and what is not when it comes to privacy, and this can often be ambiguous and challenging to define.

When exploring into privacy issues in the healthcare sector, the willingness of older adults to share health or activity data with their doctor or family members have also been measured [40] and over 72% of participants reported acceptance of in-home and computer monitoring and willingness to share the data with their doctor or family members. However, 60% reported concerns related to privacy or security and these concerns increased after one year of participation. It was concluded that involvement in this in-home monitoring study raised awareness about the potential privacy risks of the technology [40].

Although the views highlighted some concerns in regard to privacy, independently living elderly individuals were asked to discuss their perceptions and concerns towards the likelihood of using a WSN-based healthcare system in their home [41]. The results in this study indicate that independence is highly valued by elderly people and any technology that can prolong independence, tends to be highly regarded. Thus, for example the privacy of health data might not be as vital as usually considered. Also, according to the participants in a similar study, the results suggested strong acceptance of the concept of home health monitoring and the technology to make the system work [42]. The perspectives for WE in Finland were already collected in a previous study by interviews and an Internet forum survey [43]. Several important points to consider before the implementation of WE for healthcare and childcare environments were found:

- safety of children,
- individual privacy of people,
- practical issues to consider when embedding electronics to clothes, and
- usability of already existing mobile devices for such future applications.

In a study where opinions on individual privacy were collected from China and Finland, the application of Internet of Things to personal health was identified as the least problematic amongst all the applications [44]. It was stated that in the healthcare sector, the most important thing is that all the vital information is available when it is needed. Therefore, it is clear that concerns of privacy within the healthcare sector are very unclear and vary due to age, status (married/single) and potential benefit application (help to improve health or live independently). This requires further investigation and particularly views within the childcare sector where there are no published results of perception within the EU area.

This research develops on the areas addressed in this section and Section 2, filling a gap in the literature in regard to WE application in the healthcare and childcare sectors. The goal is to gather and compare the personal views of people about privacy in WE application from Finland and the UK in order to provide an account of the perceptions and highlight any potential barriers which may arise in regard to further development and application of WE (in healthcare and childcare).

## 4. Methodology: Questionnaires and Interviews

In this study, 45 people, 24 from Finland and 21 from the UK, were interviewed. The interview included the questionnaire (shown in **Table 2**) and a chance for free comments. The personal interviews were conducted by an associate of the researcher and they took place either at the interviewees working facility, home, or at a neutral, public place. Some of the interviews were done by private (e-)mails between the researcher and the interviewee. All these interviews thus had more flexibility than only a paper survey as both the researcher and the interviewee were able to ask for clarification. The genders and ages of the interviewees from both countries can be seen in **Table 3**.

## 5. Results and Discussion

The results (proportion of "Yes" and "No" responses) for the questions 1A and 1B are presented in **Table 4**. According to our results, 37 out of the total 45 interviewees would be willing to wear hospital clothes that would allow wireless reading of their name and patient number (Situation 1A). The results were similar among people from the UK and Finland and among female and male participants. If, in addition of wireless reading of the name and patient number, the hospital clothes would allow wireless reading of medical and medication records (Situation 1B), 26 out of the total 45 interviewees would be willing to wear the clothes. It can be seen that the Finnish participants are more negative towards wearing these clothes than the participants from the UK. This difference can be clearly seen in **Figure 1**, where the percentages of answers are presented to make the results more comparable.

The results for how worried would the interviewees be about the individual privacy in these two situations can be seen in **Figure 2**. In this study, the individual privacy refers to the evolving relationship between the technology and the legal right to, or public expectation of, privacy in the gathering and sharing of data about one's self. As can be seen, in both Finland and the UK, the female interviewees are more worried; the average values of results how worried would the interviewees be about the individual privacy (scale 1 - 5) are higher in both situations 1A and 1B.

It can also be seen in **Figure 2**, that the average values for the worry about individual privacy in situations 1A and 1B were: 2.25 and 3.38 in Finland, respectively, and 2.10 and 2.48 in the UK, respectively. This asserts that as the amount of user information on the clothes increases, the worry about the individual privacy gets stronger. However, in either situation, the worry cannot be considered extremely strong (scale 1 - 5). If we compare the results from Finland and the UK, it can be seen that the people in Finland are more worried about their individual privacy than the people in the UK. Unfortunately this questionnaire gives no further information on the possible reasons behind this. This interesting result definitely requires more research in the next study.

In free comments, WE in hospitals were, in general, considered useful, and people were "not too worried about basic information being read". It was, e.g., pointed out that such clothes may prevent mix-ups of patients.

**Table 2.** Questionnaire of this study.

1. Would you be willing to wear hospital clothes that.

**1(a)**. Would allow wireless reading of your name and patient number for those taking part into your care? (Yes/No)

**1(b)**. In addition to wireless reading of your name and patient number, would allow wireless reading of your medical and medication records for those taking part into your care? (Yes/No)

**2**. How worried would you be about your individual privacy in situations 1A and 1B?
(Scale = 1-5, where 1 = not worried at all 5 = very worried)

3. Would you be willing to let your child wear clothes in kindergarten that.

**3(a)**. Would allow the nurses to wirelessly read the child's name and kindergarten group? (Yes/No)

**3(b)**. In addition to the child's name and kindergarten group, would allow the nurses to wirelessly read other information, such as age, allergies, legal guardian, or contact information of guardians? (Yes/No)

**4**. How worried would you be about your child's individual privacy in situations 3A and 3B?
(Scale = 1-5, where 1 = not worried at all 5 = very worried)

**Table 3.** Genders and ages of the interviewees.

| | Finland | | UK | |
|---|---|---|---|---|
| | Female | Male | Female | Male |
| Minimum age | 29 | 28 | 15 | 18 |
| Average age | 36 | 38 | 39 | 37 |
| Maximum age | 52 | 61 | 59 | 60 |
| Number of interviewees | 12 | 12 | 13 | 8 |

**Table 4.** Results (answers "Yes" and "No") from situations 1A, 1B, 3A, and 3B.

| | | Yes/No | 1A | 1B | 3A | 3B |
|---|---|---|---|---|---|---|
| Finland | Female (N = 12) | Yes | 9 | 6 | 10 | 1 |
| | | No | 3 | 6 | 2 | 11 |
| | Male (N = 12) | Yes | 10 | 4 | 10 | 6 |
| | | No | 2 | 8 | 2 | 6 |
| | All (N = 24) | Yes | 19 | 10 | 20 | 7 |
| | | No | 5 | 14 | 4 | 17 |
| UK | Female (N = 13) | Yes | 11 | 11 | 11 | 11 |
| | | No | 2 | 2 | 2 | 2 |
| | Male (N = 8) | Yes | 7 | 5 | 4 | 2 |
| | | No | 1 | 3 | 4 | 6 |
| | All (N = 21) | Yes | 18 | 16 | 15 | 13 |
| | | No | 3 | 5 | 6 | 8 |

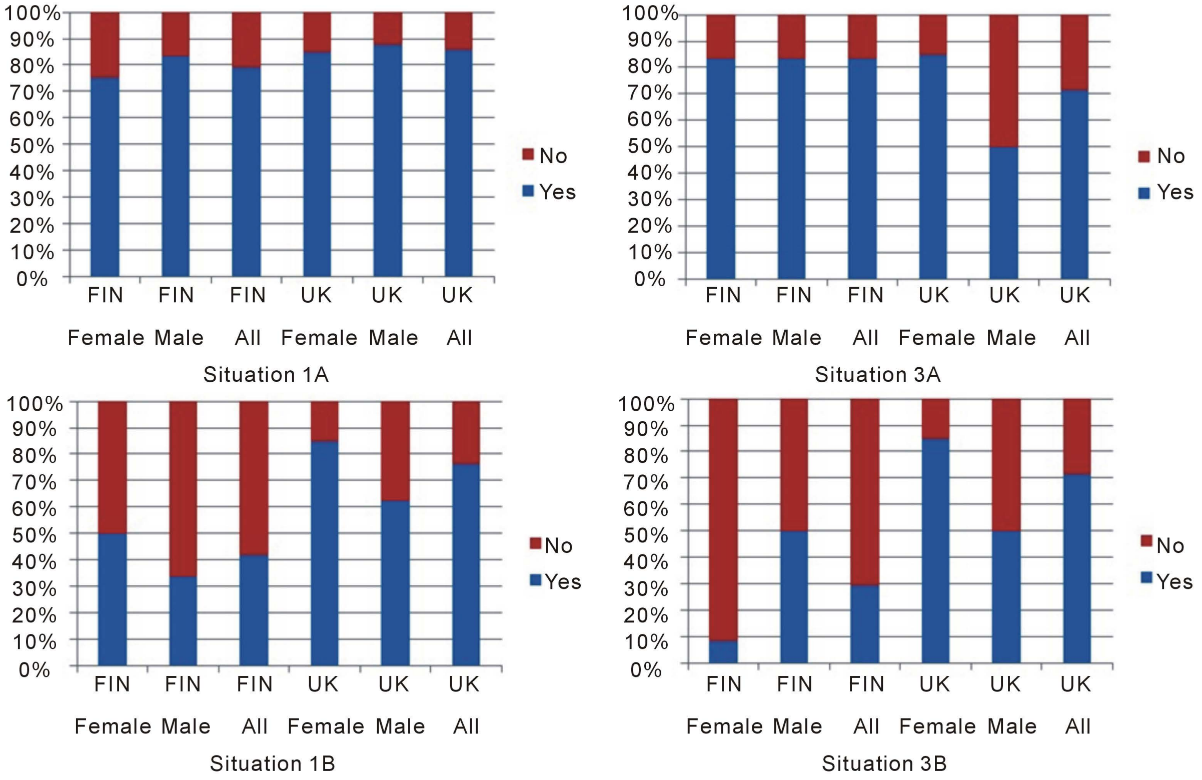

**Figure 1.** Percentages of answers "Yes" and "No" from situations 1A, 1B, 3A, and 3B.

However, it was specified that availability of medical records is good but they cannot be available for inappropriate people, not even for those working in the hospital. Some people were also worried about the expenses of adapting such technology and some were not sure how quickly the current staff in hospitals could adapt to such a new technology. Also, in some answers, the use of such technology was strongly objected: "It is unnecessary" and "It is too risky and dangerous". Thus, people seem to have several concerns over adaptation of WE in healthcare environment. These results are in line with the conclusions presented in a literature review [45], where it was stated that most systems are described in their prototype stages. Deployment issues, such as implications on organization or personnel, privacy concerns, or financial issues are mentioned rarely, though their solution is crucial in transferring promising systems to a stage of actual field operation. Thus, there is definitely a strong need for further research on the deployment of such systems, including clinical studies, economic and

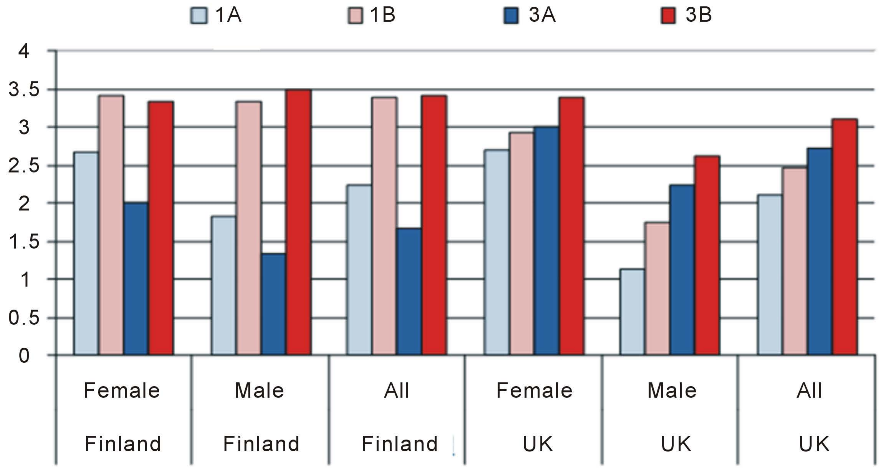

**Figure 2.** The average values of results how worried would the interviewees be about the individual privacy in situations 1A, 1B, 3A, and 3B, scale 1 - 5.

social analyses, and user studies. The users should embrace the system for full satisfaction.

**Table 4** illustrates that 35 out of the total 45 interviewees would be willing to let their child wear clothes in kindergarten that would allow the nurses to wirelessly read the child's name and kindergarten group (Situation 3A). There is no significant difference among people from the UK and Finland and among the female and male interviewees.

If, in addition to the child's name and kindergarten group the clothes would allow the nurses to wirelessly read other information, such as age, allergies, legal guardian, contact information of guardians (Situation 3B), only 20 out of the total 45 interviewees would be willing to let their child wear the clothes. In situation 3B, there was a notable difference when the answers of the female interviewees from the UK were compared to other answers; 11/13 answered "Yes" whereas the other "Yes" results were: 1/12 and 6/12 for the Finnish female and male interviewees, respectively, and 2/8 for the UK male answers. These differences can be clearly seen in **Figure 1**, where the percentages of answers are presented.

However, as shown in **Figure 2**, the UK female interviewees gave the average value of 3.38 (Scale 1 - 5) for how worried would they be about the individual privacy in situation 3B. This value is the second highest among all interviewees, right after 3.50 that were given by the male interviewees from Finland. Thus, the female interviewees from the UK are quite worried about the individual privacy of the children but would still allow them to wear wirelessly readable clothes. This is an interesting finding and will be studied further in our next study.

The suitability of WE for children was questioned in many ways in free comments. It was mentioned that if small children are able to rip an electronic component from the clothes, they may eat it, which may cause a serious danger. Also, it was mentioned that the parents need to have the option to make the decision of whether to use such devices in the kindergarten where their children are, stating also that the use of this kind of wirelessly readable clothes has to be voluntary. It was also pointed out that with children it is essential that the caregivers should know all children in person. Some people were not willing to let their children be "wirelessly connected to anything". Thus, as was the case with WE in the healthcare sector, more research on the implications, privacy concerns, and financial issues is needed.

## 6. Conclusion

Many innovative applications of WE have appeared recently and expectations about the possibilities are great. WE has an important application area in the healthcare industry and also a great potential for applications in kindergarten and primary school environments. This paper consists of a literature survey and 45 personal interviews that were conducted to study the thoughts related to the privacy of these WE applications. The results indicate that the majority of people would be contented to use WE but the application is more favorable in the UK than in Finland. The achieved results are in line with the earlier studies that have highlighted some concerns in regard to privacy but with a strong acceptance of different welfare and healthcare technologies. However, this study also asserts some interesting new findings and further investigation will be conducted in order to compare the results from other countries to see if and why the personal views differ from country to country. As this paper offers information on the public's perceptions in the UK and Finland, it is useful to those developing wearable electronic applications and those investigating individual's privacy whilst developing the future wireless world.

## Acknowledgements

Johanna Virkki would like to thank The Helsingin Sanomat Foundation.

## References

[1] Alemdar, H. and Ersoy, C. (2010) Wireless Sensor Networks for Healthcare: A Survey. *Computer Networks*, **54**, 2688-2710. http://dx.doi.org/10.1016/j.comnet.2010.05.003

[2] Niewolny, D. (2013) How the Internet of Things Is Revolutionizing Healthcare. Freescale Whitepaper. http://cache.freescale.com/files/corporate/doc/white_paper/IOTREVHEALCARWP.pdf

[3] Swan, M. (2012) Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, **3**, 217-253. http://dx.doi.org/10.3390/jsan1030217

[4] Bonfiglio, A. and De Rossi, D. (2011) Wearable Monitoring Systems. Springer, New York. http://dx.doi.org/10.1007/978-1-4419-7384-9

[5] Scarpello, M.L., Kazani, I., Hertleer, C., Rogier, H. and Ginste, D.V. (2012) Stability and Efficiency of Screen-Printed Wearable and Washable Antennas. *IEEE Antennas Wireless Propagaton Letters*, **11**, 838-841. http://dx.doi.org/10.1109/LAWP.2012.2207941

[6] Kellomäki, T., Virkki, J., Merilampi, S. and Ukkonen, L. (2012) Towards Washable Wearable Antennas: A Comparison of Coating Materials for Screen-Printed Textile-Based UHF RFID Tags. *International Journal of Antennas and Propagation*, **2012**, Article ID 476570. http://dx.doi.org/10.1155/2012/476570

[7] Kim, G., Lee, J., Lee, K.H., Chung, Y.C., Yeo, J., Moon, B-H., Yang, J. and Kim, H.C. (2008) Design of a UHF RFID Fiber Tag Antenna with Electric-Thread Using a Sewing Machine. *Microwave Conference*, Macau, 16-20 December 2008, 4 p.

[8] Roh, J.S., Chi, Y.S., Lee, J.H., Tak, Y., Nam, S. and Kang, T.J. (2010) Embroidered Wearable Multiresonant Folded Dipole Antenna for FM Reception. *IEEE Antennas and Wireless Propagation Letters*, **9**, 803-806. http://dx.doi.org/10.1109/LAWP.2010.2064281

[9] Koski, K., Koski, E., Björninen, T., Babar, A.A., Ukkonen, L., Sydänheimo, L. and Rahmat-Samii, Y. (2012) Practical Read Range Evaluation of Wearable Embroidered UHF RFID Tag. *Antennas and Propagation Society International Symposium*, Chicago, 8-14 July 2012, 2 p.

[10] Vallozzi, L., Rogier, H. and Hertleer, C. (2008) Dual Polarized Textile Patch Antenna for Integration into Protective Garments. *IEEE Antennas and Wireless Propagation Letters*, **7**, 440-443. http://dx.doi.org/10.1109/LAWP.2008.2000546

[11] Zhu, S. and Langley, R. (2009) Dual-Band Wearable Textile Antenna on an EBG Substrate. *IEEE Transactions on Antennas and Propagation*, **57**, 926-935. http://dx.doi.org/10.1109/TAP.2009.2014527

[12] Matthews, J.C.G. and Pettitt, G. (2009) Development of Flexible, Wearable Antennas. *European Conference on Antennas and Propagation*, Berlin, 23-27 March 2009, 273-277.

[13] Maleszka, T., Preisner, M. and Kabacik, P. (2009) Meshed Ground Plane Structures for Textile Antennas. *European Conference on Antennas and Propagation*, Berlin, 23-27 March 2009, 713-717.

[14] Yoo, H.-J. (2013) Your Heart on Your Sleeve: Advances in Textile-Based Electronics Are Weaving Computers Right into the Clothes We Wear. *IEEE Solid-State Circuits Magazine*, **5**, 59-70. http://dx.doi.org/10.1109/MSSC.2012.2232781

[15] Tao, X. (2005) Wearable Electronics and Photonics. CRC Press, Boca Raton.

[16] Ko, F.K., Aufy, A. and Lam, H. (2005) Electrostatically Generated Nanofibres for Wearable Electronics. Wearable Electronics and Photonics, Woodhead Publishing.

[17] Fosso Wamba, S., Anand, A. and Carter, L. (2013) A Literature Review of RFID-Enabled Healthcare Applications and Issues. *International Journal of Information Management*, **33**, 875-891. http://dx.doi.org/10.1016/j.ijinfomgt.2013.07.005

[18] Wang, S.-W., Chen, W.-H., Ong, C.-S., Liu, L. and Chuang, Y.-W. (2006) RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital. *International Conference on System Sciences*, 4-7 Janu-

ary 2006, 10 p.

[19] Hsiao, C.C., Sung, Y-J., Lau, S.-J., Chen, C.-H., Hsiao, F.-H., Chu, H.-H. and Huang, P. (2011) Towards Long-Term Mobility Tracking in NTU Hospital's Elder Care Center. *IEEE International Conference on Pervasive Computing and Communications Workshops*, Seattle, 21-25 March 2011, 649-654.

[20] Iadanza, E. and Dori, F. (2009) Custom Active RFID Solution for Children Tracking and Identifying in a Resuscitation Ward. *IEEE International Conference*, *Engineering in Medicine and Biology*, Minneapolis, 3-6 September 2009, 5223-5236.

[21] Occhiuzzi, C., Cippitelli, S. and Marrocco, G. (2010) Modeling, Design and Experimentation of Wearable RFID Sensor Tag. *IEEE Transactions on Antennas and Propagation*, **58**, 2490-2498. http://dx.doi.org/10.1109/TAP.2010.2050435

[22] Yang, L., Vyas, R., Rida, A., Pan, J. and Tentzeris, M.M. (2008) Wearable RFID-Enabled Sensor Nodes for Biomedical Applications. *Electronic Components and Technology Conference*, Lake Buena Vista, 27-30 May 2008, 2156-2159.

[23] Safavi, A.A., Keshavarz-Haddad, A., Khoubani, S., Mosharraf-Dehkordi, S., Dehghani-Pilehvarani, A. and Tabei, F.S. (2010) A Remote Elderly Monitoring System with Localizing Based on Wireless Sensor Network. *International Conference on Computer Design and Applications*, Qinhuangdao, 25-27 June 2010, V2-553-V2-557.

[24] Jung, K.K., Son, D.S. and Eom, K.H. (2009) RFID Footwear and Floor System. *World Congress on Computer Science and Information Engineering*, **3**, 72-75.

[25] Chen, Y.-C. and Lin, Y.-W. (2010) Indoor RFID Gait Monitoring System for Fall Detection. *International Symposium on Aware Computing*, Tainan, 1-4 November 2010, 207-212.

[26] Pang, Z., Chen, Q., Zheng, L. and Dubrova, E. (2013) An In-Home Medication Management Solution Based on Intelligent Packaging and Ubiquitous Sensing. *International Conference on Advanced Communication Technology*, Pyeong Chang, 27-30 January 2013, 545-550.

[27] Rotariu, C. and Manta, V. (2012) Wireless System for Remote Monitoring of Oxygen Saturation and Heart Rate. *Federated Conference on Computer Science and Information Systems*, Wroclaw, 9-12 September 2012, 193-196.

[28] Vijayalakshmi, B. and Ram Kumar, C. (2012) Patient Monitoring System Using Wireless Sensor Based Mesh Network. *International Conference on Computing Communication & Networking Technologies*, Coimbatore, 26-28 July 2012, 1-6.

[29] Haahr, R.G., Duun, S., Thomsen, E.V., Hoppe, K. and Branebjerg, J. (2008) A Wearable "Electronic Patch" for Wireless Continuous Monitoring of Chronically Diseased Patients. *International Summer School and Symposium on Medical Devices and Biosensors*, Hong Kong, 1-3 June 2008, 66-70.

[30] Kellomäki, T., Whittow, W.G., Heikkinen, J. and Kettunen, L. (2009) 2.4 GHz Plaster Antennas for Health Monitoring. *European Conference on Antennas and Propagation*, Berlin, 23-27 March 2009, 211-215.

[31] Fang, Z., Wei, L., Chen, W. and He, Y. (2012) A RFID-Based Kindergarten Intelligence Security System. *IEEE International Conference on E-Business Engineering*, Hangzhou, 9-11 September 2012, 321-326.

[32] Krsmanovic, M., Muric, G. and Gospic, N. (2011) Improvement of Children Safety by Using RFID Based Service. *Telecommunications Forum*, Belgrade, 22-24 November 2011, 130-133.

[33] Lin, C.J., Lee, T.L., Syu, S.L. and Chen, B.W. (2010) Application of Intelligent Agent and RFID Technology for Indoor Position: Safety of Kindergarten as Example. *International Conference on Machine Learning and Cybernetics*, **5**, 2571-2576.

[34] Feng, H.L. and Fu, W.X. (2010) Study of Recent Development about Privacy and Security of the Internet of Things. *International Conference on Web Information Systems and Mining*, **2**, 91-95.

[35] Kurkovsky, S., Syta, E. and Casano, B. (2011) Continuous RFID-Enabled Authentication: Privacy Implications. *IEEE Technology and Society Magazine*, **30**, 34-41. http://dx.doi.org/10.1109/MTS.2011.942306

[36] Song, W.J., Son, S.H., Choi, M. and Kang, M. (2006) Privacy and Security Control Architecture for Ubiquitous RFID Healthcare System in Wireless Sensor Networks. *International Conference on Consumer Electronics*, 7-11 January 2006, 239-240.

[37] Choi, S.S., Choi, M.K., Song, W.J. and Son, S.H. (2005) Ubiquitous RFID Healthcare Systems Analysis on PhysioNet Grid Portal Services Using Petri Nets. *International Conference on Information*, *Communications and Signal Processing*, Bangkok, 2005, 1254-1258.

[38] Anderson, G. and Lee, G. (2008) Why Consumers (Don't) Adopt Smart WE. *IEEE Pervasive Computing*, **7**, 10-12. http://dx.doi.org/10.1109/MPRV.2008.64

[39] Choe, E.K., Consolvo, S., Jung, J., Harrison, B. and Kientz, J.A. (2011) Living in a Glass House: A Survey of Private Moments in the Home. *International Conference on Ubiquitous Computing*, Beijing, 17-21 September 2011, 41-44.

[40] Boise, L., Wild, K., Mattek, N., Ruhl, M., Dodge, H.H. and Kaye, J. (2013) Willingness of Older Adults to Share Data

and Privacy Concerns after Exposure to Unobtrusive In-Home Monitoring. *Gerontechnology*, **11**, 428-435. http://dx.doi.org/10.4017/gt.2013.11.3.001.00

[41] Steele, R., Lo, A., Secombe, C. and Wong, Y.K. (2009) Elderly Persons' Perception and Acceptance of Using Wireless Sensor Networks to Assist Healthcare. *International Journal of Medical Informatics*, **78**, 788-801. http://dx.doi.org/10.1016/j.ijmedinf.2009.08.001

[42] Mann, W.C., Marchant, T., Tomita, M., Fraas, L. and Stanton, K. (2002) Elder Acceptance of Health Monitoring Devices in the Home. *Care Management Journals*, **3**, 91-98.

[43] Virkki, J. and Raumonen, P. (2013) Perspectives for Wearable Electronics in Healthcare and Childcare. *E-Health Telecommunication Systems and Networks*, **2**, 58-63. http://dx.doi.org/10.4236/etsn.2013.23008

[44] Virkki, J. and Chen, L. (2013) Personal Perspectives: Individual Privacy in the IOT. *Advances in Internet of Things*, **3**, 21-26. http://dx.doi.org/10.4236/ait.2013.32003

[45] Orwat, C., Graefe, A. and Faulwasser, T. (2008) Towards Pervasive Computing in Health Care—A Literature Review. *BMC Medical Informatics & Decision Making*, **8**, 26. http://dx.doi.org/10.1186/1472-6947-8-26

# Personal Perspectives for Smart Vehicles and Driving

[1] Yan Liu, [2] Yu Zhai, [3] Minghao Yang, [4] Feiyuan Long, [5] Johanna Virkki
[1,2,3,4] Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[5] Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
[1] yliu357-c@my.cityu.edu.hk, [2] yzhai8962@gmail.com, [3] yangminghao1990@gmail.com, [4] daisylonelone2013@gmail.com,
[5] johanna.virkki@tut.fi

## ABSTRACT

It is not yet clear which of future smart technologies will actually be accepted as part of our everyday lives. In this research, the thoughts of 248 people about smart parking and smart cars and driving systems were collected by interviews and with an Internet survey in Europe and Asia. Firstly, it was found that different people have very different thoughts about what the widely used terms “smart cars and smart drive systems” mean. However, according to our results, the majority of the answerers would be willing to use these smart applications. In general, the Asian answerers were found to be more worried about these new applications than people from Europe, and the reliability of the technology together with cost were considered as the major worries. People were found to be quite willing to let their personal information and driving habits to be recorded by these smart applications. However, the information about the people travelling in the car was considered private. Some major differences were found in results gathered with different methods, which is also important to take into account in further research.

**Keywords:** *Internet of Things, Internet survey, interviews, personal perspectives, smart driving, smart cars, smart parking*

## 1. INTRODUCTION

The Internet of Things (IOT) means connecting daily things and versatile devices in order to create an omnipresent computing world. In the IOT, things will exchange data and information about the environment, while reacting autonomously to different events, influencing the environment, and creating services with or without human intervention. Possible applications of the IOT are versatile in all areas of life [1] [2]. A number of countries and districts have realized the importance of the IOT in the recovery of economic growth and sustainability, amongst them the European Union, the United States, and China. Thus, companies, universities, and research institutions currently take an active part in the IOT development worldwide.

Due to the technology advancement in the IOT, everything is becoming “smart” and “intelligent”, even cars and driving. The potential uses of smart car and driving system applications are almost limitless [3]. Smart cars are to perform sophisticated driver support and automated control functionalities in an unstructured, dynamic world. The intelligent car could understand the situation it is facing and could be able to adapt its internal functionalities accordingly. However, the resulting behavior should be safe under all conditions. Further, self-driving cars, which sense their surroundings with versatile techniques, resulting in less-stressed "drivers", higher efficiency (the driver can do something else during driving), and increased safety and less pollution, are currently a hot topic [4][5].

One basic application area of smart driving is smart parking. Today, searching for a vacant parking space in a metropolitan area is a daily, time-consuming concern for most drivers. It also causes traffic congestion and air pollution by drivers constantly cruising in certain area only for an available parking space. Thus, there is also a need for smarter parking mechanisms, e.g., parking space management, car guidance, parking lot reservation, automatic payment, etc. [6]. The concept of smart parking systems and their categories is studied and the classifications of various existing systems are explained, e.g., in [7].

Despite the fast development of versatile applications, it is not yet clear which of these technologies will actually be accepted as a part of our everyday lives. For example, in an interview study made in Finland, the IOT and its applications were seen tempting, in principle, but the necessity of the versatile applications was also questioned [8]. During the last two decades, user acceptance models that reflect people’s willingness to accept a given technology have been proposed, tested, refined, extended, and unified. For example, in an interesting study conducted in China, the authors proposed an IOT acceptance model that consists of several factors: the results showed particularly strong support for the effects of perceived usefulness, ease of use, enjoyment, and behavioral control, and also of social influence [9]. The results from another study indicated that the acceptance of IOT services is influenced by various contradicting factors, such as perceived privacy risks and personal interests. It was also assumed that legislation, data security and transparency of information influence the adoption behavior [10]. In another study, made in China, it was found that usefulness plays an important role in acceptance of the IOT [11]. Previous studies and the developed user acceptance models have contributed to our understanding of user technology acceptance factors and their relationships. Naturally, they also have found to have their limitations, such as the relatively low explanatory power and inconsistent influences of the factors across studies, leading, e.g., to development of an integrative model [12].

The personal thoughts of potential end users of the IOT and its applications, i.e., “ordinary people”, offer an interesting and important point of view. In this research, the thoughts of 248 people from Europe and Asia were collected by interviews and with an Internet survey. The main focus was to find answers to the following questions:

a. Are the answerers already familiar with these applications?
b. Do the answerers feel that the applications would be use full in their lives?
c. Are the answerers likely to pay extra to use the applications?
d. Are the answerers willing to provide their personal information for the applications?
e. Are there any privacy concerns or concerns about the practicability, cost, or reliability of the technology used in these applications?

This paper is organized as follows: The introduction section shortly introduces the concepts of the IOT, smart cars and driving systems, and smart parking. It also introduces the goals of this study. Section 2 presents the performed interviews and the Internet survey, including the information on the answerers and the presented questions. The collected answers and examples from free comments are presented and discussed in section 3. The last section summarizes the results and presents the conclusions of this paper.

## 2. INTERVIEWS AND INTERNET SURVEY

All the data for this research was collected during June-August 2014. In the first part of this research, 95 people were personally interviewed and Table 1 shows detailed information about the answerers. People of different age, of both gender and of different occupation were chosen from Europe (50 people, all of them from Finland) and from Asia (45 people, all of them from Hong Kong and mainland China). Personal interviews took place either at the answerers working facility or at a neutral, public place. Some of the interviews were done by private e-mails between the researcher and the answerer. All these interviews thus had more flexibility than an anonymous paper or Internet survey, as both the researcher and the answerer were able to ask for clarification.

The second part of this study was an Internet survey, where 153 answers were collected, again from people of different age, of both gender, and of different occupation (See Table 1). There were 50 people from Europe (from Finland, Sweden, Portugal, Germany, Italy, Bulgaria, Norway, Russia, Slovenia, United Kingdom, Spain, and France) and 103 from Asia (from mainland China, Hong Kong, Iran, India, Korea, and Afghanistan).

At the beginning of the interviews and the Internet survey, it was very briefly (by a couple of examples) explained what is meant by smart cars and parking and driving systems in this study. The following examples were given: Smart parking is "to make the process of parking more efficient and convenient, e.g., by smart reservation, charging, and real time monitoring". Smart cars and driving systems are "to collect and transmit information of the vehicle and help to implement car control and coping with emergencies". The seven questions of the interview study are listed next.

**1a.** Have you heard about smart parking systems before?

(Yes/No)

**1b.** Would you be willing to use smart parking?

(Yes/No)

**1c.** Are you willing to pay an extra fee for a smart parking system?

(Yes/No)

**2a.** Have you heard about smart cars and driving systems before?

(Yes/No)

**2b.** Would you be willing to use smart cars and driving systems?

(Yes/No)

**3.** What are your major worries about smart cars and driving systems, if any?

- Your individual privacy
- Reliability of technology
- Practicability
- Cost
- Other

**4.** When do you think that smart cars and driving systems will be in everyday use?

- In the near future
- During 5-10 years
- During 11-20 years
- Longer than 20 years
- Never

The Internet survey covers all the questions from the interview and the following extra question:

**5a.** Would you allow a smart driving system to record your name and plate number?

(Yes/No)

How worried would you be about your individual privacy in above situation? (Scale=1-5; 1=not worried at all, 5=very worried)

**5b.** Would you allow a smart driving system to record your parking time and place?

(Yes/No)

How worried would you be about your individual privacy in above situation? (Scale=1-5; 1=not worried at all, 5=very worried)

**5c.** Would you allow a smart driving system to record your vehicle speed?

(Yes/No)

How worried would you be about your individual privacy in above situation? (Scale=1-5; 1=not worried at all, 5=very worried)

**5d.** Would you allow a smart driving system to record the information of people who are in your car?

(Yes/No)

How worried would you be about your individual privacy in above situation? (Scale=1-5; 1=not worried at all, 5=very worried)

**Table 1:** Gender, age, and nationality of the answerers

| | | Internet Survey | | | Interviews | | |
|---|---|---|---|---|---|---|---|
| **All** | | Asian | European | All | Asian | European | All |
| | | 103 | 50 | 153 | 45 | 50 | 95 |
| **Gender** | Male | 50 | 26 | 76 | 25 | 29 | 54 |
| | Female | 53 | 24 | 77 | 20 | 21 | 41 |
| **Age** | 18-25 | 74 | 18 | 92 | 30 | 23 | 53 |
| | 26-35 | 20 | 25 | 45 | 15 | 13 | 28 |
| | 36-45 | 3 | 4 | 7 | 0 | 6 | 6 |
| | 46-55 | 6 | 1 | 7 | 0 | 6 | 6 |
| | >55 | 0 | 2 | 2 | 0 | 2 | 2 |

**Table 2:** The answers to questions about smart parking

| | | | | |
|---|---|---|---|---|
| **1a. Have you heard about smart parking systems before?** | | | | |
| **Interviews** | | | | |
| | Asian | European | Male | Female |
| **Yes** | 58 % | 36 % | 52 % | 39 % |
| **No** | 42 % | 64 % | 48 % | 61 % |
| **Internet Survey** | | | | |
| | Asian | European | | |
| **Yes** | 65 % | 60 % | | |
| **No** | 35 % | 40 % | | |
| **1b. Would you be willing to use smart parking?** | | | | |
| **Interviews** | | | | |
| | Asian | European | Male | Female |
| **Yes** | 87 % | 86 % | 81 % | 93 % |
| **No** | 13 % | 14 % | 19 % | 7 % |
| **Internet Survey** | | | | |
| | Asian | European | | |
| **Yes** | 80 % | 86 % | | |
| **No** | 20 % | 14 % | | |
| **1c. Are you willing to pay an extra fee in a smart parking system?** | | | | |
| **Interviews** | | | | |
| | Asian | European | Male | Female |
| **Yes** | 49 % | 50 % | 54 % | 44 % |
| **No** | 51 % | 50 % | 46 % | 56 % |

| Internet Survey | | |
|---|---|---|
| | Asian | European |
| **Yes** | 42 % | 54 % |
| **No** | 58 % | 46 % |

## 3. RESULTS AND DISCUSSION

This section introduces and discusses the collected answers. All the examples of the achieved free comments are presented as direct quotes and their text is *italicized*.

### 3.1 Smart Parking

According to the interviews and the Internet survey, 58 % and 65 % of the Asian people were familiar with smart parking, respectively. The numbers for European people were 36 % and 60 %, respectively. These results are presented in Table 2. There is a significant difference between the results from the interviews and the Internet survey, especially in the case of the European answerers. This can be partly explained by the fact that all of the answerers in the interviews were from Finland, were parking space is not such a big problem, whereas in the Internet survey, there were answerers from several European countries. Also, the fact that the answerers of the Internet survey probably are more familiar with new technologies may have affected the results. It was noticed that a higher percentage of male answerers were familiar with smart parking systems than female answerers (percentages 52 % and 39 %, respectively) but female answerers were more willing to use these systems (93 % of the female and 81 % of the male). In general, smart parking systems were seen in a positive way: 86 % of the European answerers both from the interviews and from the Internet survey considered smart parking to be useful in their lives and the numbers from the Asian answerers were quite similar, being 87 % and 80 %, respectively. Also, about half of all answerers were willing to pay an extra fee for smart parking systems (See Table 2). However, in several comments in was stated that the price must not be too high for them to use the system.

In free comments, especially self-parking cars were mentioned several times. Following quotes are examples of the versatile comments about what is smart parking: *"Something to make your parking easier; cars parking by themselves; cars parking by using sensors; system that will help you to find your car from the parking lot; mobile phone payment and parking space reservation; leaving the car into the parking lot and the car parking itself; poor parking skill people need this system, and specially for the down town (busy) area; automatic parking fee payment system; smart phone can reserve the parking space"*.

### 3.2 Smart Cars and Driving systems

In the interviews, 60 % of the Asian and 70 % of the European answerers were familiar with smart cars and driving systems. However, many of them mentioned that they are only "familiar with the concept" and not with any further details. In the Internet survey, 59 % of the Asian and 90 % of the European were familiar with these applications. It was also again noticed that a higher percentage of male answerers were familiar with smart cars and driving systems than female answerers (percentages 70 % and 59 %, respectively). However, again female answerers were a little bit more willing to use them (85 % of the female and 74 % of the male answerers said "yes").

The terms "smart cars and driving systems" include a huge variety of applications. Also in this study, it came clear from the free comments that different people have very different thoughts about what are smart cars and smart driving systems: some quite basic applications, e.g., lane departure warning were mentioned, whereas others mentioned self-driving cars. This also has an effect on the results of willingness to use the technology, as people probably feel differently about the use of a lane departure warning system than the use of a self-driving car. Thus, these results will only be used to study the feelings of people about the smart applications they know, regardless of what these smart applications actually are. Naturally, the next step is to focus on people's thoughts about specific applications, instead of the whole wide concept. However, according to our results, a major percentage of the answerers thought that they would be willing to use smart cars and driving systems. For the European answerers, the percentages of "yes"-answers in the interviews and in the Internet survey were 84 % and 86 %, respectively and for the Asian answerers the percentages were 73 % and 85 %, respectively.

Following quotes are examples of the comments about what are smart cars and driving systems: *"Google cars; lane departure warning; cars driving by themselves; some small things to help control cars; cars monitoring and sensing the environment; safe cars and safety alerts; automatic maps; checking locations and distances from A to B; some small things to help control cars; for large vehicles; monitor the road temperature; maps and apps"*.

As can be seen from Table 4, the reliability of the technology is the major worry in smart cars and driving systems for both genders and for both European and Asian answerers. Many people chose more than one option as their major worry and cost can be considered as the other main worry. The individual privacy was not generally seen as a major worry. Only among the Asian answerers in the interviews, 40 % of the answerers named it as a major worry. One reason for this may be that car- and driving-related IOT applications do not feel like applications that track their user´s personal information, actions, behavior and ongoing preferences, like some other IOT applications. In general, it seems that Asian people are more worried than people from Europe; the percentages are higher in all options (individual privacy, reliability of technology, practicability, and cost). Also in a previous study about versatile IOT applications, the answerers from Finland were less worried about the individual privacy in the IOT than the answerers from China [13]. Again, it was noticed that the answers gathered by interviews were different to those gathered by the Internet survey, which is an important point to consider in future research.

Smart cars and driving systems also raised a number of questions about future regulations and legislation. In free comments, it was questioned, e.g., that *“when smart cars crash, who will take the responsibility, since the vehicle was driving by itself?”* and”*if one is smart and another is non-smart, how can smart driving system communicate with the regular car or its driver?”*. The legislation, regulations, and standards definitely will require a significant amount of collaborated work before we can drive around with self-driving smart cars, but also before people can completely trust on more basic applications in the field.

As can be seen from Table 5, people have very different thoughts about the possible schedule of smart cars and driving systems coming to everyday use. For example, in the Internet survey, about half of the answerers thought it would happen during following 5-10 years and 20 % of the Asian and 28 % of the European answerers felt that it will take 11-20 years.

**Table 3:** The answers to questions about smart cars and driving systems

| **2a. Have you heard about smart cars and driving systems before?** | | | | |
|---|---|---|---|---|
| **Interviews** | | | | |
| | Asian | European | Male | Female |
| **Yes** | 60 % | 70 % | 70 % | 59 % |
| **No** | 40 % | 30 % | 30 % | 41 % |
| **Internet Survey** | | | | |
| | Asian | European | | |
| **Yes** | 59 % | 90 % | | |
| **No** | 41 % | 10 % | | |
| **2b. Would you be willing to use smart cars and driving systems?** | | | | |
| **Interviews** | | | | |
| | Asian | European | Male | Female |
| **Yes** | 73 % | 84 % | 74 % | 85 % |
| **No** | 27 % | 16 % | 26 % | 15 % |
| **Internet Survey** | | | | |
| | Asian | European | | |
| **Yes** | 85 % | 86 % | | |
| **No** | 15 % | 14 % | | |

**Table 4:** The major worries about smart cars and driving systems

| **3. What are your major worries about smart cars and driving systems, if any?** | | |
|---|---|---|
| | **Interviews** | |
| | Male | Female |
| Your individual privacy | 30 % | 22 % |
| Reliability of technology | 69 % | 61 % |
| Practicability | 17 % | 34 % |
| Cost | 34 % | 54 % |
| Others | 4 % | 5 % |
| | Asian | European |
| Your individual privacy | 40 % | 14 % |
| Reliability of technology | 71 % | 60 % |

| | | |
|---|---|---|
| Practicability | 40 % | 10 % |
| Cost | 54 % | 32 % |
| Others | 2 % | 6 % |
| | **Internet Survey** | |
| | Asian | European |
| Your individual privacy | 26 % | 21 % |
| Reliability of technology | 77 % | 39 % |
| Practicability | 44 % | 12 % |
| Cost | 47 % | 27 % |
| Others | 3 % | 1 % |

**Table 5:** The answers to question about the possible schedule of smart cars and driving systems coming to everyday use

**4. When do you think smart cars and driving systems will be in everyday use?**

| | **Interviews** | | | | **Internet Survey** | |
|---|---|---|---|---|---|---|
| | Male | Female | Asian | European | Asian | European |
| **Near future** | 26% | 27% | 24% | 28% | 24% | 10% |
| **5-10 years** | 28% | 51% | 38% | 38% | 50% | 54% |
| **11-20 years** | 34% | 20% | 27% | 28% | 20% | 28% |
| **> 20 years** | 11% | 2% | 9% | 6% | 6% | 8% |
| **Never** | 1% | 0% | 2% | 0% | 0% | 0% |

**Table 6:** What kind of information would people be willing to allow smart driving systems to record and how worried would they be about their individual privacy.

**5a. Would you allow a smart driving system to record your name and plate number?**

**5b. Would you allow a smart driving system to record your parking time and place?**

**5c. Would you allow a smart driving system to record your vehicle speed?**

**5d. Would you allow a smart driving system to record the information of people who are in your car?**

| | **5a.** | | **5b.** | | **5c.** | | **5d.** | |
|---|---|---|---|---|---|---|---|---|
| | Asian | European | Asian | European | Asian | European | Asian | European |
| **Yes** | 57% | 68% | 58% | 74% | 84% | 74% | 15% | 28% |
| **No** | 43% | 32% | 42% | 26% | 16% | 26% | 85% | 72% |

**How worried would you be about your individual privacy in above situation? (Scale: 1-5)**

| | | Average value |
|---|---|---|
| **5a.** | Asian | 3.23 |
| | European | 3.08 |
| **5b.** | Asian | 3.33 |
| | European | 3.32 |
| **5c.** | Asian | 2.42 |
| | European | 2.94 |
| **5d.** | Asian | 3.80 |
| | European | 3.96 |

In addition, 24 % of the Asian and 10 % of the European felt it will happen in the near future. Similar major dispersion was also found in the answers of the interviews, also shown in Table 5. One major reason for these differences may be the discovered fact that people have very different thoughts about what is meant by smart cars and driving systems. However, this diversity of results is also in line with the diversity of the results of another study, where it was inquired what the answerers think will be the possible schedule for the current Internet to grow into the IOT and this kind of all-around network to come to use [13].

As can be seen from the results presented in Table 6, most people from Europe are willing to let smart driving systems to record their name and plate number, parking time and place, and their vehicle speed. The percentages of "yes"-answers for these situations where 68 %, 74 % and 74 %, respectively. The people from Asia were not as willing to get their name and plate number and the parking time and place recorded, the percentages of "yes"-answers were 57 % and 58 %, respectively. However, 84 % of the answerers from Asia were willing to let their speed be recorded. In this situation (the recording of the vehicle speed) the average number of worry (between 1-5) was the lowest: 2.94 for the European and 2.42 for the Asian answerers. It is notable that, e.g., the vehicle speed and plate number are already recorded in many roads all over the world, with or without the driver willing to give the information. Also, in some countries and regions, it is possible to get your name from your car plate number by a single phone call or text message. According to the results, only 15 % (Asian answerers) and 28 % (European answerers) were willing to let the information about the people who are in their car to be recorded. Thus, there seems to be a strong line of privacy. In this situation also the average value of worry (between 1-5) was the highest: 3.80 for the Asian people and 3.96 for the European people.

## 4. CONCLUSIONS

Due to technology advancement, even cars and driving are becoming "smart". The potential future applications of smart cars and driving systems are endless. In this study, the thoughts of 248 people about these applications were collected from Europe and Asia by interviews and with an Internet survey. The first finding was that people have very different thoughts about what this huge amount of applications, referred as "smart cars and driving systems" means. It was noticed that the majority of the answerers would be willing to use smart cars and driving systems as well as smart parking. In general, the Asian answerers were found to be more worried about these new applications than people from Europe and the reliability of the technology together with cost were considered as the major worries. People were found to be quite willing to let their name and plate number, parking time and place, and vehicle speed to be recorded by these applications. However, the information about the people travelling in the car was considered private. In some cases, a significant difference between the results from the interviews and the Internet survey was noticed, which needs to be taken into account in the future research, when deeper analyses are done.

## ACKNOWLEDGEMENTS

This research was supported by Helsingin Sanomat Foundation and AdvIOT, European Commission Marie Curie IRSES project. The authors would also like to thank the City University of Hong Kong Overseas Internship Scheme 2014.

## REFERENCES

[1] Libelium, "50 Internet of Things applications", 2012. Available at: http://www.libelium.com/top_50_iot_sensor_applications_ranking (accessed 20 July 2014)

[2] B. Guo, D. Zhang, Z. Wang, "Living with Internet of Things: The Emergence of Embedded Intelligence", Proceedings of the Internet of Things (iThings/CPSCom), October 2011.

[3] J.P., Hubaux, S. Capkun, L. Jun, "The Security and Privacy of Smart Vehicles", IEEE Security & Privacy, vol.2, no.3, 2004, pp. 49-55.

[4] M. Sunwoo, K. Jo, D. Kim, J. Kim, C. Jang, "Development of Autonomous Car – Part I: Distributed System Architecture and Development Process", IEEE Transactions on Industrial Electronics, 10p. Published online, DOI: 10.1109/TIE.2014.2321342

[5] M. Gerla, L. Eun-Kyu G. Pau, L. Uichin, "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds", Proceedings of the IEEE World Forum, Internet of Things (WF-IoT), March 2014.

[6] S.V. Srikanth, P.J. Pramod, K.P. Dileep, S. Tapas, M.U. Patil, C.B.N. Sarat, "Design and Implementation of a Prototype Smart PAR King (SPARK) System Using Wireless Sensor Networks", Proceeding of the International Conference on Advanced Information Networking and Applications Workshops, (WAINA '09), May 2009.

[7] G. Revathi, V.R.S. Dhulipala, "Smart Parking Systems and Sensors: A Survey", Proceedings of the International Conference on Computing, Communication and Applications (ICCCA), February 2012.

[8] J. Virkki, "Finnish Perspectives for the IOT", American Journal of Networks and Communications, vol. 2, no. 2, 2013, pp. 23-27.

[9] G. Lingling, B. Xuesong, "A Unified Perspective on the Factors Influencing Consumer Acceptance of Internet of Things Technology", Asia Pacific Journal of Marketing and Logistics, vol. 26, no. 2, 2014, pp.211-231

[10] T. Kowatsch, W. Maass, "Privacy Concerns and Acceptance of IoT Services", The Internet of Things 2012 – New Horizons, IERC Cluster book, Halifax, UK.

[11] H. Wang, Y. Yan, Z. Hu, Y. Zhang, "Consumer Acceptance of IOT Technologies in China: An Exploratory Study", Proceedings of the

International Conference on Technology Education (ICTE), November 2011.

[12] H. Sun, P. Zhang, “The role of Moderating Factors in User Technology Acceptance”, International Journal of Human-Computer Studies, vol. 64, no. 2, 2006, pp. 53-78.

[13] J. Virkki, L. Chen, "Personal Perspectives: Individual Privacy in the IOT", Advances in Internet of Things, vol. 3 no. 2, 2013, pp. 21-26.

## AUTHOR PROFILES

Yan Liu and Yu Zhai are currently studying MSc courses in the Department of Electronic Engineering, City University of Hong Kong, China. They carried out an overseas internship in Tampere University of Technology, Finland, during summer 2014.

Minghao Yang and Feiyuan Long from the Department of Electronic Engineering, City University of Hong Kong, China, carried out technical work in Tampere University of Technology, Finland, as part of the European Commision funded Marie Curie IRSES AdvIOT project during summer 2014.

Johanna Virkki received the MSc and PhD degrees in Electrical Engineering from Tampere University of Technology, Finland, in 2008 and 2010, respectively. She is currently working as a Postdoctoral Researcher with the Department of Electronics and Communications Engineering, Tampere University of Technology, Finland.

**Open Journal of Social Sciences, 2014, 2, **-****
Published Online November 2014 in SciRes. http://www.scirp.org/journal/jss
doi

# A Survey Study of the Usefulness and Concerns about Smart Home Applications from the Human Perspective

**Yu Zhai[1], Yan Liu[1], Minghao Yang[1], Feiyuan Long[1], Johanna Virkki[2]**

[1]Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[2]Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
Email: johanna.virkki@tut.fi

Received **** 2014

## Abstract

**It is not yet clear how smart home technologies and applications will actually be accepted as part of our everyday lives. In this research, the thoughts of 248 people about smart homes were collected by interviews and with an Internet survey in Europe and Asia. It was found that people have very versatile thoughts about what the term "smart home" means in practice and when smart houses will become part of our daily lives. The Asian answerers can be considered to be slightly more optimistic about the schedule. The majority of the answerers were found to be interested in versatile smart home applications and willing to live in a smart house. The cost can be considered to be their biggest worry and the Asian answerers were found to be more worried about the reliability, practicability, and cost than the answerers from Europe. Also some privacy concerns were found from both the European and the Asian answerers.**

## Keywords

**Asia, Europe, Internet Survey, Interviews, Personal Perspectives, Smart Homes**

## 1. Introduction

The growth of the Internet of Things (IOT) means more and more daily things and devices connecting each other and creating a pervasive computing world where they will exchange data and information about the environment, while reacting independently to different events, influencing their surroundings, and creating services with or without human intervention. The IOT has potential applications in all areas of life [1] [2]. Despite the

**How to cite this paper:** Author 1, Author 2 and Author 3 (2014) Paper Title. *Open Journal of Social Sciences*, **2**, **-**.
http://dx.doi.org/10.4236/***.2014.*****

fast development of versatile applications, it is not yet clear which of these will actually be accepted as a part of our daily lives. For example, in a study made in Finland, the IOT and its applications were seen tempting, in principle, but the necessity of the versatile applications was also questioned by the answerers [3]. During the last two decades, user acceptance models to reflect people's willingness to accept new technologies, e.g., smart products [4], have been developed, tested, refined, extended, and unified. For example, in a study from China, the authors proposed an IOT acceptance model consisting of several factors: the results showed particularly strong support for the effects of perceived usefulness, ease of use, enjoyment, and behavioral control, and also of social influence [5]. Also the results of another study showed that the acceptance of IOT services would be affected by various contradicting factors, such as perceived privacy risks and personal interests. It was also assumed that legislation, data security and transparency of information influence the adaptation [6]. In a yet another study, made in China, it was found that usefulness plays an important role in acceptance of the IOT [7].

One of the most important IOT application areas are smart houses [8]. Smart home, comprising smart devices and things in the home context, promises enormous possibilities to our future life, e.g., by automation of the home, housework, or household activities. At the same time, smart homes will probably have their own influence to change our living habits. Moreover, as home is not just a physical house for people [9], in addition to technology development, the needs and thoughts of future smart home inhabitants also need to be studied. For example, a survey focusing on the activities and habits that people do at home that they would not want to be recorded has been conducted, and bedroom has been found to be the most private place [10]. One of the most important challenges in convincing users to adopt this kind of all-around network in their home is the protection of privacy. Concerns over privacy can spread wide, particularly as these wireless systems can track users' actions, behaviour and ongoing preferences. Possible privacy problems, however, are not caused by the technology alone, but primary through activities of people, businesses, and the government [11] [6]. One study exploring the social barriers to smart home diffusion, including how these vary by expertise, life-stage, and location, highlighted the importance of control, security, and cost [12]. The results of another study, analyzing the attitudes of users towards different types of ambient assisted living services, showed that users were not yet (in 2011) very familiar with the vision of smart technology at home and reported hesitancy and aloofness towards using such technologies. Persons with many social contacts and a high interest in technology showed the highest acceptance for electronic services at home. The results for the different applications were insensitive to gender and age [13]. One major reason for the unenthusiastic acceptance might be the fact that current developments in this sector are in many parts focusing on technical feasibility, inspired by technical disciplines, leaving the human factor in these systems fairly under developed. However, at least at the current maturity of technical solutions, the human perspective should be incorporated into technical designs as soon as possible [14].

The personal thoughts and feelings of people who are potential end users of the IOT and its applications, *i.e.*, "ordinary people", are an important research area. In this research, the thoughts of 248 people from Europe and Asia were collected by interviews and with an Internet survey. The main focus was to find answers to the following questions:

1) Are the answerers already familiar with smart houses and smart home applications?

2) Do the answerers feel that smart home applications would be useful in their lives?

3) Are there any privacy concerns or concerns about the practicability, cost, or reliability of the technology used in these applications?

This paper is organized as follows: The introduction section introduces the topic and the goals of this study. Section 2 presents the performed interviews and the Internet survey, including the information on the answerers and the presented questions. The collected answers and examples from free comments are presented and discussed in Section 3. The last section summarizes the results and presents the conclusions of this paper.

## 2. Interviews and Internet Survey

All the data for this research was collected during June-August 2014. In the first part of this research, 95 people were interviewed and **Table 1** shows more information about the answerers. People of different age, of both gender and of different occupation were chosen from Europe (50 people, all of them from Finland) and from Asia (45 people, all of them from Hong Kong and mainland China). Personal interviews took place either at the answerers working facility or at a neutral, public place. Some of the interviews were done by private e-mails between the researcher and the answerer. All these interviews thus had more flexibility than an anonymous paper

**Table 1.** The answerers of this study.

| | | Internet survey | | | Interviews | | |
|---|---|---|---|---|---|---|---|
| | | Asian | European | All | Asian | European | All |
| **All** | | 103 | 50 | 153 | 45 | 50 | 95 |
| **Gender** | Male | 50 | 26 | 76 | 25 | 29 | 54 |
| | Female | 53 | 24 | 77 | 20 | 21 | 41 |
| **Age** | 18 - 25 | 74 | 18 | 92 | 30 | 23 | 53 |
| | 26 - 35 | 20 | 25 | 45 | 15 | 13 | 28 |
| | 36 - 45 | 3 | 4 | 7 | 0 | 6 | 6 |
| | 46 - 55 | 6 | 1 | 7 | 0 | 6 | 6 |
| | >55 | 0 | 2 | 2 | 0 | 2 | 2 |

or Internet survey, as both the researcher and the answerer were able to ask for clarification. However, personal interviews are quite time-consuming and thus also a more effective method to gather data was needed.

The second part of this study was an Internet survey, where 153 answers were collected, again from people of different age, of both gender, and of different occupation (also shown in **Table 1**). There were 50 people from Europe (from Finland, Sweden, Portugal, Germany, Italy, Bulgaria, Norway, Russia, Slovenia, United Kingdom, Spain, and France) and 103 from Asia (from mainland China, Hong Kong, Iran, India, Korea, and Afghanistan).

The interviews consisted of the following questions:

1a) Have you heard about smart homes before? (Yes/No)

1b) What have you heard about them? What do you know about smart homes?

1c) Would you be willing to live in a smart home? (Yes/No)

2) What kind of smart home applications are you or your friends/family interested in? (Including a list of applications)

3) What are your major worries about smart homes, if any? (Including a list of possible worries)

4) When do you think smart homes will become a part of our everyday life?

The Internet survey covers all the questions from the interviews and the following extra question:

5a) Would you allow your smart home to record people's personal information when they enter the house? (Yes/No)

5b) Would you allow your smart home to record your movement around the house? (Yes/No)

5c) Would you allow your smart home to record your house health status? (Yes/No)

5d) Would you allow your smart home to record your personal health status? (Yes/No)

Also: How worried would you be about your individual privacy in above situations 5(a)-5(d)? (Scale: 1 - 5; 1 = not worried at all, 5 = very worried).

## 3. Results and Discussion

This section introduces and discusses the collected answers. All the examples of the achieved free comments are presented as direct quotes and their text is *italicized.*

As can be seen from **Table 2**, 76% of the Asian and 64% of the European answerers in the interviews were familiar with smart homes. The percentages were 74% (Asian) and 88% (European) in the Internet survey. There is a significant difference between the results from the interviews and the Internet survey in the case of the European answerers. This can be partly explained by the fact that all of the answerers in the interviews were from Finland, whereas in the Internet survey there were answerers from several European countries. Thus, one limitation in the use of the interview results of this study is that people from Finland and China are not representative enough to reflect the attitudes of European people and Asian people, respectively. However, also the fact that the answerers of the Internet survey probably are more familiar with new technologies in general may have affected the results. The percentages of Asian answerers were similar in the interviews and in the Internet survey also with question 1(c), where 82% (interviews) and 86% (Internet survey) of the Asian answerers were

**Table 2.** Answers to questions 1(a) and 1(c) about smart homes.

| 1(a). Have you heard about smart homes before? | | |
|---|---|---|
| | Interviews | |
| | Asian | European |
| Yes | 76% | 64% |
| No | 24% | 36% |
| | Internet survey | |
| | Asian | European |
| Yes | 74% | 88% |
| No | 26% | 12% |
| **1(c). Would you be willing to live in a smart home?** | | |
| | Interviews | |
| | Asian | European |
| Yes | 82% | 74% |
| No | 18% | 26% |
| | Internet survey | |
| | Asian | European |
| Yes | 86% | 92% |
| No | 14% | 8% |

willing to live in a smart home. Again, there was a difference in the answers from Europe: 74% (interviews) and 92% (Internet survey) were willing to live in a smart home. However, according to these results, in all cases, the majority of the answerers were willing to live in a smart home.

Following quotes are examples of the versatile comments about what people have heard or what they know about smart homes: "*App to control everything*; *automatic AC*, *lights*, *heating*; *sound control for the lights*; *refrigerators can order food automatically*; *automatically monitor electricity usage*; *lock home and alarm system*; *wireless detector to detect who is in your home*; *iPad can control the home applications*; *solar energy roof*; *home appliances are connected by the wireless network*; *automatically tell you what is turned on*/*off by phone*".

Automatic heating and lightning control were the most often mentioned applications and also automatic fridge was mentioned several times. Some of the answerers from Finland mentioned smart or automatic sauna. In free comments, it was stated that modern houses already can have smart hardware installed and thus it should be easy to implement a smart home. However, it was also commented that integration of such smart applications to existing houses may be difficult and expensive. In some comments, the whole concept was questioned and it was, e.g., stated that smart homes are "*only things seen in the movies*". Many people also commented that although they have heard about smart homes, they do not actually know what the smart homes will be like in real life and what they can expect and demand from the future smart applications at home. Thus, also the results of the acceptance of the whole smart home concept in this study have to be seen as acceptance of what the answerers think the future smart homes will be like and what applications they think smart homes will include.

The smart home applications in this study were chosen to be from versatile areas of everyday life. In **Table 3**, it is presented what kind of smart home applications the answerers were interested in. Many people chose more than one application and all of the applications gained some interest. However, in free comments it was, e.g., stated that people are "*living just fine without these new applications*". These comments are in line with the earlier mentioned results achieved in [3]. As can be seen, a single application cannot be named to be the most popular, although, e.g., temperature & humidity control and smart cleaning can be considered to be interesting ones among all answerers. In the future, it is important to study the opinions and interests of people application by application and also empirical user studies can be valuable. For example, in one study, a simulation of a smart fridge was developed and the people's opinions on smart fridge offering different assistance functions were studied [15]. In our study, the Asian answerers were more interested in different smart home applications than the answerers from Europe. It was also noticed that the European Internet survey answerers were not particularly interested in any of the applications, compared to all other answerers. It is surprising, since 92% of them answered that they would like to live in a smart home.

The answers to question about the major worries related to smart homes can be seen in **Table 4**. In general, the Asian people were more worried than the people from Europe; the percentages are higher in all options (individual privacy, reliability of technology, practicability, and cost) and the same result was achieved both in the Internet survey and in the interviews. Also in a previous study about versatile IOT applications, the answerers from Finland were less worried about the individual privacy in the IOT than the answerers from China [16]. Among the Asian answerers, cost can be named as the biggest worry, although also other percentages were quite high. In the European interviews (people from Finland), cost was clearly the main worry. However, among the European answerers of the Internet survey, there is no single major worry.

**Table 3.** Answers to question 2 about smart homes.

| 2. What kind of smart home applications are you or your friends/family interested in? | | | | |
|---|---|---|---|---|
| **Interviews** | | | **Internet survey** | |
| | Asian | European | Asian | European |
| Security control | 56% | 40% | 44% | 14% |
| Temperature & humidity control | 49% | 52% | 65% | 11% |
| Smart lighting | 51% | 36% | 69% | 10% |
| Home entertainment system | 38% | 26% | 57% | 11% |
| Yard management system | 31% | 14% | 39% | 4% |
| Smart cleaning | 53% | 50% | 75% | 11% |
| Senior nursing system | 53% | 26% | 60% | 7% |
| Childcare system | 42% | 20% | 74% | 7% |
| Disabled nursing system | 40% | 12% | 29% | 2% |
| Energy management system | 47% | 40% | 69% | 11% |
| Window & curtain control system | 22% | 18% | 56% | 8% |
| Pets feeding system | 7% | 16% | 33% | 5% |

**Table 4.** Answers to question 3 about smart homes.

| 3. What are your major worries about smart homes, if any? | | | | |
|---|---|---|---|---|
| | **Interviews** | | **Internet survey** | |
| | Asian | European | Asian | European |
| Yourindividualprivacy | 56% | 38% | 37% | 30% |
| Reliability of technology | 49% | 28% | 55% | 27% |
| Practicability | 53% | 6% | 53% | 15% |
| Cost | 62% | 54% | 61% | 26% |
| Other | 2% | 2% | 2% | 2% |

As can be seen from **Table 5**, people have very different thoughts about the possible schedule of smart homes coming to everyday use. For example, in the Internet survey, 42% of the answerers thought it would happen during following 5 - 10 years and 29% of the Asian and 38% of the European answerers felt that it will take 11 - 20 years. In addition, 21% of the Asian and 8% of the European felt it will happen in the near future. In general, the Asian answerers can be considered to be slightly more optimistic about the schedule. None of the answerers felt that this would never happen. Similar major dispersion was also found in the answers of the interviews, also shown in **Table 5**. One major reason for these differences may be the found fact that people have very different thoughts about what is meant by smart homes coming to everyday life and even what is meant by smart home. However, this diversity of results is also in line with the diversity of the results of another study (published 2013), where it was inquired what the answerers think will be the possible schedule for the current Internet to grow into the IOT and this kind of all-around network to come to use [16].

The privacy concerns of future smart technology users are an important research area. For example, in one study, the reputation of the retailer and acceptance of RFID-based information services was investigated. Results showed that people are moderately privacy aware and that their privacy awareness is negatively related to their acceptance of the service. Also, a group of "extreme rejecters" that hold highly negative attitudes and significantly bias group means were found [17]. Also in our study, when the answerers were asked to give a number for their amount of worry about their individual privacy in different scenarios, the whole scale from 1 to 5 was used by the answerers. For our study, we chose 4 different scenarios (5(a) - 5(d)) and chose to present the average number of worry for each group (see **Table 6**). In an earlier study about people's worries related to their individual privacy, among different IOT applications, the applications related to personal health were considered the least worrying ones and the applications related to personal finances were found to be the most worrying ones [16].

It can be seen from **Table 6** that about half of all the Asian answerers and 32% of the European answerers would allow a smart home to record people's personal information when they enter the house. The average number of worry in this situation was 3.55 for the Asian and 3.72 for the European answerers. Only 31% of the Asian would allow the house to record their movement around the house, whereas the percentage for European answerers was 60%. There was also a difference in the average value of worry in this question; the average value of worry (between 1 - 5) was 3.65 for the Asian and 3.14 for the European answerers. Almost all of the answerers would allow their smart home to record the house health status and the average numbers of worry were also quite low in this case for both Asian and European answerers; 2.35 and 2.22, respectively. Also, 83% of the Asian and 78% of the European answerers would allow their own personal health status to be monitored by their house. The average number of worry for Asian and European answerers was 2.79 and 3.18, respectively. Thus, people were quite willing to let their smart home to record information about their own health and the health of the house but not so willing to let people's personal information or their movement around the house to be recorded.

## 4. Conclusions

The personal thoughts and feelings of people who are potential end users of the IOT and its applications, *i.e.*, "ordinary people" offer important information for people working to develop the IOT and its applications, e.g.,

**Table 5.** Answers to question 4 about smart homes.

| **4. When do you think smart homes will become a part of our everyday life?** | | | | |
|---|---|---|---|---|
| | **Interviews** | | **Internet survey** | |
| | Asian | European | Asian | European |
| In the near future | 24% | 18% | 21% | 8% |
| During 5 - 10 years | 36% | 26% | 42% | 42% |
| During 11 - 20 years | 29% | 36% | 29% | 38% |
| Morethan 20 years | 11% | 20% | 8% | 12% |
| Never | 0% | 0% | 0% | 0% |

**Table 6.** Answers to question 5 about smart homes.

| **5(a). Would you allow your smart home to record people's personal information when they enter the house?**<br>**5(b). Would you allow your smart home to record your movement around the house?**<br>**5(c). Would you allow your smart home to record your house health status?**<br>**5(d). Would you allow your smart home to record your personal health status for your safety and health?** | | | |
|---|---|---|---|
| | | **Yes** | **No** |
| **5(a)** | Asian | 47% | 53% |
| | European | 32% | 68% |
| **5(b)** | Asian | 31% | 69% |
| | European | 60% | 40% |
| **5(c)** | Asian | 95% | 5% |
| | European | 94% | 6% |
| **5(d)** | Asian | 83% | 17% |
| | European | 78% | 22% |

| **How worried would you be about your individual privacy in above situation?** | | |
|---|---|---|
| | | **Average value** |
| **5(a)** | Asian | 3.55 |
| | European | 3.72 |
| **5(b)** | Asian | 3.65 |
| | European | 3.14 |
| **5(c)** | Asian | 2.35 |
| | European | 2.22 |
| **5(d)** | Asian | 2.79 |
| | European | 3.18 |

smart home applications. In this research, the thoughts of people about different aspects of smart homes were collected. It was found that majority of the answerers were somehow familiar with smart homes and also willing to live in a smart house. However, people were found to have different thoughts about what is actually meant by smart homes and they also had different thoughts about the possible schedule of smart homes coming to everyday use. The Asian answerers can be considered to be slightly more optimistic about the schedule than the answerers from Europe. People were found to be interested in versatile smart home applications and cost can be considered to be the biggest worry. In general, the Asian people were more worried about the reliability, practicability, and cost than the people from Europe. Also some concerns about the individual privacy were found both from Europe and Asia, related to a smart home recording the habits, movement, and information of the inhabitants. In future research, it is also important to study the smart home environment application by application, not just the whole wide concept.

## Acknowledgements

This research was supported by Helsingin Sanomat Foundation. The authors would also like to thank the City University of Hong Kong Overseas Internship Scheme 2014.

## References

[1] Libelium (2012) 50 Internet of Things Applications. http://www.libelium.com/top_50_iot_sensor_applications_ranking

[2] Guo, B., Zhang, D. and Wang, Z. (2011) Living with Internet of Things: The Emergence of Embedded Intelligence.

*Internet of Things* (*iThings*/*CPSCom*).

[3] Virkki, J. (2013) Finnish Perspectives for the IOT. *American Journal of Networks and Communications*, **2**, 23-27.

[4] Mayer, P., Volland, D., Thiesse, F. and Fleisch, E. (2011) User Acceptance of "Smart Products": An Empirical Investigation. *Wirtschaftsinformatik Proceedings*, Paper 9.

[5] Gao, L.L. and Bai, X.S. (2014) A Unified Perspective on the Factors Influencing Consumer Acceptance of Internet of Things Technology. *Asia Pacific Journal of Marketing and Logistics*, **26**, 211-231. http://dx.doi.org/10.1108/APJML-06-2013-0061

[6] Kowatsch, T. and Maass, W. (2012) Privacy Concerns and Acceptance of IoT Services. The Internet of Things 2012—New Horizons, IERC Cluster Book, Halifax.

[7] Wang, H., Yan, Y., Hu, Z. and Zhang, Y. (2011) Consumer Acceptance of IOT Technologies in China: An Exploratory Study. *International Conference on Technology Education* (*ICTE*), Chengdu, 23-25 July 2011, 2430-2435.

[8] Aldrich, F. (2003) Smart Homes: Past, Present and Future, In: Harper, R., Ed., *Inside the Smart Home*, Springer Verlag, Berlin, 17-36. http://dx.doi.org/10.1007/1-85233-854-7_2

[9] Saizmaa, T. and Hee-Cheol, K. (2008) Smart Home Design: Home or House? *International Conference on Convergence and Hybrid Information Technology*, Busan, 11-13 November 2008, 143-148.

[10] Choe, E.K., Consolvo, S., Jung, J., Harrison, B. and Kientz, J.A. (2011) Living in a Glass House: A Survey of Private Moments in the Home. In: *Proceedings of the* 13*th International Conference on Ubiquitous Computing*, ACM, New York, 41-44.

[11] Solove, D.J. (2006) A Taxonomy of Privacy. *University of Pennsylvania Law Review*, **154**, Paper No. 129.

[12] Balta-Ozkan, N., Davidson, R., Bicket, M. and Whitmarsh, L. (2013) Social Barriers to the Adoption of Smart Homes. *Energy Policy*, **63**, 363-374. http://dx.doi.org/10.1016/j.enpol.2013.08.043

[13] Ziefle, M., Rocker, C. and Holzinger, A. (2011) Perceived Usefulness of Assistive Technologies and Electronic Services for Ambient Assisted Living. *Proceedings of the* 5*th International ICST Conference on Pervasive Computing Technologies*, Dublin, 23-26 May 2011, CD-ROM.

[14] Gaul, S. and Ziefle, M. (2009) Smart Home Technologies: Insights into Generation-Specific Acceptance Motives, HCI and Usability for e-Inclusion. *Lecture Notes in Computer Science*, **5889**, 312-332. http://dx.doi.org/10.1007/978-3-642-10308-7_22

[15] Rothensee, M. (2008) User Acceptance of the Intelligent Fridge: Empirical Results from a Simulation. The Internet of Things. *Lecture Notes in Computer Science*, **4952**, 123-139. http://dx.doi.org/10.1007/978-3-540-78731-0_8

[16] Virkki, J. and Chen, L. (2013) Personal Perspectives: Individual Privacy in the IOT. *Advances in Internet of Things*, **3**, 21-26. http://dx.doi.org/10.4236/ait.2013.32003

[17] Rothensee, M. and Spiekermann, S. (2008) Between Extreme Rejection and Cautious Acceptance, Consumers' Reactions to RFID-Based IS in Retail. *Social Science Computer Review*, **26**, 75-86.

*Social Networking*, 2014, 3, 41-49
Published Online January 2014 (http://www.scirp.org/journal/sn)
http://dx.doi.org/10.4236/sn.2014.31005

# Perspectives for Sharing Personal Information on Online Social Networks

**Chi Kin Chan[1], Johanna Virkki[2]**
[1]Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[2]Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
Email: ckchan334@student.cityu.edu.hk, johanna.virkki@tut.fi

Received November 21, 2013; revised December 23, 2013; accepted January 11, 2014

## ABSTRACT

**The goal of this research was to study how people feel about sharing personal information on social networks. The research was done by interviews; 50 people were interviewed, mostly from mainland China, Hong Kong, and Finland. This paper presents the included 12 questions and discusses the collected answers. It was discovered, e.g., that 38 out of the 50 answerers use social media every day and share versatile personal information on the Internet. Half of the answerers also share information about other people on the Internet. It was also discovered that compared to male answerers, the female answerers were more active in sharing information about other people. There was a significant variety in opinions: what should be the age limit for sharing personal information online, while 22 out of the 50 answerers felt that there is no need for an age limit at all. According to the answers, only a few people use social media for making new friends. Instead, an important reason for using social media is that their existing friends are using. An interesting finding was that the answerers see the Internet as a part of the real world; the privacy that you have on the Internet is the privacy that you have in the real world.**

## KEYWORDS

**Information Sharing; Social Media; Social Networks; Personal Information; Privacy**

## 1. Introduction

New social media applications are constantly booming. The trend of always increasing number of users who share multimedia content with real or virtual friends was highlighted in a study that measured the consumer usage, attitude, and interest in adopting social media platforms. It was conducted in 29 countries and involved 17,000 individuals [1]. With the even growing popularity and usage of online social media services, people now have accounts (sometimes several) on multiple and diverse services.

The personal information commonly shared on social media includes, e.g., personal identifiers (name, birth date, photos), contact information (email and physical addresses, telephone numbers), social links (friends, interests), and online activities (search history, games). Besides the information that the user knowingly discloses, the use of the network itself reveals information to the service provider; e.g., IP (Internet Protocol) address, used browser, time of connection, and other visited profiles. This information can also allow the service provider to customize its services on the basis of the secondary data collected. Available information can be used to create a digital footprint of any user using social media services [2-4].

While sharing information is the main purpose of social media, privacy is the major concern; it has been noted that some people aren't concerned about security and privacy on social media sites, although one of their main reasons for using such sites is to share information [5,6]. Also, most users click to accept privacy notices and consent declarations without reading or understanding them [7]. However, the data collected in social networking services tend to last, with the added risk of being linked in diverse ways. This combination of disclosure, storage, and linkage is the core of the privacy problem. Thus, one important issue related to these different social media applications is the data aggregation (combining seemingly non-sensitive separate bits of information may well reveal additional, possibly sensitive, information). Similar effect can occur when data collected for one purpose are used for a different purpose without the person's approval [8,9].

Individual privacy in social media is an active research area. For example, a study that investigated American, Chinese, and Indian social networking site users' privacy attitudes and practices, based on 924 responses, found the American respondents to be the most privacy concerned, followed by the Chinese and Indians, respectively [10]. In a study, where opinions on individual privacy were collected from 22 people working with different aspects of research and development of the Internet of Things (IOT) in China and Finland, individual privacy problems existing today were stated. In general, the answerers from Finland were less worried about the individual privacy in different IOT applications than the answerers from China [11]. In a yet another study, French and Chinese social network service users did possess significantly different privacy belief and trust. Specifically, French users were found to be more concerned about their privacy while using the Internet and they felt less comfortable in giving personal info [12]. Also, in one study, individuals using Facebook and MySpace expressed similar levels of concern regarding Internet privacy. Facebook users were more trusting of the site and its members, and more willing to include identifying information in their profile. However, MySpace users were more active in the development of new relationships. It was concluded that the interaction of trust and privacy concern in social networking sites is not yet understood to a sufficient degree to allow accurate modeling of behavior and activity [13].

Also, the behavior and thoughts of active users of social media, the teenagers, have been studied. Teens share a wide range of information about themselves on social media sites; also the sites themselves are designed to encourage the sharing of information and the expansion of networks. However, few teens have a fully public approach to social media. Instead, they take a selection of steps to restrict and prune their profiles, and their patterns of reputation management on social media vary greatly according to their gender and network size; girls are more likely than boys to restrict access to their profiles. These are among the key findings of a survey of 802 teens, which examined their privacy management on social media sites [14]. In addition, according to a survey of 802 parents and their teenage children, most parents of teenagers are concerned about what their teenage children do online and how their behavior could be monitored by others. Some parents are taking steps to observe, discuss, and check up on their children's digital footprints [15]. In a yet another study, it was found out that students are more likely to have a private profile in social media if their friends and roommates also have. In addition, women are more likely to have private profiles than men, and having a private profile is associated with a higher level of online activity [16]. A gender gap when it comes to the way male and female social media users choose to manage their profiles was also found in another study [17]. According to findings of this study, women are much more conservative in the basic settings they choose in social media; 67% of female profile owners restrict access to friends only compared with 48% of male profile owners.

In this study, "social media" refers to social networking sites, like Google+, Facebook, and LinkedIn, as well as to information- and media-sharing sites, like Twitter and Instagram. This work shares some similar objects to the studies above. The goal is to gather the thoughts that people have about sharing their own personal information, as well as sharing personal information about other people in social media. It has been stated that what really haunts people is typically user-generated content, *i.e.*, information that people themselves, their friends, and other social media users upload to social media websites [7]. It has also been stated that privacy problems are not caused by the technology alone, but primary through activities of people, businesses, and governments [18].

## 2. Survey

For this research, 50 people from Asia (38 people) and Europe (12 people) were interviewed. Most of the answerers were from mainland China, Hong Kong, and Finland, but there were also individual answerers from Singapore, Ireland, and Russia. People of different age and of both gender (see **Table 1**), were interviewed. Personal interviews were conducted by an associate of the researcher, and they took place at a neutral, public place. Some of the interviews were done by private e-mails between the researcher and the answerer, and some of the answers were collected with an Internet questionnaire. This study consists of 12 questions that are listed in **Table 2**.

## 3. Results and Discussion

Question 1 wanted to know how often the answerers use

**Table 1. Genders, age groups, and nationalities of the answerers in this study.**

| Gender | | | Age group | | | | Nationality | |
|---|---|---|---|---|---|---|---|---|
| All | M | F | <20 | 20 - 30 | 30 - 40 | 50 - 60 | Asian | European |
| 50 | 31 | 19 | 3 | 40 | 6 | 1 | 38 | 12 |

**Table 2. Questions of the study.**

1. How often do you visit social networking websites?
- <1 day per week
- 1 to 3 days per week
- 4 to 6 days per week
- Everyday

2. Why are you using these?
- Because your friends are using
- Because it is an easy way to get new information
- Because you want to share something interesting with others
- Because you want to make new friends
- Because it is easy to keep contact with friends abroad
- Because it can closer the relationship between people
- Because you want to record important things in your life
- Other

3. What personal information do you share on the Internet?
- Photo
- Name
- Age
- Gender
- Nationality
- Birthday
- Relationship status
- Home address
- Mobile number
- E-mail address
- Workplace
- Education background
- Other

4. Who has access to your information?
- Your family members
- Your boyfriend/girlfriend/spouse
- Your friends
- Your colleagues
- Anyone
- Other

5. What are your considerations before you share some information?
- Importance of information
- Safeness of website
- Necessity of sharing
- Number of possible viewers
- Identity of possible viewers
- Possible consequences of sharing
- Other

6. Do you share information about other people on the Internet? Yes/No

7. Do you ask for permission before sharing the information? Yes/No

8. Why/Why not?

9. Do you think there should be an age limit for people to share their information on the Internet? If yes, what is the appropriate age?
- <10 years old
- 10 - 13 years old
- 14 - 17 years old
- 18 - 21 years old
- >21 years old
- No age limit required

10. Informational privacy is the right of an individual to exercise control over the collection, use, disclosure, and retention of his or her personal information. Do you think there are differences between privacy on the Internet and privacy in the real world? Yes/No

11. If yes, what are the differences?/If no, why?

12. How much do you think a person can currently affect his/her own individual privacy on the Internet? Scale = 1 - 5, where 1 = A person can completely control his/her own individual privacy, 5 = A person has no control over his/her own individual privacy

social networking websites. The answers can be seen in Table 3. According to these results, 38 answerers out of the total 50 use social media every day. Only 4 answerers use social media less that 1 day a week. These numbers can also be supported by a study published at the beginning of 2012, where it was found out that two-thirds of online adults have a profile on a social networking site [17].

The possible reasons for their use of social media were asked in Question 2, and the answers can be seen in Table 4. Two of the most popular reasons were "because your friends are using" (42 answerers out of the total 50) and "because it is an easy way to get new information" (41/50). Many of the answerers gave more than one reason. Quite surprisingly, only 4 people answered their reason for the use of social media to be making new friends. There were 3 answerers who had some other reason for their use and one of them explained the reason to be "work-related". Nowadays many people have a "work profile" on social media and this profile may be totally separated from their real-life friends. It can also be assumed that different social media sites are used for different reasons. This was also discussed in a study where a comparative analysis showed that Facebook is about having fun and knowing about the social activities occurring in one's social network, whereas instant messaging is geared more toward relationship maintenance and development [19].

In Question 3, it was asked what personal information the answerers are willing to share on the Internet. These results can be found from Table 5. As natural, name (45/50) and photo (42/50) were the most shared pieces of information. It should be noted, however, that many people have to share their photo, name, mobile number, and e-mail address on the Internet because of their work. However, 32 people out of the total 50 also share their birthday on the Internet, which probably is not needed for work. The natural next things to ask in Question 4, was who has access to that shared information. These results can be seen in Table 6. Only 9 out of the total 50 answerers allow anyone to see their information. These answerers probably include people who have to share something because of their work. This result is in line with the results achieved in [14]. Only 24 and 21 answered their family and spouse, respectively, to have access to their information, whereas 43 out of the total 50 answered that their friends are allowed to see their information. Some people probably count their spouse and family into their "Internet-friends". However, not everybody just wants to share the same information with their family and with their friends.

In Question 5, the possible considerations before sharing personal information on the Internet were asked. The importance of the information (31 answerers out of the total 50) and the necessity of sharing (27/50) were the most often mentioned considerations. Instead, the number (12/50) and identity (17/50) of the possible viewers were the least mentioned considerations. Again, many people gave more than one answer. These results are presented in Table 7.

**Table 3. Answers to Question 1; How often do you visit social networking websites (How many days a week)?**

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| <1 day | 4 | 2 | 2 | 1 | 3 |
| 1 - 3 days | 2 | 1 | 1 | 0 | 2 |
| 4 - 6 days | 6 | 5 | 1 | 5 | 1 |
| Every day | 38 | 23 | 15 | 32 | 6 |

**Table 4. Answers to Question 2; Why are you using these?**

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| Because your friends are using | 42 | 25 | 17 | 34 | 8 |
| Because it is an easy way to get new information | 41 | 24 | 17 | 33 | 8 |
| Because you want to share something interesting with others | 21 | 11 | 10 | 16 | 5 |
| Because you want to make new friends | 4 | 3 | 1 | 3 | 1 |
| Because it is easy to keep contact with friends abroad | 27 | 16 | 11 | 23 | 4 |
| Because it can closer the relationship between people | 18 | 10 | 8 | 14 | 4 |
| Because you want to record important things in your life | 14 | 4 | 10 | 11 | 3 |
| Other | 3 | 2 | 1 | 0 | 3 |

**Table 5.** Answers to Question 3; What personal information do you share on the Internet?

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| Photo | 42 | 24 | 18 | 32 | 10 |
| Name | 45 | 28 | 17 | 33 | 12 |
| Age | 23 | 14 | 9 | 18 | 5 |
| Gender | 39 | 22 | 17 | 33 | 6 |
| Nationality | 27 | 16 | 11 | 19 | 8 |
| Birthday | 32 | 16 | 16 | 26 | 6 |
| Relationship status | 14 | 9 | 5 | 10 | 4 |
| Home address | 2 | 2 | 0 | 1 | 1 |
| Mobile number | 4 | 3 | 1 | 2 | 2 |
| E-mail address | 23 | 14 | 9 | 20 | 3 |
| Workplace | 12 | 7 | 5 | 6 | 6 |
| Education background | 25 | 14 | 11 | 17 | 8 |
| Other | 1 | 1 | 0 | 1 | 0 |

**Table 6.** Answers to Question 4; Who has access to your information?

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| Family | 24 | 17 | 7 | 20 | 4 |
| Spouse | 21 | 13 | 8 | 17 | 4 |
| Friends | 43 | 27 | 16 | 35 | 8 |
| Colleagues | 22 | 14 | 8 | 17 | 5 |
| Anyone | 9 | 5 | 4 | 5 | 4 |
| Other | 2 | 1 | 1 | 1 | 1 |

**Table 7.** Answers to Question 5; What are your considerations before you share some information?

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| Importance of information | 31 | 22 | 9 | 26 | 5 |
| Safeness of website | 24 | 15 | 9 | 17 | 7 |
| Necessity of sharing | 27 | 16 | 11 | 20 | 7 |
| Number of possible viewers | 12 | 6 | 6 | 10 | 2 |
| Identity of possible viewers | 17 | 11 | 6 | 13 | 4 |
| Possible consequences of sharing | 20 | 13 | 7 | 12 | 8 |
| Other | 0 | 0 | 0 | 0 | 0 |

In Question 6, it was asked if the answerers share information about other people on the Internet. The answers are shown in **Table 8**. According to these results, about half of the answerers (26 answerers out of the total 50) do share information about other people. It can be seen that among the male answerers, there are less people (12/31) who share information about other people than among the female answerers (14/19). In Question 7, more information was asked from those who do share information about other people, particularly, do the answerers ask for permission before sharing the information. These answers can be seen in **Table 9**. As can be seen, out of the total 26 answerers, who share information about other people, 18 say that they also ask for permission before sharing. It can also be seen that male answerers (10/12) ask for permission more often than female answerers (8/14). These are interesting findings as in earlier studies, e.g., [14,16,17] it has been found out that compared to male users, female social media users are more concerned about the privacy of, at least, their own profile. In Question 8, it was asked Why/Why not do the answerers ask for permission before sharing information about other people. Examples of the most common given answers are presented in Table 10. The main reasons for not sharing were, as one can expect, courtesy and respect to other people's privacy. On the other hand, in other answers, it was stated many times that there is no need to ask for permission before sharing information about other people. It was also mentioned that the shared information is nothing important and that is why the people will not mind the sharing.

In Question 9, it was asked if there should be an age limit for people to share their information on the Internet. The results can be seen in Table 11. Almost half of the answerers (22 answerers out of the total 50) felt that there is no need for an age limit and 5 answerers felt that

**Table 8. Answers to Question 6; Do you share information about other people through the Internet?**

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| Yes | 26 | 12 | 14 | 19 | 7 |
| No | 24 | 19 | 5 | 19 | 5 |

**Table 9. Answers to Question 7; Do you ask for permission before sharing the information?**

| | All N = 26 | Male N = 12 | Female N = 14 | Asian N = 19 | European N = 7 |
|---|---|---|---|---|---|
| Yes | 18 | 10 | 8 | 13 | 5 |
| No | 8 | 2 | 6 | 6 | 2 |

**Table 10. Question 8; Why/Why not?**

**YES**

- "May contain sensitive information"
- "To respect my friends and protect their privacy to some extent"
- "A basic courtesy is to respect the privacy of others"
- "It's their privacy and the rights remain with them."
- "Respect"
- "Privacy"
- "Public image matters."
- "If I would share, I would ask, naturally."

**NO**

- "No need. If it's too bad, I won't."
- "They know what I do."
- "If they don't like they will del tag."
- "I think they won't feel bad for the sharing."
- "Just small things, not important!"
- "Because I think the information will not affect the person in a bad way. For example I will share a photo which is my friend and I stay together and do something together. It is somehow like information that sharing what my friend and I has done. Some photo will be eliminated instead of uploaded such as a naked photo of my friend."
- "It seems not necessary to ask for permission."
- "They didn't ask for."

the age limit should be under 10 years. However, there were also 11 answerers who felt that the age limit should be over 18 years. Thus, there is a significant variety in opinions. Currently the age limit in many social networking sites is 13 years. However, in many social networking websites the age verification systems can be passed solely by the children lying about their age.

In Question 10, it was asked if the answerers feel that there are differences between privacy on the Internet and privacy in the real world. The answers can be found from Table 12. More information about the possible differences was asked next, in Question 11, and the examples of the most common given answers are presented in Table 13. Out of the total 50 answerers, 26 felt that there is a difference. In many answers it was stated that it is easier to share information on the Internet and also easier to find information about other people from the internet. Thus, it is easier to keep your privacy in the real world. However, one interesting point was noticed; many of the answerers feel that the Internet is part of the real world, "just another different platform of social network only". This is natural for the younger people, since they have never known a world without the Internet or mobile phones. Thus, the privacy that you have on the Internet is the privacy that you have in the real world.

Question 12 asked how much do the answerers think a person can currently affect his/her own individual privacy on the Internet; scale = 1 - 5, where 1 = A person can completely control his/her own individual privacy and 5 = A person has no control over his/her own individual privacy. These answers are presented in Table 14. None of the answerers felt that a person can completely control his/her own individual privacy. In addition, 5 of the 50 answerers felt that a person currently has no control over his/her individual privacy on the Internet. The average value of all the answers was 3.3. The same question was part of a study done in Finland, where the average value of all the answers among 22 people (11 Finnish people working with different aspects of IOT development and 11 ordinary Finnish people) was 2.6 [20]. In a yet another study, where 22 people working with different aspects of IOT development were interviewed in Finland and in China with the same question, it was found out that the answerers from Finland were less worried about the individual privacy on the Internet than the answerers from China [11]. Unfortunately, the same kind of comparison cannot be done in this study, as there are significantly different amounts of answerers from different countries.

## 4. Conclusion

In this study, thoughts about sharing personal information on online social networks were collected by interviews. The interviewees were mostly from mainland China, Hong Kong, and Finland. Most of the answerers use social media every day and share versatile personal information on the Internet. However, only a few answerers use social media for making new friends. Instead, they use social media because also their existing friends are using. Other findings of this study include that about half of the answerers also share information about other people through the Internet. Some of them do not feel the need to ask for permission before sharing, but most of them feel that courtesy and respect of privacy require them to ask for permission. It was also found out that female answerers were more active than male answerers in sharing information about other people. In addition,

**Table 11. Answers to Question 9; Do you think there should be an age limit for people to share their information through the Internet? If yes, what is the appropriate age?**

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| <10 | 5 | 3 | 1 | 3 | 1 |
| 10 - 13 | 4 | 2 | 2 | 2 | 2 |
| 14 - 17 | 8 | 4 | 4 | 5 | 3 |
| 18 - 21 | 11 | 5 | 6 | 7 | 4 |
| >21 | 0 | 0 | 0 | 0 | 0 |
| No | 22 | 17 | 5 | 21 | 1 |

**Table 12. Answers to Question 10; Do you think there are differences between privacy on the Internet and privacy in the real world?**

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| Yes | 26 | 15 | 11 | 19 | 7 |
| No | 22 | 14 | 8 | 17 | 5 |

**Table 13.** **Answers to Question 11; If yes, what are the differences?/If no, why?**

YES

- "People are more willing to share due to the anonymity on the Internet."
- "We are more alert about our privacy in real world than on the Internet."
- "In real world, we will give our personal information to someone mainly through applying something such as jobs or a school etc. Nowadays, Hong Kong already has a law that the company or firm cannot use people individual information without that people's permission. In internet, we will give our personal information to someone mainly through our own sharing such a sharing in Facebook r twitter. But in internet, there is nearly no way stopping others to use or watch your individual information as there is no law to restrict people. Moreover the technology of stealing other people information is easy through internet. So in internet, we cannot really control our privacy indeed."
- "In the real world there is no easy access to people's information unless it is disclosed to you by the person themselves or others. On the Internet other people can easily search others up."
- "We can use incorrect information without monitoring on the Internet."
- "In reality, privacy is easier to protect."
- "Cause they are in different platform."
- "Information privacy is the same thing in both world but the right is more difficult to protect in cyber world."
- "There is easier access to information through Internet."
- "People have no idea what they do on the Internet."

NO

- "People should get same privacy no matter where they are."
- "Internet also is in the real world, it seem so different but just another different platform of social network only."
- "The content of information is more or less the same."
- "All are about my privacy no matter it is on the Internet or real world.
  I think we should not divide into two categories because they all deserve our attention to protect it."
- "Both ways involve the chance of disclosing others info so they're more or less the same. So if there's any very personal and confidential info about others, we should respect others and ask for permission before disclosing it."
- "Internet is a part of real world."
- "Your information should always be limited to people you want to share it with, no matter where it is."

**Table 14.** **Answers to Question 12; How much do you think a person can currently affect his/her own individual privacy on the Internet? Scale = 1 - 5.**

| | All N = 50 | Male N = 31 | Female N = 19 | Asian N = 38 | European N = 12 |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 |
| 2 | 5 | 3 | 2 | 3 | 2 |
| 3 | 26 | 19 | 7 | 19 | 7 |
| 4 | 13 | 6 | 7 | 12 | 1 |
| 5 | 5 | 3 | 2 | 4 | 1 |

there was a significant variety in opinions if there should be an age limit for sharing personal information online; almost half of the answerers felt that there is no need for an age limit, whereas many felt that the age limit should be over 18 years. One thing that was discovered is that many of the answerers felt that the Internet is a part of the real world. Thus, the privacy that you have on the Internet is the privacy that you have in the real world.

## Acknowledgements

The authors would like to thank the City University of Hong Kong Overseas Internship Scheme 2013. Johanna Virkki would like to thank the Helsingin Sanomat Foundation.

## REFERENCES

[1] T. Smith, "Power to the People, Wave.3," 2008. http://www.universalmccann.com/Asets/wave-3-20080403093750.pdf

[2] A. Malhotra, L. Totti, W. Meira, P. Kumaraguru and V. Almeida, "Studying User Footprints in Different Online Social Networks," *Proceedings Advances in Social Networks Analysis and Mining*, Istanbul, 26-29 August 2012, pp. 1065-1070.

[3] ENISA, European Network and Information Security Agency, "Security Issues and Recommendations for Online Social Networks" 2007. http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks

[4] P. Campisi, E. Maiorana and A. Neri, "Privacy Protection in Social Media Networks a Dream That Can Come True?" *Proceedings Digital Signal Processing*, Marco Island, 4-7 January 2009, pp. 1-5.

[5] K.W Miller and J. Voas, "Who Owns What? The Social Media Quagmire," *IT Professional*, Vol. 14, No. 6, 2012, pp. 4-5. http://dx.doi.org/10.1109/MITP.2012.116

[6] N. Baracaldo, C. Lopez, M. Anwar and M. Lewis, "Simulating the Effect of Privacy Concerns in Online Social Networks," *Proceedings IEEE International Conference on Information Reuse and Integration*, Las Vegas, 3-5 August 2011, pp. 519-524.

[7] L. Determann, "Social Media Privacy: A Dozen Myths and Facts," *Stanford Technology Law Review*, 2012. http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf

[8] B. Krishnamurthy, "Privacy and Online Social Networks: Can Colorless Green Ideas Sleep Furiously?" *IEEE Security & Privacy*, Vol. 11, No. 3, 2013, pp. 14-20. http://dx.doi.org/10.1109/MSP.2013.66

[9] D. J. Solove, "I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review*, Vol. 44, 2007, GWU Law School Public Law Research Paper No. 289.

[10] Y. Wang, G. Norcie and L. F. Cranor, "Who Is Concerned about What? A Study of American, Chinese and Indian Users Privacy Concerns on Social Network Sites," *Proceedings International Conference on Trust & Trustworthy Computing*, Pittsburgh, 22-24 June 2011, p. 8.

[11] J. Virkki and L. Chen, "Personal Perspectives: Individual Privacy in the IOT," *Advances in Internet of Things*, Vol. 3, No. 2, 2013, pp. 21-26. http://dx.doi.org/10.4236/ait.2013.32003

[12] L. Chen and H. K. Tsoi, "Privacy Concern and Trust in Using Social Network Sites: A Comparison between French and Chinese Users," *Proceedings Human-Computer Interaction*, Lisbon, 5-9 September 2011, pp. 234-241.

[13] C. Dwyer, S. R. Hiltz and K. Passerini, "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace," *Proceedings Americas' Conference on Information Systems*, Springfield, May 2007, p. 10.

[14] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith and M. Beaton, "Teens, Social Media, and Privacy," *Pew Internet & American Life Project*, 2013 http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx

[15] M. Madden, S. Cortesi, U. Gasser, A. Lenhart and M. Duggan, "Parents, Teens, and Online Privacy," *Pew Internet & American Life Project*, 2012 http://pewinternet.org/Reports/2012/Teens-and-Privacy.aspx

[16] K. Lewis, J. Kaufman and N. Christakis, "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," *Journal of Computer-Mediated Communication*, Vol. 14, No. 1, 2008, pp. 79-100. http://dx.doi.org/10.1111/j.1083-6101.2008.01432.x

[17] M. Madden, "Privacy Management on Social Media Sites," *Pew Internet & American Life Project*, 2012. http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx

[18] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, No. 3, 2006, GWU Law School Public Law Research Paper No. 129.

[19] A. Quan-Haase and A. L. Young, "Uses and Gratifications of Social Media: A Comparison of Facebook and Instant Messaging," *Bulletin of Science, Technology & Society*, Vol. 30, No. 5, 2010, pp. 350-361. http://dx.doi.org/10.1177/0270467610380009

[20] J. Virkki, "Finnish Perspectives for the IOT," *American Journal of Networks and Communications*, Vol. 2, No. 2, 2013, pp. 23-27. http://dx.doi.org/10.11648/j.ajnc.20130202.11

**Journal of Social Sciences (COES&RJ-JSS)**
**ISSN (E): 2305-9249 ISSN (P): 2305-9494**
**Publisher: Centre of Excellence for Scientific & Research Journalism**
**Online Publication Date: 1st April 2014**
**Online Issue: Volume 3, Number 2, April 2014**
http://www.centreofexcellence.net/J/JSS/JSS Mainpage.htm

# Perspectives for sharing photos of children online

Johanna Virkki, Chi Kin Chan

## Abstract

The goal of this study was to gather the thoughts people have about sharing photos of children online. The work was done by gathering a literature review, studying 29 Internet forum discussions (in English and Finnish), and by personal interviews of 50 people (from Asia and Europe). Eight main viewpoints for sharing photos of children online were discovered that also supported the findings of earlier studies. Also, it was found that compared to the male users, the female users are more active in sharing information about other people online and also feel freer to share the information without asking for permission.

## Keywords

Information sharing, interviews, online social networks, photos.

## Citation

Virkki, Johanna; Chan, Chi Kin; Perspectives for sharing photos of children online; (April, 2014); Journal of Social Sciences (COES&RJ-JSS), Vol. 3, No. 2, pp: 357-366.

## 1. Introduction

Today's young parents are the first generation to raise kids in the age of social media. The trend of continuously increasing number of users sharing multimedia content was highlighted in a study that measured the consumer usage, attitude, and interest in adopting social media platforms (Smith, 2008). People today have accounts (sometimes several) on versatile social media applications and new applications are constantly booming. Commonly shared personal information includes, e.g., personal identifiers, contact information, social links, and online activities. For example, posting original photos and videos online has increased significantly in the past year; half of wired users post original photos online (Duggan, 2013). Besides the information the user knowingly discloses, the use of the service itself reveals information to the service provider; e.g., IP (Internet Protocol) address, used browser, time of connection, and other visited profiles. The service provider can thus customize its services on the base of the secondary data collected. Available information can be used to create a digital footprint of the user (Malhotra et al., 2012; ENISA, 2007; Campisi et al., 2009).

While sharing (personal) information is the main purpose of online social networks, privacy is the major concern. It has been studied that some people aren't concerned about the security and privacy on social media applications, although their main reason for using such applications is to share information (Miller and Voas, 2012; Baracaldo et al., 2011). Correspondingly, most users click to accept privacy notices and consent declarations without understanding or even reading them (Determann, 2012). Nevertheless, the data collected in online social networking applications tends to stay online, with the added risk of being linked in diverse ways. Thus, one important issue related to these different social media applications is the data aggregation (joining seemingly non-sensitive separate bits of information may well reveal additional information). Similar effect can occur when data collected for one purpose is used for a different purpose without the person's approval or even knowledge (Krishnamurthy, 2013; Solove, 2007). An interesting survey on social networks' privacy leaks and the potential hazards for users are presented in (Michalopoulos et al., 2010).

Virtual life and online individual privacy are active research areas worldwide. For example, a study that investigated American, Chinese, and Indian users of social networking applications and studied their privacy attitudes and practices, found the American respondents to be the most privacy concerned, followed by the Chinese and Indians, respectively (Yang et al., 2011). In another study, where opinions on individual privacy were collected from people working with different aspects of the Internet of Things (IOT) in China and Finland, the answerers from Finland were less worried about the individual privacy in different IOT applications than the answerers from China (Virkki and Chen, 2013). In a yet another study, it was found that French and Chinese online social networking users possessed significantly different privacy belief and trust. Specifically, French users were found to be more concerned about their privacy in the Internet and they felt less comfortable in giving personal info (Chen and Tsoi, 2011). Also, in one study, individuals using Facebook and MySpace expressed similar levels of concern regarding the Internet privacy. However, Facebook users were more trusting of the site and its members, and more willing to include identifying information in their profile. On the other hand, MySpace users were more active in the development of new relationships. It was concluded that the interaction of trust and privacy concern in social networking applications was not yet understood to a sufficient degree to allow accurate modeling of behavior and activity (Dwyer et al., 2007). In a more recent study, an interesting literature review (Kuss and Griffiths, 2011), with thought-provoking references like (Wilson et al., 2010; Kirschner and Karpinski, 2010; Barker, 2009), it was indicated that extraverts seem to use social networking sites for social enhancement, whereas introverts use them for social compensation, which in both cases appears to be related to greater usage, as does low conscientiousness and high narcissism. Negative correlates of usage include the shrinkage in real life social community participation and academic achievement, each of which may be indicative of potential addiction. Thus, virtual life and online individual privacy are important and challenging research topics.

Also, an interesting research area, the virtual lives of active users of social media applications, the teenagers, has been under study. Teens share a wide range of information about themselves on social media sites but few teens have a fully public approach to social media. Instead, they take a selection of steps to restrict their profiles, and their patterns of reputation management on social media vary greatly according to their gender and network size; girls are more likely than boys to restrict access to their profiles. These are among the key findings of a recent survey that examined teenagers' privacy management on social media applications (Madden et al., 2013). In addition, according to another survey, most parents of teenagers are concerned about what their teenage children do online and how their behavior could be monitored by others. Some parents are taking steps to observe, discuss, and check up on their children's digital footprints (Madden et al., 2012). In a yet another study, it was found out that students are more likely to have a private profile in social media if their friends and roommates also have. In addition, women are more likely to have private profiles than men. Also, having a private profile is associated with a higher level of online activity (Lewis et al., 2008). A gender gap when it comes to the way male and female social media users choose to manage their profiles was also found in another study (Madden, 2012). According to findings of this study, women are much more conservative in the basic settings they choose in social media; 67 percent of female profile owners restrict access to friends only compared with 48 percent of male profile owners.

What haunts people and their privacy is typically user-generated content, i.e., information that people themselves, their friends, and other social media users upload online (Determann, 2012). It has also been stated that privacy problems are not caused by the technology alone, but primary through activities of people, businesses, and governments (Solove, 2006). According to one study, 11 percent of online social networking users have posted online content they regret (Madden, 2012). In another study, it was discovered that 8 percent have requested someone to remove information about them that was posted online, including photos or videos (Madden and Smith, 2010).

Thus, social media applications have collected a great amount of data and are today also functioning as tools for computational social science. Online social networking has made available a rich and versatile dataset covering large sections of the population (Oboler et al., 2012). This work shares some similar objects to the studies above. The goal is to gather the thoughts people have about sharing photos of children online. The work was done by gathering a literature review, by studying 29 Internet forum discussions, and by 50 personal interviews. The work presented here is organized as follows: After this literature survey, the Internet forum survey and the conducted interviews will be introduced. The third section presents and discusses the gathered results, while the last section provides the conclusions of this study.

## 2. Internet forum survey and interviews

### *2.1 Internet forum survey*

For this survey, 29 Internet discussions handling the topic of sharing photos of children online were studied; 11 discussions were in English and 18 were in Finnish. Many of the discussions took place in discussion forums that were related to parenting, but the topic was also discussed, e.g., in comments of online magazine articles and blogs. The oldest discussion was started in March 2007 and the newest in October 2013. There were all together 1857 studied messages. The survey was divided into two main topics:

1. How do the answerers feel about sharing photos of children online?
2. What are the main viewpoints presented in these discussions?

### *2.2. Interviews*

For this research, 50 people from Asia (38 people) and Europe (12 people) were interviewed. Most of the answerers were from mainland China, Hong Kong, and Finland, but there were also individual answerers from Singapore, Ireland, and Russia. People of different age and of both gender (See Table 1), were interviewed.

Some of the interviews were done as personal interviews that were conducted by an associate of the researcher, some were done by private e-mails between the researcher and the answerer, and some of the answers were collected with an Internet questionnaire. Some of the results of this interview study were published in our previous paper (Chan and Virkki, 2013) but it also includes interesting unpublished information, e.g., answers to the following two questions:

1. Do you share information about other people through the Internet?
   - Yes/No
2. Whose information do you think you can share without asking for permission?
   - Your children
   - Your other family members
   - Your boyfriend / girlfriend / spouse
   - Your friends
   - Your colleagues
   - Anyone
   - Others, who?

Table 1. Gender, age group, and nationality of the answerers in this study.

| | **Gender** | | **Age group** | | | | **Nationality** | |
|---|---|---|---|---|---|---|---|---|
| All | M | F | < 20 | 20-30 | 30-40 | 50-60 | Asian | European |
| 50 | 31 | 19 | 3 | 40 | 6 | 1 | 38 | 12 |

## 3. Results and discussion

### *3.1 Internet forum survey results*

The first studied topic, how do people feel about sharing photos of children online, showed clearly three main opinion groups: those who say they share photos of their children online; those who say they share photos of their children online, but mention this to be only to limited people; and those who say they do not share photos of their children online. All messages (out of the 1857 studied messages) that clearly stated an opinion were selected and these opinions can be seen in Table 2. As can be seen, 61 percent of the answerers share photos of their children online. However, 34 percent of the answerers share only to limited people. Thus, they seem to trust the privacy settings of the online applications. It should be noted that also some of the answerers who stated that they share photos online (27 percent of the answerers) may have limited the access to friends only; they just did not mention it.

Table 2. How people feel about sharing photos of children online.

| Percent | Opinion |
|---|---|
| 27 % | Share photos of children online |
| 34 % | Share photos of children online, but only to limited people |
| 39 % | Do not share photos of children online |

The polarized public debate about whether or not privacy can be dismissed as a leftover in the information age was previously introduced in an interesting study (Madden, 2012). Basically, some people think that if people are willing to share versatile personal information about their lives on social networking applications, they must have abandoned any realistic expectation of privacy. Some researchers have suggested that online social network users are uniquely unconcerned about privacy; continuous use of social media without any major negative experiences may lessen their concerns about sharing information. However, some people say that the users still care about their privacy online but those sensitivities have been influenced by technology companies that can profit from availability of personal information. Also, users may be more open with what they share because they don't completely understand how their data is stored and used. Just because people want to post some information publicly online does not mean they quietly gave up all control over the information they want to share (Madden, 2012). This ongoing debate is supported by the findings of our Internet forum survey; in these 29 studied Internet discussions, eight main viewpoints for sharing photos of children online were discovered, and they are listed next.

1. It is OK if only photos where the child cannot be identified are shared.
   - Shared photos are taken so that the face cannot be identified or the child is so young that identification is not possible.
   - No full name of the child is given online with the photo.

2. It is OK if no photos that can be harmful to the child are shared.
   - No bath photos or beach photos are shared.

3. It is OK if the photos are only available to a limited amount of people.
   - Photos can be shared if they are only shared to a certain group of people.
   - "As long as you click that only friends can see your photos, you're safe."

4. It is not safe even if the photos are only available to a limited amount of people.
   - This kind of privacy is not real and although shared only with limited access to them, these photos will not necessary stay private because other people can share them forward.
   - Some social media applications, for example Facebook, own the uploaded photos.
   - The privacy settings and rules in social media applications can change.

5. It is not an issue.
   - If someone sees photos of a child, it will cause no damage to the child.
   - Children are outside all the time (parks, shops, beaches) and anyone can see them, sharing a photo online is nothing different.
   - "I still don't see the problem with someone knowing what you or your kids look like."

6. It is an issue.
   - It is parents´ responsibility to protect the privacy of their children.
   - Everybody, also minors, should be able to decide themselves if they want their photos to be shared online.

7. Other people sharing photos online can be an issue
    - Other relatives of the children can share photos; parents should be able to decide the rules to this, but some people do not listen to the parents.

8. It is part of the modern world
    - Today's young parents are first generation to raise kids in age of social media. In the internet age, privacy is just less important to people.
    - "The world is changing, get used to it!"

### *3.2 Interview results*

According to results from the interviews, half of the answerers (26 answerers out of the total 50) share information about other people online. What is notable is that 14 out of the 19 female answerers (74 percent) say that they share information about other people, compared to 12 out of the 31 male answerers (39 percent). These results can be seen in Table 3.

As can be seen from Table 4, there is also a difference among female and male answerers in question "Whose information do you think you can share without asking for permission?" Out of the all answerers, 42 percent feel that they cannot share information about other people without permission and the percentages for male and female answerers are 48 percentages and 32, respectively. Actually, the percentage of female answerers to share information of certain people group without permission is bigger than that of male answerers for every people group. These are interesting findings, as in earlier studies, e.g., (Lewis et al., 2008) and (Madden, 2012) it has been found that compared to male users, female social media users are more concerned about the privacy of, at least, their own profile. According to our results, 36 percent of the answerers feel that they can share information about their friends online, without asking for permission. However, only 14 percent of the answerers feel that they can share information about their children online, without asking for permission. There is again a notable difference among male and female answerer percentages (10 percent and 21 percent, respectively, think they can share information about children without permission). This clear difference between genders definitely is a topic for our further research.

The result of only 14 percent of the answerers feeling they can share information about their children online without permission is not in line with the results achieved in the Internet forum survey, where 27 percent of the answerers share photos of their children online and 34 percent of the answerers share photos of their children online, but only to limited people. One reason may be that many people share photos of children who are too young to be able to give permission and thus no permission is asked. Also, many people probably think they actually are the ones to give the permission for sharing photos their children, as one writer in an Internet discussion stated: "Parents can decide as they are responsible for other decisions too".

Table 3. Answers to "Do you share information about other people through the Internet?"

| | **All**<br>**N=50** | **Male**<br>**N=31** | **Female**<br>**N=19** |
|---|---|---|---|
| Yes | 26 | 12 | 14 |
| No | 24 | 19 | 5 |

Table 4. Answers to "Whose information do you think you can share without asking for permission?"

| | All | Male | Female |
|---|---|---|---|
| | N=50 | N=31 | N=19 |
| Your children | 14 % | 10 % | 21 % |
| Your other family members | 20 % | 16 % | 26 % |
| Your boyfriend / girlfriend / spouse | 20 % | 19 % | 21 % |
| Your friends | 36 % | 32 % | 42 % |
| Your colleagues | 14 % | 10 % | 21 % |
| Anyone | 0 % | 0 % | 0 % |
| Other | 0 % | 0 % | 0 % |
| None of these | 42 % | 48 % | 32 % |

## 4. Conclusions

Online information sharing has become a mainstream activity. Consequently, the public debate about privacy has been spreading. This study started with a literature survey in order to give an understanding on the magnitude of the topic. The thoughts people have about sharing photos of children online were gathered from different countries by Internet forum survey and personal interviews. It was discovered that while some parents think it is OK to share photos of children, some think it is OK if they can only be accessed by selected people (34 percent of the messages in this study), while others (39 percent of the messages in this study) feel it is not OK, no matter what the circumstances are. In the Internet forums, eight main viewpoints for sharing photos of children online were discovered that also supported the findings of earlier studies. Furthermore, in the personal interviews, it was found that compared to the male answerers, the female answerers are more active in sharing information about other people online, and also feel freer to share the information without asking for permission.

## Acknowledgments

The authors would like to thank the Helsingin Sanomat Foundation.

## References

Baracaldo, N. Lopez, C., Anwar, M. and Lewis, M. (2011) "Simulating the Effect of Privacy Concerns in Online Social Networks" Proceedings of IEEE International Conference on Information Reuse and Integration, pp. 519-524.

Barker, V. (2009) "Older Adolescents' Motivations for Social Network Site Use: The Influence of Gender, Group Identity, and Collective Self-esteem" Cyberpsychology Behavior and Social Networking, volume 12, number 2, pp. 209-213.

Campisi, P., Maiorana, E., and Neri, A. (2009) "Privacy Protection in Social Media Networks a Dream That Can Come True?" Proceedings of International Conference on Digital Signal Processing, 5p

Chan C.K. and Virkki, J. (2014) "Perspectives for Sharing Personal Information on Online Social Networks" Social Networking, volume 3, number 1, pp. 41-49.

Chen, L. and Tsoi, H.K. (2011) “Privacy Concern and Trust in Using Social Network Sites: A Comparison between French and Chinese Users” Proceedings of International Conference on Human-Computer Interaction, pp. 234-241.

Determann, L. (2012) “Social Media Privacy: A Dozen Myths and Facts” Stanford Technology Law Review, at http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf , accessed 1 January 2014.

Duggan, M. (2013) “Photo and Video Sharing Grow Online” Pew Internet & American Life Project, at http://www.pewinternet.org/Reports/2013/Photos-and-videos.aspx , accessed 8 December 2013

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007) “Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace” Proceedings of Americas' Conference on Information Systems, 10p.

ENISA, European Network and Information Security Agency, 2007. "Security Issues and Recommendations for Online Social Networks" at http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks , accessed 8 February 2014.

Kirschner P.A. and Karpinski, A.C. (2010) “Facebook and Academic Performance” Computers in Human Behavior, volume 26, pp. 1237-1245.

Krishnamurthy, B. (2013) "Privacy and Online Social Networks: Can Colorless Green Ideas Sleep Furiously?" IEEE Security & Privacy, volume 11, number 3, pp.14-20.

Kuss D.J. and Griffiths, M.D. (2011) “Online Social Networking and Addiction—A Review of the Psychological Literature” International Journal of Environmental Research and Public Health, volume 8, number 9, pp. 3528-3552.

Lewis, K., Kaufman, J., and Christakis, N. (2008) “The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network” Journal of Computer-Mediated Communication, volume 14, number 1, pp. 79-100.

M. Madden, et al. (2013) “Teens, Social Media, and Privacy,” Pew Internet & American Life Project, at http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx , accessed 10 November 2013.

M. Madden, et al. (2012) “Parents, Teens, and Online Privacy,” Pew Internet & American Life Project, at http://pewinternet.org/Reports/2012/Teens-and-Privacy.aspx , accessed 13 October 2013.

Madden M. and Smith, A. (2010) “Reputation Management and Social Media”, Pew Internet & American Life Project, at http://pewinternet.org/Reports/2010/Reputation-Management.aspx , accessed 7 January 2014.

Madden, M. (2012) “Privacy Management on Social Media Sites,” Pew Internet & American Life Project, at http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx , accessed 5 October 2013.

A. Malhotra, et al. (2012) "Studying User Footprints in Different Online Social Networks" Proceedings of International Conference on Advances in Social Networks Analysis and Mining, pp. 1065-1070.

Michalopoulos D. and Mavridis, I. (2010) "Surveying Privacy Leaks through Online Social Network" Proceedings of Panhellenic Conference on Informatics, pp.184-187.

Miller K.W. and Voas, J. (2012) "Who Owns What? The Social Media Quagmire" IT Professional, volume 14, number 6, pp. 4-5.

Oboler, A., Welsh, K., and Cruz, L. (2012) "The Danger of Big Data: Social Media as Computational Social Science" First Monday, volume 17, number 7- 2.

Smith, T. (2008) "Power to the People, Wave.3," at http://www.universalmccann.com/Assets/wave-3-20080403093750.pdf , accessed 5 Novermber 2013.

Solove, D.J.  (2006) "A Taxonomy of Privacy" University of Pennsylvania Law Review, volume 154, number 3, GWU Law School Public Law Research Paper No. 129.

Solove, D.J. (2007) "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" San Diego Law Review, volume 44, GWU Law School Public Law Research Paper No. 289.

Virkki J. and Chen, L. (2013) "Personal Perspectives: Individual Privacy in the IOT," Advances in Internet of Things, volume 3, number 2, pp. 21-26.

Wang, Y.,  Norcie, G., and Cranor, L.F. (2011) "Who Is Concerned about What? A Study of American, Chinese and Indian Users Privacy Concerns on Social Network Sites" Proceedings of International Conference on Trust & Trustworthy Computing, 8p.

Wilson, K., Fornasier, S., and White, K.M. (2010) "Psychological Predictors of Young Adults' Use of Social Networking Sites" Cyberpsychology Behavior and Social Networking, volume 13, number 2, pp. 173-177.