Advances in Internet of Things, 2013, 3, 21-26
http://dx.doi.org/10.4236/ait.2013.32003 Published Online April 2013 (http://www.scirp.org/journal/ait)

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:

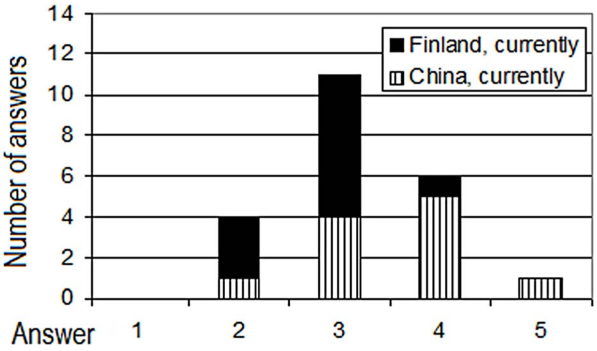

Figure 1. Results from Question 1. Opinions on how much people can currently affect their individual privacy in the Internet.

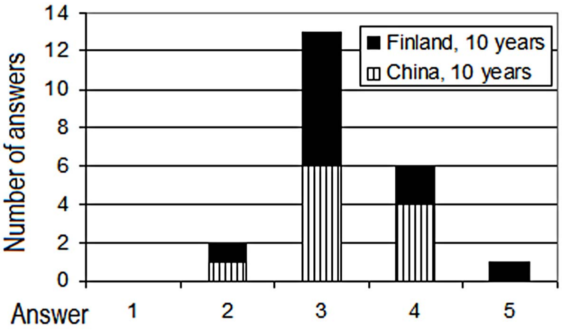

Figure 2. Results from Question 5. Opinions on how much people can affect their individual privacy in the Internet after 10 years.

"*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

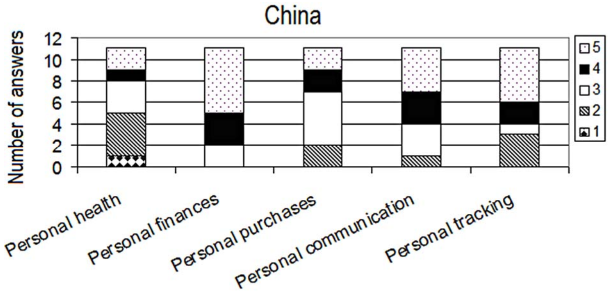

Figure 3. Results from Question 2. Opinions on individual privacy in different Internet/IOT applications in China.

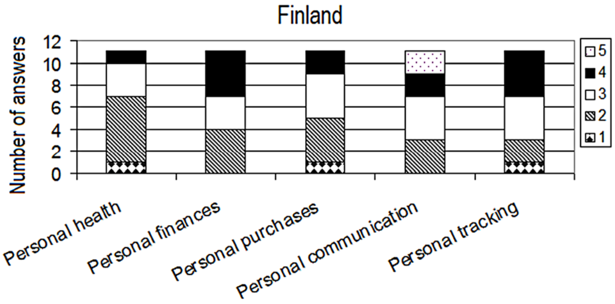

Figure 4. Results from Question 2. Opinions on individual privacy in different Internet/IOT applications in Finland.

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**.

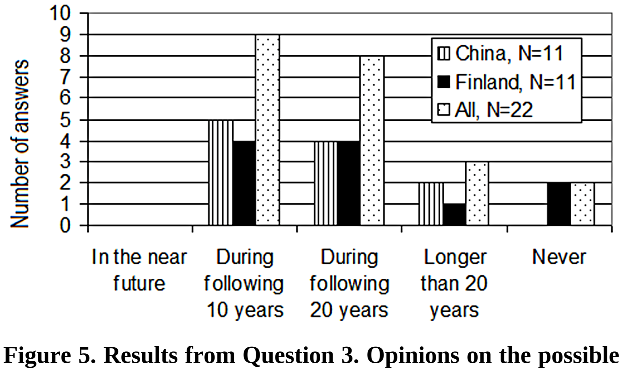

Figure 5. Results from Question 3. Opinions on the possible schedule for the current Internet to grow into IOT and this kind of all-around network to come to use.

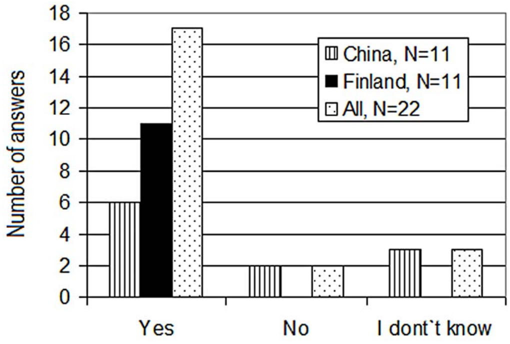

Figure 6. Results from Question 4. Opinions on if the use of at least some IOT applications will be mandatory in the future.

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.