Control vs Convenience: Critical Factors of Smart Homes

Carmen Flores Montano
IT University of Göteborg, Chalmers
Forskningsgången 6
417 56 Göteborg, Sweden
carmenfloresm@gmail.com

Mattias Lundmark
IT University of Göteborg, Chalmers
Forskningsgången 6
417 56 Göteborg, Sweden
lundmarm@ituniv.se

Wolfgang Mähr
IT University of Göteborg, Chalmers
Forskningsgången 6
417 56 Göteborg, Sweden
wm@njyo.net

ABSTRACT
In this paper we investigate four aspects that govern user attitudes about Smart Homes: *Control*, *Privacy*, *Security* and *Convenience*. Smart Homes increase the level of convenience or security but do not come without drawbacks. Since Smart Homes are used in an integral part of people's lives we expect fear and distrust towards too much automation in this area. We expect these feelings to be related to the interconnection of these four aspects in a way that causes the increase of one factor to result in the decrease of another.

We conducted twelve interviews, based on scenarios. Each scenario combines two or more of these four dimensions in order to estimate the future users' fears and concerns.

The result of the study is that everyday users want support for the boring housework, but are afraid to use complex systems. We found interdependency between the four aspects, making it hard for Smart Homes to be deployed on a larger scale anytime soon. Finding ways to create balanced systems that provide high security and convenience with only a moderate loss of privacy and control might result in better and wider spread Smart Home systems.

Author Keywords
Home, Smart Home, ubiquitous computing, convergence, domestic technologies, automation

ACM Classification Keywords
H.1.2 User/Machine Systems - Human Factors

1. INTRODUCTION
The advancing technologies affect every part of our life and environment and bring with each evolutionary step new benefits and drawbacks like help, fear and dependency.

Ubiquitous computing (UbiComp), as defined by Mark Weiser in 1988 [1], is the next big step in enhancing our lives by the use of computing power. Its goal, to make computing power omnipresent by integrating it into every object, should lead to an improved and more comfortable environment. One major marketing target for UbiComp is the field of consumer electronics, which includes Smart Homes. Smart Homes are computationally enhanced houses with the capability to act autonomously and to learn how to support their inhabitants in more ways than just providing shelter from wind, weather and other adversaries of the world.

The intention of this paper was to look into the unbiased feelings that everyday people have towards omnipresent computing in a very private situation: domestic life. There have been earlier studies with workshops informing persons about the domain that might appeal more to logic; this study's target was to appeal to gut feeling and emotional decisions. We feel that these are critical factors for the design of Smart Homes and therefore should not be neglected.

This paper starts with a compilation of related work followed by essential concept definitions for the comprehension of this paper. After this, the hypothesis is presented. Thereafter the approach of the study is explained, followed by a description of the results. Finally, these results are discussed and a future outlook is given.

2. RELATED WORK
2.1 Defining consumer needs
Green et al. [2] conducted an extensive study of user attitudes about requirements regarding Smart Home technology. By having 55 participants take part in eight two-hour workshops before the actual study, they assured that the subjects had similar knowledge and experience regarding Smart Homes. This seems like a good technique, but we felt that the workshops might color the subjects opinions, depending on the content and example applications that were presented. In our study, we tried a different approach - using scenarios with strictly defined conditions to give the subjects a common ground to base their decisions upon.

2.2 Grouping requirements into modular concepts
Another study conducted by The Internet Home Alliance [3] evaluated a number of home automation concepts through a group discussion with 48 consumers. These concepts where divided later on into different concept groups.

The most important one was called *Safety and Security Management* and focused on detection and reaction on potential problems such as keeping the family safe and protecting their home. We wanted to investigate these issues further, especially since preventing emergencies through a vast network of sensors can help save money. This provides peace of mind to the inhabitants of Smart Homes, when not at home. Taking the safety and security issue into consideration we wrote different scenarios where the homeowners got contacted by the Smart Home system.

Another very appealing concept group was the *Environmental control* with the task to adapt the indoor and outdoor environments after the homeowner's desires. This was perceived by some participants as luxurious, but not necessary, which also made this issue interesting to investigate further.

The *Energy monitor* concept mentioned in the Internet Home Alliance study was not taken into consideration since financial issues were not covered by this study, as our focus did not have an economical point of view.

The result of the Internet Home Alliance study was three basic consumer desires: *Convenience*. The system should bring together

disparate services into a single interface, allowing easy access and control from in- and outside. *Peace of mind*. The system should monitor safety and security (i.e. smoke detectors, water leaks, intruders, etc.) and therefore alleviates the inhabitants' worries. *Efficiency* allows homeowners to save time by unifying and automating tasks and to save money by reducing energy usage.

2.3 Challenges for designing Smart Homes

Edwards and Grinter [4] carried out a study resulting in a list of seven challenges that need to be overcome before realization of the Smart Home concept makes sense. These seven challenges ended in one chief challenge for designers and potential inhabitants: Balancing the desire for innovative technological capabilities with the desire for a domestic lifestyle. This lifestyle should be *easy*, *calming* and *technologically predictable***,** according to Edwards and Grinter.

The results from the Internet Home Alliance match the results by Edwards and Grinter pretty well so that we can regard their conclusions as equivalent and use them as starting points for our scenarios.

3. DEFINITIONS

To be able to measure and discuss the impact of Smart Homes on their inhabitants, a metering domain and terminology was defined. We used four dimensions for classifying Smart Homes:

Control. The extent a person can manipulate one's environment and the possibility to rely on it to behave in an expected way. This can be compared with root access on computer systems: the owner should be able to override the system.

Privacy. The extent a person can be confident that private information is not disclosed. This implies the inhabitants' private data is being protected of illegal access from inside and outside the system.

Convenience. The measure of time and effort saved by the use of the system. An increase of convenience could for example come from the system automatically switching on and off lights upon room entry and exit.

Security. The extent an inhabitant is free of physical danger and therefore enjoys peace of mind. In this work we focus only on physical security since computer security issues are covered sufficiently by the privacy dimension.

4. HYPOTHESIS

After the dimensions have been defined, we can have a closer look on their relation. The reason that Smart Homes are purchased and therefore developed is the prospect of gained convenience and security. At the same time privacy and control over the Smart Home system is intended to continue at the current high level or even to increase. Since these dimensions are interrelated (Fig. 1), an emphasis of one dimension usually goes on the cost of another dimension. One rather obvious connection is between control and convenience: More convenience can easily be reached by letting loose of control. At the same time an increase of convenience can be achieved by easing privacy, and results in less security. Our hypothesis (see Fig. 1) is that higher security goes on the cost of on of the other three dimensions. Higher convenience requires less control or less privacy. To achieve better control, privacy has to be slashed. These connections work also in the other direction.

5. METHOD

5.1 Participants

Smart Home design is a rapidly growing and increasingly lucrative field with multiple, diverse stakeholders [5]. Since the primary goal of this study was to indicate the existence of undesirable functionality in everyday use of Smart Home systems, we focused solely on people who will live in such homes. Our twelve survey subjects were chosen from this group - as possible future users of Smart Home technology.

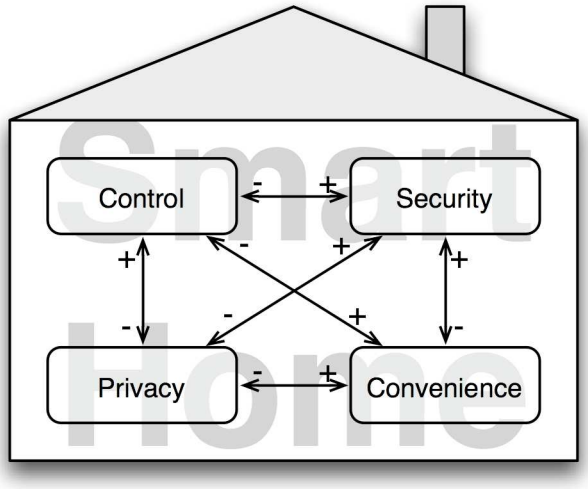

Figure 1. Relation of the four dimensions used to classify Smart Homes

5.2 Survey construction

The interviews consisted of two different parts – five open-ended questions and nine scenarios. We chose this mix to get lengthy answers as well as briefer, quantitative answers [6].

After answering the general questions about Smart Homes, the subjects were introduced to nine scenarios with multiple answer possibilities. The setting for all the scenarios consisted of a family including the test subject, his or her partner and their two children, age 5 and 8, living in a future Smart Home. The subjects were explicitly instructed to ignore financial matters and assume that all the functionality were free.

To construct the scenarios a brainstorming was used to search for possible functionality. The results were then combined with existing and proposed functionality from other sources [7, 8]. The resulting lists of functionality was incorporated into nine scenarios, each describing a setting, scene or situation were the subject was asked to make a choice about the design of the subject's Smart Home. Each scenario combined two or more of the four dimensions mentioned earlier in order to estimate the future users' fears and concerns.

6. RESULTS

This is a short summary of the survey results. The complete results and discussion can be found in the full paper [10]. The answers of the scenarios can be seen in Figure 2, the summary of the open questions is that many people expressed fears of becoming dependant and helpless, in case that something malfunctioned or was destroyed.

The first scenario (S1, "Babysitter") asked if the subject would feel comfortable leaving the children in the custody of a Smart Home for an evening. The answer possibilities ranged from high convenience and low control (leaving children) to high control and low convenience (not leaving children). People were not keen on leaving the children alone as they said that the children could be unpredictable and that the impersonal system might not be able to handle such situations as good as a real baby-sitter.

The next scenario (S2, "Burglary") described an ongoing burglary, which would take place while the family was on vacation. The subjects were asked how they wanted a system reacting from enforcing high security and low control (electroshock) to using low security and high control (do

nothing).

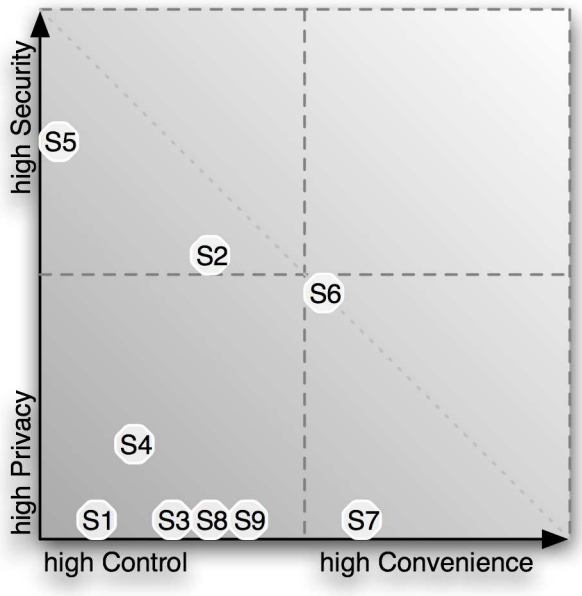

Figure 2. The results of the subjects' answers to the scenarios

Most subjects felt uncomfortable with the idea of the smart home automatically applying defence mechanisms like electroshocks, and preferred to notify the police and delegate the responsibility.Most subjects felt uncomfortable with the idea of the Smart Home automatically applying defence mechanisms like electroshocks, and preferred to notify the police and delegate the responsibility.

Scenario three (S3, "Automatic Grocery Shopping") presented the idea of automatic shopping support, that would relieve users from daily grocery shopping. The answer possibilities ranged from high convenience and low control (users choose overall food-quality, system makes menu) to low convenience and high control (not use at all). The majority of subjects wanted to define every single good, and a few wanted to choose the menu and leave the rest to the system.

The "Intruder" scenario (S4) addressed the issue of privacy on and off the Internet. The subjects were asked which type of data an intruder needed access to make them refuse to switch the system on again after removing the security issue. The answer possibilities ranged from high privacy and low convenience (not turning on at all) to low privacy and high convenience (turn on in any case). The answers showed that half of the subjects would not switch the system on again, the others reacted sensibly to financial and surveillance data being compromised.

The fifth scenario (S5, "Surveillance") asked in which rooms the subjects did not want surveillance by video cameras. Multiple answers were possible with each additional selection resulting in lower privacy but higher security (more cameras). The most common places in which the subjects did not want surveillance were the toilet and the bedroom.

The next scenario (S6, "Restricted Access") was access rights to the system control and other parts of the system. The subjects could choose functions they wanted the access to be restricted, more restrictions of dangerous appliances resulted in higher security but lower convenience. Most subjects wanted restrictions on installation of new software and use of kitchen tools, some chose to restrict access to door locks, heating and outgoing calls.

The "Christmas Chores" scenario (S7) proposed that typical preparatory tasks would be done by the system to support the subjects. Each additional support resulted in higher convenience but lower control. A majority of the subjects did not want any help with the selection of Christmas gifts but did not mind receiving help with controlling the ambient lighting, selecting the music, adapting the heating or purchasing the food.

The "Cleaning" scenario (S8) targeted people's tolerance with irreversal rearrangement tasks of the autonomous system - here destroying a 100 SEK note when cleaning. The answer possibilities ranged from high convenience and low control (continue using) to low convenience and high control (not use any more). Two thirds of the subjects chose to not switch on the system again; the rest accepted the loss and the implied problems.

The last scenario (S9, "Filtering") tested the subjects' acceptance to censorship and filtering by having the Smart Home filter all suspicious parts from incoming media signals (like mails, news and phone calls) to protect the children from exposure. The answer possibilities ranged from high convenience and low control (use the proposed dumb filter) to low convenience and high control (no filtering). Most of the subjects did not want to use the system at all. The rest wanted an authentication system to avoid filtering of own material, nobody accepted the system as proposed.

7. DISCUSSION

7.1 Convenience

Convenience is one of the key selling points for Smart Homes. The convenience of skipping the boring everyday life chores (like pouring a bath or cleaning the floor) require a transfer of control or privacy to the system. As long as the user can override the control and no failures occur (like for example a flooded bathroom) this loss is acceptable to many. The results of the scenarios showed that the subjects were only willing to release little control to the system to gain convenience. In matters affecting children the subjects did not trust the system being flexible and self-learning enough to react appropriately - ironically this can also happen to parents. However, parents have morality that keeps them off taking insane decisions, something that a machine still has problems with.

7.2 Security

Smart Homes intend to enhance security, but with complex access systems, automated locking of doors, surveillance cameras or motion sensors this comes at the expense of privacy and control.

7.3 Privacy

The answers in our scenario S5 ("Surveillance") and a poll in 2003 by Harris Interactive show that privacy is an important part of our life. 64% of 1010 interviewed Americans have "strong feelings about privacy and are very concerned to protect themselves from the abuse or misuse of their personal information by companies or government agencies" [9]. Disclosure of private things (e.g. e-mail) does not seem to be a problem for most people since they beforehand consciously decided that they take that risk, when storing them. In the decision about storing or not we seem to be aware that the danger of unveiling exists. The thought of external storage of things without our knowledge (e.g. taping phone calls, camera surveilling toilets) is nevertheless uncomfortable.

7.4 Control

Control was the central topic of this work - of both the answers and the scenarios. Control is power and having control is freedom (from George Orwell's "1984"). Freedom in Smart Homes is to be able to execute one's ideas and to be sure that everything behaves the way it is expected. A powerful and convenient system however might bring obstacles to one's plans and the fear of such a system going berserk is big. Especially for our homes - an important and critical environment - such technology still seems too error-prone, too complex. Other critical areas like for example transportation still provide alternatives upon failure. With uncritical systems

like home entertainment and media we are more reluctant towards errors. If our video-recorder breaks, not our whole life is affected like it could be when the Smart Home rejects to open any door when we are inside and the house is on fire. Smart Homes combine the fragility of computer systems with the criticalness of basic needs like food, shelter or security.

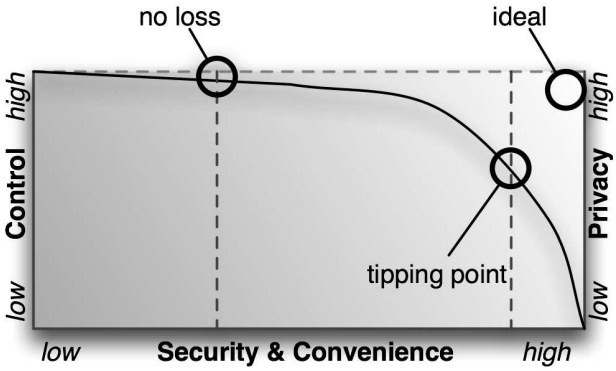

Figure 3. The correlation between increased security and convenience at the expense of control and privacy

Figure 3 shows the correlation of benefits and drawbacks between security/convenience, control and privacy. Since we believe this correlation to be non-linear, we think that it could be interesting to create different Smart Homes for different target groups.

Low-tolerance users might favor a system with gained security and convenience without loss of privacy and control. This could be achieved by creating systems that prevent dangerous situations but still are easy to override. An example could be a bath tub that automatically stops filling water before overfilling in case the user is not present; if present the user might be warned by a sound but maintains control over the filling process.

Systems targeting medium-tolerance users could bring along moderate loss of control and privacy. Such a system could - freely adapted from Parteo's Principle - provide comfort in 80% of the situations but lead to additional user effort in the other 20%. In an analogous example, the bath tub could calculate or learn the ideal water quantity and temperature and automatically fill the tub accordingly. In the rare case that the user should need the water for another purpose, the user would be required to interfere with the system.

Systems targeting medium-tolerance can have moderate loss of control and privacy as long as the security and convenience gains are disproportionally higher, which is true up to the tipping point. Moving beyond this point yields only minor increases in security and convenience for a larger amount of sacrificed control and privacy. Such a system could - freely adapted from Parteo's Principle - provide comfort functionality that fit in 80% of the cases but may lead to additional user effort in 20% of the times. As an analogous example, the bath tub could calculate or learn the ideal volume and temperature of the bathing water and automatically fill the tub accordingly. In the rare case that the user wants to pour the water for some other purpose, the user is then required to modify the result.

8. CONCLUSION

Today's Smart Homes are not ready for large scale deployment, since their time has not come yet. On one hand, technology is too vulnerable (i.e. viruses, hackers or power-downs) to guarantee the same level of reliability as a screwdriver. On the other hand, humans have to learn to let go of control when they want to gain convenience - something that mankind has done since the invention of the wheel.

Self-learning and creative computer systems may be an answer to these problems. The time needed to develop these techniques to a sufficient level can be used to resolve existing privacy and control issues. Until then the market seems to prefer small but specialized solutions, and since advancing technology influences us humans and our society the perception of this domain may change over time. When Smart Homes will be as simple to use as a computer and as reliable as a car, they will become interesting for consumers.

9. FUTURE WORK

This work recommends conducting larger studies to further research people's attitudes towards Smart Homes. Special emphasis could be put on control and people's ability to hand over this control to autonomous systems, a critical issue revealed in this study. Another interesting question is the different attitudes of diverse demographic groups such as people with children versus people without children. Further, the scenario of increased control on the expense of privacy was not included in this study. A scenario of for example spouses monitoring each other could be interesting to evaluate as well.

10. ACKNOWLEDGMENTS

We thank the participants of our study for their time and thoughts. We also thank everybody who supported us in this work in other ways but also in our everyday life.

11. REFERENCES

[1] Weiser, M. Ubiquitous Computing. http://www.ubiq.com/hypertext/weiser/UbiHome.html

[2] Green W., Gyi D., Kalawsky R., Atkins D. Capturing user requirements for an intergrated home environment. 2005.

[3] The Internet Home Alliance. Safe, Secure and Comfortable Home Research Study. http://www.internethomealliance.com/pilots_projects/family/docs/SSCHIndustrySummary.pdf

[4] Edwards W. K., Grinter R. E. At Home with Ubiquitous Computing: Seven Challenges. *Proceedings of the 3rd international conference on Ubiquitous Computing*. Springer-Verlag, London, England. 2001.

[5] Rout P. A. Digital homes – for richer for poorer, who are they for? *BT Technology Journal 20*, 2 April (2002).

[6] Schumacher, M. Creative Conversations: The Writer's Complete Guide to Conducting Interviews. Writer's Digest Books, USA, 1990.

[7] Park S. H., Won S. H., Lee J. B., Kim S. W. (2003). Smart home – digitally engineered domestic life. *Personal Ubiquitous Computing*, 189-196. Springer-Verlag, London, England.

[8] Microsoft. Windows Home Concept. White paper, 2004.

[9] Taylor, H. Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. *The Harris Poll® #17*. Harris Interactive, USA, 2003. http://www.harrisinteractive.com/harris%5Fpoll/index.asp?PID=365

[10] Flores Montano, C., Lundmark, M., Mähr, W. (2005) *Undesirable Functionality in Future Smart Homes: An Estimation of Future User's Feelings and Expectations.* Unpublished, available upon request.