A “Kinder” Surprise: Big Brother Is Watching You(r Humidity Values)

Albrecht Kurze
Faculty of Computer Science
Chair Media Informatics
Chemnitz University of Technology
09107 Chemnitz, Germany

Arne Berger
Faculty of Computer Science
Chair Media Informatics
Chemnitz University of Technology
09107 Chemnitz, Germany

Sören Totzauer
Faculty of Computer Science
Chair Media Informatics
Chemnitz University of Technology
09107 Chemnitz, Germany

firstname.lastname@
informatik.tu-chemnitz.de

Abstract

In 1984 the Ministry of Truth controls the populace with cameras and microphones to maintain its totalitarian dictatorship. The boundaries between work, home and third places have vanished. Now, 32 years from that fictional vision, we have arrived at the Internet of Things (IoT). Though Orwell has prepared us for the dangers of visual and audio data in our homes, are we fully prepared for the Smart Wireless Things deceptively promising convenience and luxury while monitoring our very behavior? Is it possible for a thermometer or a luxmeter to be as dangerous for our privacy as a camera or microphone? We present a selfmade, inconspicuous surveillance kit for teaching people about privacy and agency in their new IoT home environment. Further, we present our (basic) findings from a first fieldwork.

Author Keywords

Smart Wireless Things; Internet of Things; Making.

ACM Classification Keywords

H.5.2. [Information Interfaces and Presentation]: Prototyping, Input devices and strategies.

Introduction

The Internet of Things is arriving in the (smart) home. More and more everyday objects in the home are

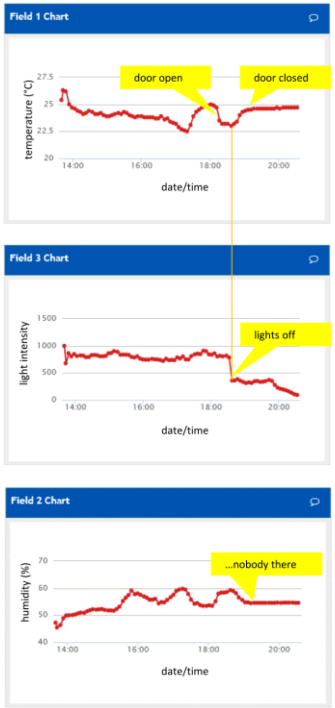

Figure 1: llustrative example of simple sensor data interpreted. We collected with some prototypes of the *Surveillance Egg* some of this data at work and at home and and see even from very simple sensors some interesting information in there.

sensor equipped and connected. This includes devices dedicated to environmental monitoring but also devices including this functionality as a side effect.

These connected devices offer new chances and new possibilities, e.g. more comfort, more security, more safety, and more efficiency. They might also introduce some new risks and threats that the users are not aware, e.g. surveillance that violates the privacy of the users, e.g. monitoring of sleep times. It might not even need a camera or a microphone to break the intimacy of a home. Even simple and at first sight totally harmless sensors, e.g. for light, temperature or humidity, may reveal a lot about the people, their presence or absence, the daily routines, maybe even about their behavior and their preferences. Understanding both sides, chances and risks, requires awareness and agency in the usage of these devices. It might be necessary to teach the users. We developed and field-tested a probe pack of seemingly harmless sensors in order to understand how people in the home use these sensors, what scenarios they develop, what agency they get, and what can be seen in the collected data - by them and by us. We involved participants to understand what they thought is in the data and what we know is in the data. This shows the people directly the power and potential harm/ramifications of this data. Additionally, we indirectly learn how to design critical smart devices that teach about the power of seemingly harmless sensors.

(Un-) Personal data (?): I know how long you slept/showered/worked yesterday

In contrast to cameras and microphones sensors like a thermometer, a luxmeter, or a hygrometer might not be seen as risks. Nevertheless, all the data of these sensors may have stories to tell: the light level in the living room, the temperature and humidity in the sleeping room, kitchen or bathroom, an accelerometer on the door of the flat or the fridge. Every single measurement might be small data with only a few bytes. However, they might gain power from big data, from time series, from the comparison, between days, weeks, other users, the correlation with other data and their meaningful interpretation. These data might reveal when somebody is at home, when they cook, shower, sleep, and watch TV etc. (figure 1).

We see the sensor equipped devices in different forms. First, integrated in already existing devices, making them smart, e.g. smart fridge. Second, in small, cheap, and ubiquitous sensor devices, even in small scale, like Smart Dust [2]. Third, in the form of augmented mundane objects. The sensors might be hidden, maybe not visible or recognizable to be there, sitting in the dark. This potential of (covert) ubiquitous surveillance and all the implications associated raise show the critical aspects in the approach. Some of these devices and their data might be owned by the inhabitants, some by the landlord, some might controlled by somebody completely different, e.g. the vendors or some data collectors. AAL-upgrade homes, already equipped with sensors, and access to the data not limited to the users of the flat but available for their owners is such a scenario. It might give the landlord the ability to check whether the tenants treat their flat well, e.g. keep the humidity in a desired range. It might be fair for a rented flat - on base of an agreement. Maybe even a low-level surveillance, some kind of supervision or even the suspicion to be monitored will result in behavior changes.

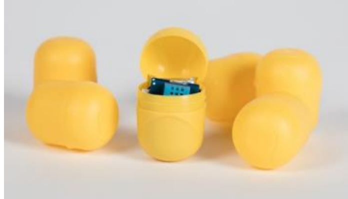

Figure 2: Surveillance Egg first iteration. A *Kinder Surprise* capsule with an IoT surprise.

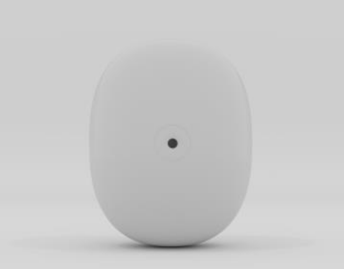

Figure 3: Surveillance Egg next iteration. The final enclosure is still in development. (CGI)

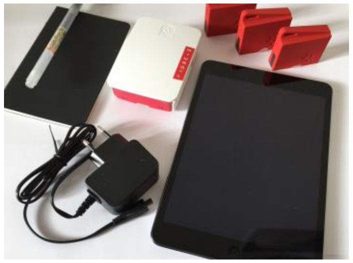

Figure 4: A probe pack with several sensors (SensorTags), a Raspberry Pi, an iPad, and a documentation booklet.

Agency of sensors in smart things

At the same time the technology is ready for a wide spread deployment in the homes, are the inhabitants also ready? We expect that naive users do not think in sensors or actuators, that they not understand what possibilities exist, how sensors work or how they might be integrated in products. Therefore, we developed tools to support our participatory design process [1]. These tools offer abstract representations of different sensors in one device and different actuators in another device, communicating wirelessly.

Based on the *Kinder Surprise* candy/toy we developed the concept of the *Surveillance Egg*. In its original form the *Kinder Surprise* is a chocolate candy for kids containing a surprise like a toy or a collectible. However, our surprise is not necessarily kinder than other seemingly harmless sensor devices. The inner plastic capsule is hiding Maker components instead of toys: a battery, an MCU with WiFi (ESP8266) and some simple sensors - ready to monitor its environment (figure 2). Choosing the inconspicuous hull of a children candy therefore resembles the principle of the new IoT paradigms at its core. For further usage in scale, we wanted even smaller devices with even more of these harmless sensors. In the TI SensorTag we found a suitable base for our further development with a compact size, energy efficient BLE, openness in hardware and software to adapt it for our purposes, and different sensors (thermometer, luxmeter, hygrometer, barometer, accelerometer, gyroscope, and magnetometer). We plan to redesign the devices, back to the initial idea, to make them more like normal household objects (figure 3).

Probe packs: sensors in the wild

We created probe packs (in the concept of cultural probe) containing all necessary components for the participants to use these simple sensors in their own flats and to document their usage (figure 4). A Raspberry Pi 3 connects to the wireless sensor devices and preprocesses the incoming data before forwarding it to our servers for data storage. Each participants gets a ready to use configured iPad to see live and historic data of the sensors in customized graphs. We planned different field phases with actual usage of the sensors. We started with students and colleagues, followed by ordinary elderly users. Do the participants have valid concepts of what to measure to gain a desired insight? What usage scenarios will they develop? What data from their private life are the participants willing to reveal? Do the participants will use the sensors, once they understood, what they might reveal? Will the participants develop some ideas how to hack sensors, e.g. with lids, hermetic enclosures or artificial light sources etc.? We will look at the data with the participants in workshops to interpret the collected data together with them, to see patterns and anomalies, and to gain insights. We expect that this looking at the data of even these simple sensors will lead to a big surprise for the participants in the end.

Point of debate / workshop contribution

What implications might harmless simple connected sensors have in the smart home – and how can we, as researchers, critically reflect on them along with the users?

We will come with some of our artifacts and are interested to demonstrate them in the AirBnB flat. Currently we field-test the devices without the final

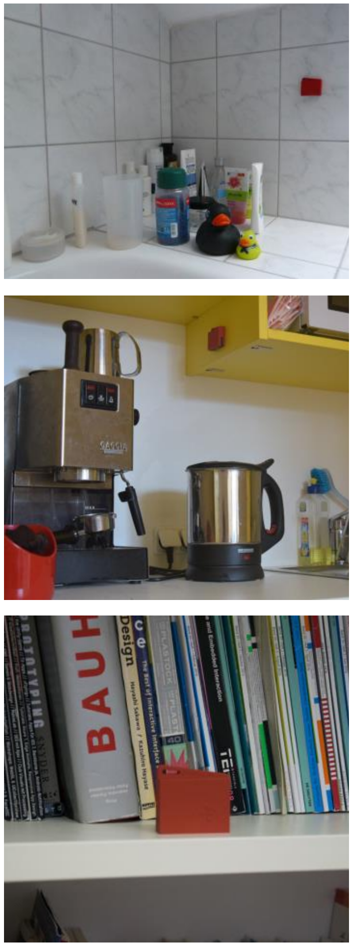

Figure 5: Sensors oft he probe pack in action - in the bathroom, in the kitchen, and in the living room

(c) Photographs by *Miteinander*.

enclosure, but we will try to bring the final form to the workshop. We are interested in feedback to our realization, the appearance, the size, the material, functionality, and want to discuss the critical maybe even subversive ramifications. We predefined some scenarios: where to install the sensors, what to measure and what to find out. Maybe the workshop participants will come up with new and maybe even crazy ideas in the flat if we let them place the sensors. We can show live data but also some previously collected data for usages where longer data collection is necessary for meaningful insights. Internet connectivity within the venue would be helpful, either wireless or wired.

About us

The contributors work in an interdisciplinary team called *Miteinander* (German for *together*) at Chemnitz University of Technology, bringing together competence in design, computer science, social sciences and engineering. We investigate participation and co-creation for smart connected technology within the realm of demographic change and community work.

About Albrecht Kurze: I am a computer scientist. My research interests are networking aspects in all flavors. In my interdisciplinary PhD thesis I quantified the relationship between QoS and QoE for mobile services with about 300 participants. At *Miteinander* I am in charge for the engineering and IoT. The interdisciplinary approach in our team shifted my focus and view once again - away from only looking on the technology - much more to the users and the implications we create with the technology. I am a tinkerer since my elementary school days and nowadays I am back at tinkering in the office.

About Arne Berger: Officially a computer scientist with a doctorate in engineering, my research takes an inter- and transdisciplinary research through design approach at the intersection of design ethnography and interaction design. I am the principal investigator of the Interaction Design Research Lab team *Miteinander*. My research focuses on early stages of design processes. I am mainly interested in how meaningful participation can be initiated, how people can be empowered and engaged to collaboratively create possible futures together. These days I am also turning towards more ethnographical design research work. I am somewhat well travelled and take local food a bit too serious.

About Sören Totzauer: I am a computer scientist with a degree in bioinformatics. My major and foremost research interest is how people can be motivated to take up agency for themselves, especially regarding the oncoming socio-technological paradigm shift.

Acknowledgement: This research is funded by the German Ministry of Education and Research (BMBF) under grant number FKZ 16SV7116.

References

1. Kevin Lefeuvre, Sören Totzauer, Andreas Bischof, Albrecht Kurze, Michael Storz, Lisa Ullmann, and Arne Berger. 2016. Loaded Dice: Exploring the Design Space of Connected Devices with Blind and Visually Impaired People. In Proc. of NordiCHI '16. ACM, New York, NY, USA. http://doi.org/10.1145/2971485.2971524
2. Joseph M. Kahn, Randy H. Katz, and Kristofer SJ Pister. 1999. Next century challenges: mobile networking for "Smart Dust." In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, 271–278.