TAGGED! About the potential effects of RFID-„smart“ Everyday Objects (THESIS)

RFID (= Radio Frequency Identification), a so-called „smart“ technology, belongs to the automatic identification techniques and currently constitutes a very fast developing market. According to many studies, the future prognostics of the branch look very optimistic. Whether or not these prognostics will prove true in the future remains to be seen. What can be noticed already, however, is the fact that RFID is not only implemented in industry, manufacturing or supply-chain-management applications, but increasingly in the everyday environment of the public. Whereas RFID is promoted as one of the most innovative and profit promising technologies in the field of business and industry, privacy activists warn the public about the dangers arising from the invasion of RFID into everyday life and call RFID-labels „Spy Chips“ or „Little Brothers“[1]. Some even fear the decline of democratic values and the liberal constitutional state.[2] This situation led to the following questions: What actually is RFID? How does it work technically? Which applications are already implemented today? Which applications are planned for the future or will be possible? What could be chances, but also possible risks emerging from RFID? Who has influence on the ongoing development process of RFID and who will be accountable for negative outcomes?

The work is structured in two main parts. The first part deals with the definition of „smart“, an analysis of today’s promoted „smart“ objects and the scientific theory of „Ubiquitous Computing“ (= UC) as the main theory of „smart“ environments. The second part deals with RFID as a „smart“ technology, its technical background, today’s applications of RFID, possible effects on everyday life arising from potential future applications and today’s controversial discussions of different stakeholders about the issue.

The following paragraph roughly outlines the results of the analysis. „Smart“ used as a term for describing certain characteristics of things, people or actions reveals to be very dependent on its context and is often played with because of its different meanings especially for commercial or marketing purposes. Therefore its meaning is very blurred and often not clear. Surprisingly even for the technological term „smart“ various definitions can be found. This leads to the conclusion that today „smart“ cannot and should not be used as a means of accurate definition. Therefore throughout the work „smart“ is set into quotation marks to indicate the relativity of the term or it is complemented with the addition „RFID“ in order to emphasize the special characteristics of this technology.

UC deals with „smart environments“ meaning the theory of enhancing the everyday environment with computer technology. The goal is to make information accessible from anywhere and to construct a network of things via the internet. In 1991 Mark Weiser, the „father“ of UC, expected the transition

1 CASPIAN: „How ‚spychips’ pose a threat to your privacy.“, http://www.spychips.com/, (accuracy: 16.3.2005); Andersja 18.6.2004: "Maybe it'll be Little Brother watching you", http://www.rfidbuzz.com/news/2004/maybe_itll_be_little_brother_watching_you.html, (accuracy: 1.7.2005)

2 Brust, Friedhelm 28.12.2004: RFID und die Arbeitswelt. http://www.rifid.de/neu/analysen/arbeitswelt.html, [Stand: 16.3.2005]

from the internet era to the UC era to take place between 2005 and 2020.[3] From this point of view it is extremely interesting to take a look at one of the key technologies of UC now.

When looking at potential effects of RFID it becomes clear that the assessment of the technology is strongly tied to the kind of application it is used for. While having tremendous positive effects like even life saving functions in some medical applications, the decline of costs and optimization of processes in many economic applications or simply time saving qualities in the public transportation system, at the same time RFID constitutes a possible danger for data privacy and civil liberties. After having evaluated the current situation, I see a danger in the reckless attitude of some operators of RFID-systems toward personal data, but also in the state's attitude based on recent government regulations and statements of the German Minister of the Interior showing a tendency of ignoring data privacy more and more in favor of stricter security laws. But on the other hand I also blame the people as well, because in recent decades a familiarization with state surveillance practices, as one focus of the work, has been noticed and a wide spread lack of critical reflection of this process as well as of the introduction of new technologies in general.

But unlike many critical articles evoking a feeling of panic, the discussion should not only be seen as a risk controversy, but above all as an essential part of the democratic system relying on the constant process of balancing common welfare and the freedom of the individual, the subjective benefits and the social costs. At this point the development process is still widely open, which is one explanation why it has become such an issue over the past couple of months. Finally all social actors are equally involved in the process and are equally responsible for the development of a technology. These include the technical developers by setting the frame for certain using possibilities or excluding them, the designers of RFID-applications by deciding upon the interfaces and the type of interaction, the operators of RFID-systems by deciding upon the purpose of the system and the treatment of personal data and the affected people, the state as a regulatory instance, as well as society itself, whose acceptance or denial of a technology has a strong impact on the future development like activists have shown in the past for example.

3 Weiser, Mark und Brown, John Seely 5.10.1996: The Coming Age of Calm Technology. http://www.ubiq.com/hypertext/weiser/acmfuture2endnotes.htm, [accuracy: 24.10.2004]

Alerting in the present situation is the fact that only a very small percentage of people know about RFID, its main characteristics and application purposes. According to a study published at the beginning of 2005 only an average of 18% of Europeans have ever heard of RFID – in Germany even less - only 15%.[4] Although the main mass media like newspapers and television have not reported much about the discussion, in recent months it has shown to become an issue in some specialized press articles. But the reports are often very biased or controversial and therefore often lead to an even greater insecurity of the readers instead of providing rather objective information. However, for a public discussion as part of the democratic system it is necessary for people, first of all to know about RFID as a technology and also about the applications planned for the near future and their possible impacts. What is also greatly missing these days is the conscious practical experience of people with RFID systems, since usually they remain almost „invisible“ in the background and are only visible for their operators, but not for the people possibly affected.

For all these reasons I decided to create an art installation with the intention of raising the awareness for RFID in the public and to help clarify the current debate a little for people who do not know anything or not much about RFID, or those who have become insecure from controversial reports. The medium has to be an installation, because virtual data and physical objects are closely linked through RFID. The installation is based on an entertaining narrative approach, which should first of all invite the users to interact with it while gaining their own experiences and getting an idea of what other applications might be possible, useful or even dangerous. Another area of interest is the semantic level: „How does it feel, when everyday objects become ‘smart’?“ and: „What would it be like, if already today every item was tagged?“ While nowadays private individual applications of RFID rarely exist, the installation should also raise the awareness for the potential private use of RFID still widely lying idle.

The installation consists of a shelf in which several everyday objects are presented. At first sight it looks like an ordinary shelf, which could be part of everyone’s living room. In the middle of the shelf there is one empty cubicle and a screen display. When the user places one of the RFID-tagged objects inside this cubicle, the hidden antenna reads the ID-number and the linked data is displayed on the screen above. Each object is a symbolic trophy and tells a short story about how, where or from whom it has been stolen by means of a mixture of short movie-clips, picture sequences, sound files or song extracts. Only after having viewed some of the objects’ information it becomes clear, that all these objects have been stolen by a young lady in her mid-twenties over a certain period of time and that she has been collecting and proudly presenting them in this shelf. She does not steal because of financial problems, but in order to make her boring ordinary life more adventurous. All the objects represent souvenirs of illegal situations. By spending some time exploring the objects closely more and more parts of the protagonist’s personality and the development of her criminal career can

4 Capgemini (Hrsg.) 2005: RFID and Consumers - What European Consumers Think About Radio Frequency Identification and the Implications for Business. http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf, [accuracy: 22.2.2005], page 4

be revealed. The concept offers „quick entertainment“ by viewing only a few objects, „deeper insight“ for those who spend more time exploring the objects and „hidden features“ for the curious.

In order to contrast this personal content with commercial applications, the documentation of the stolen objects is embedded into a fictional commercial RFID Software called „HOMEiDENT“. When placing the object in the special cubicle, the fictional „manufacturer’s information” is displayed at first hinting at possible other applications before switching to the local private database. This contrast is underlined by the implemented styles. The „manufacturer’s information“ has a very clean professional look including a consistent picture style, while the „private information“ has a inconsistent amateurish and scrap book type of style.

Beyond, the theme of (mis-)using RFID for categorizing and documenting stolen things, ironically plays with the fact that traditionally RFID is used for anti-theft purposes at retail.