Extended Abstract

Ubiquitous Computing and Privacy

Henning Lübbecke

Grafenwerther Str. 5, 53604 Bad Honnef
E-Mails: henning.luebbecke@privatbaz.bund.de

Accepted:

Introduction

Ubiquitous computing is a topic in sciences for almost 3 decades and there are the very first application of ubiquitous computing in real life. People wish with ubiquitous computing to ease in work and allday routines, they hope for a rise of security and to extended their senses and memory. Every day objects would have sensors and/or RFID-tags. These sensors and RFID-tags can be read ubiquitously and personal data are inquired, computed and/or stored. Ubiquitous computing needs an infrastructure of ubiquitous surveillance.

In the future many participants, in constantly changing settings, with manifold goals in very different contexts will take part in ubiquitous computing. Systems will organize them selves, unnoticed by the ones affected, and mysterious for them.

Privacy laws of today hold for situations with few participants in their straight defined roles. They claim to establish transparency, attachments, needs, control abilities, and participation of the affected ones. But these laws are not made for situations with many participants, in a variaty of constantly changing rules, under different goals in each role. Privacy laws must accommodate to the needs of ubiquitous computing to realize a right to informational selfdetermination (9).

New Privacy Laws should address the following principles:

1. data should be fair and be computed law-abiding,
2. data should only computed on their purpose,
3. data should be appropriate, relevant and not excessive,
4. data should be precise and up-to-date,
5. data should remain as local as possible,
6. data shouldn’t be stored longer than necessary,
7. appropriate punishments must be possible (11).

To realize all this in ubiquitous computing, it is necessary to integrate privacy principles into the technology. In networks of sensors and RFID-Systems privacy is ment to the appropriate handling and transfer of the ubiquitous surveillance infrastructures they realize (9).

Surveillance has allways to faces. It is necessary and supportive for securety, crime prevention and crime detection. On the other hand surveillance changes behaviour, people fell unfree and inhibited (6,7). Because of the latter people will stay anonymous in public spaces (6, 11). Concepts like the principle of agreeing with the gethering, computing and storing of data, like we know it today, didn't function in the context of ubiquitous surveillance. "If I couldn't buy some thing to eat without surveillance, how can the acceptance be free?"(6). In future the Focus of privacy law should be more to the person than to the data. Privacy in ubiquitous computing and surveillance is more and more a problem of anonymity and untraceability. But anonymity of users and untraceability of each kind of "items of interest" would make a lot of applications of ubiquitos computing impossible. Though anonymity and untraceability are only senseless against attackers and not the legal users of surveillance. The legality of surveillance in ubiquitous computing and surveillance is to be ruled out in privacy law.

Anonymity

From the view of technology anonymity is the state of non identifiability within a set of subjects (e. g. people) the anonymity set. The anonymity set is a set of subjects which are able to trigger actions and/or which are addressed by actions. I. e. subjects are sender or receiver within a set of senders respectively a set of receivers. If a attacker is unable to identify the connection between a single user and a specific sender resepctively to receiver, then the user is anonymous. Anonymity is not the anonymity of senders and receivers, it's the anonymity of users (8).

Welbourne et. al. have engineered tools for RFID-Systems with which users can delete the data the system has stored about them. The user can easily implement rules about who should read which data when, and which concatenations the system is allowed to do. With this it is possible to implement anonymity ("nobody is allowed to read personal data"), but the system functions nevertheless. Also the requirements of systems and authorities can be implemented and recorded. This is an example for technologies with which anonymity can be implemented in ubiquitous computing and ubiquitous surveillance (12).

Untraceability

Also untraceability is described from a technological view here. Therefore we define Data, Entities, Identities, Users, Objekts, Subjects, Services, Ressources, and so on, or instances of them as Items of Interest (IOI). IOI are „things" which an attacker is interested in. IOI are untraceable, if an attacker is unable to see a relation between two or more IOI's or to trace an IOI in a network. For instance if in a Car to Car Safety Message System there is a message exchange, then messages has to be untraceable to one of the car's such that there is no possiblity to trace the track of the car (10,2,5,1,3,8).

The same holds when clothes have RFID-tag's on it and when they pass different readers in a while (4).

Untraceability in this way can be implemented as follows (4):

1. the reader sends a messag to the tag with a nouce-identifier N_R.

2. the tag generates a new nouce-identifier N_T and sends this, the encrypted tag-ID h(ID) und the encrypted nouce-identifier pair $h_{(ID)}(N_R,N_T)$ back to the reader. The reader passes that triple to the application system. The application system decodes with the key h and computes with the known nouce-identifier N_R the nouce-Identifier N_T. With this the application can verify the ID of the tag.
3. If the application system accepts the tag, it computes a new tag-ID. The tag also computes a new tag-ID with the same algorithm. The application system with new tag-ID generates the encrypted message $h_{(ID+1)}(N_T,N_R)$ and send this to the tag.
4. The tag evaluates the message and the new ID. If the received ID is the same as the ID computed by the tag, the old ID and the nouce-Identifier N_T are erased from the tag-store.

For an attacker the tag is untraceable, because it changes its ID with each message transfer. Traceability of the tag by the applicationsystem is still possible (4).

The above examples presented for implementing anonymity and untraceability show the possibility to implement privacy in ubiquitous systems as it is required by Roßnagel (9). Needed are the legal frameworks to require such privacy features in ubiquitous systems. By defining this sort of legal framework there should be answers to the following questions:

1. Who is the owner of the data an RFID-Reader explores and an application system computes and stores?
2. Are there marking obligations for items with RFID-tags on it (e.g. clothing, food)?
3. Is it necessary to require offical approval for the installation of RFID-readers and sensors?

When CCTV in public places appeared in the 1990'iesth Gras (6) showed that it is much more difficult to regulate and rule the use of technologie when already installed, than before installation and use. Therefore it is important that legislation keeps pace with technological progress.

References and Notes

1. Arapinis, M.;Chothia, T.;Ritter, E.;Ryan, M.: Analysing Unlinkability and Anonymity Using the Applied Pi Calculus http://www.cs.bham.ac.uk/~tpc/Papers/csf10.pdf, visited 16.12.14
2. Blues Team: Unverkettbarkeit und Pseudonymität in der digitalen Welt, http://blues.inf.tu-dresden.de/prime/EUT_Tutorial_V0/german/german/Content/Unit2/dig.%20unlink.htm, visited 16.12.14
3. Brusó, M.; Chatzikokolakis, K.;Etalle, S.; Den Hartog, J.: Linking Unlinkability https://hal.inria.fr/hal-00760150/PDF/Unlinkability.pdf, besucht am 16.12.14
4. Dimitriou, T: A Lightweight RFID Protocol to protect against Traceability an cloning attacks, http://www.ait.gr/export/TDIM/various/RFID-securecomm05.pdf, visited 18.2.15
5. Fischer, L.: Measuring Unlinkability for Privacy Enhancing Technologies, http://tuprints.ulb.tu-darmstadt.de/2367/1/lars_fischer_dissertation.pdf, visited 16.12.14
6. Gras, M. L.: The Legal Regulaiton of CCTV in Europe, http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/3375/3338, visited 17.02.15

7. Gerichtshof der Europäischen Union: „Der Gerichtshof erklärt die Richtlinie über die Vorratsspeicherung von Daten für ungültig“, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf, visited 17.02.15
8. Pfitzmann, A.; Hansen, M.: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, http://freehaven.net/anonbib/cache/terminology.pdf, visited 16.12.14
9. Roßnagel, A.: Datenschutz in einem informatisierten Alltag, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf, visited 19.11.14
10. Rost, M.; Pfitzmann, A.: Datenschutzziele, http://download.springer.com/static/pdf/814/art%253A10.1007%252Fs11623-009-0072-9.pdf?auth66=1416396902_c7935e6bcf15afa95108ffb192c1fd9f&ext=.pdf, visited 19.11.14
11. Taylor, N. : State Surveillance and the Right to Privacy, http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/3394/3357, visited 17.02.15
12. Welbourne, E.; Battle, L.; Cole, G.; Gould, K.; Rector, K.; Raymer, S.; Balazinska, M.; Borriello, G.: Building the Internet of Things Using RFID, http://www.researchgate.net/profile/Kyle_Rector/publication/220491250_Building_the_Internet_of_Things_Using_RFID_The_RFID_Ecosystem_Experience/links/0c960519d82721508d000000.pdf, visited 18.2.15