Andreas Pfitzmann 1958-2010: Pioneer of Technical Privacy Protection in the Information Society

Hannes Federrath, Marit Hansen, Michael Waidner

Andreas Pfitzmann 1958-2010

Pioneer of Technical Privacy Protection in the Information Society

Hannes Federrath, Marit Hansen, Michael Waidner[1]

Abstract. On September 23rd 2010, Prof. Dr. Andreas Pfitzmann died at the age 52 after a short but serious illness. The focus of his reasoning had been the individual and with him the society, in which he lives. During his life as a researcher Andreas Pfitzmann contributed decisively and groundbreakingly to the technical implementation of the constitutional right to informational self-determination.

The academic career of Andreas Pfitzmann began in 1982 at the University of Karlsruhe as a research fellow at the chair of Prof. Winfried Görke. From the beginning he was certain that even though his research work had to have a strong technical core, it was at the same time more important to have social significance and value. In 1983, the Federal Constitutional Court of Germany developed in its Census Decision the term "Right to Informational Self-Determination". Andreas Pfitzmann was one of the first to recognize that the implementation of this right could only succeed if law and technology interacted.

In 1983, the Federal Constitutional Court declared: "Under the modern conditions of data processing free development of personality requires the protection of the individual against the unlimited survey, storage, use and disclosure of his personal data. [...] Whoever cannot overlook with sufficient certainty, which of the information regarding him in certain areas of his social environment are known, and whoever cannot measure the knowledge of possible communication partners to any degree, can be fundamentally limited in his personal freedom to plan and make decisions out of his own self-determination. A society in which the citizen cannot know anymore, who knows what, when and at which opportunity about him, is not compatible with the right to informational self-determination." (1. BvR 209/83 paragraph C II.1, p. 43)

[1] Our thanks for references, amendments und corrections go to Katrin Borcea-Pfitzmann, Rüdiger Dierstein, Rüdiger Grimm, Hermann Härtig, Steffen Hölldobler, Hartmut Pohl, Kai Rannenberg and Manfred Reitenspieß. The text was translated from German to English by Donate Reimer. An extended German version of this text has been published in Informatik Spektrum Heft 1, 2011.

Working for a university department specialized in computer architecture and fault tolerance, Andreas Pfitzmann began to research network anonymity, pseudonyms, signatures and electronic legal transactions in 1983. Together with his students then and later colleagues, Birgit Pfitzmann and Michael Waidner, he founded a working group and converted his office into the "Café Pfitzmann" as the group, that worked there more or less around-the-clock, consumated enormous quantities of coffee, peppermint tea and chocolate.

Within a year the group developed basic terms for what was later to be called "Privacy by Technology" and "Multilateral Security": Privacy has to be supported, controlled and finally enforced by technology. Privacy cannot only be achieved by law. Systems that are used by multiple parties have to support the security interests of all these parties. Then revolutionary and utopian, these thoughts now are commonly used in Computer Science as „Privacy Enhancing Technologies (PETs)".

In 1984, Andreas Pfitzmann met the American cryptographer David Chaum. Chaum then worked for the CWI in Amsterdam, where he developed the cryptographic background for pseudonymity and anonymity within networks. Andreas Pfitzmann soon recognized the practical potential of the theoretical works of David Chaum and an intensive working relationship developed between the two groups that continued over many years.

Andreas Pfitzmann began to probe the theoretical concepts of David Chaum and others as to their pracitical value. Then as now, privacy and security were seen as in opposition to one another within the political debate. With their publicaton "Legal Security despite Anonymity" the group around Andreas Pfitzmann tried to explain coherently to lawyers and technicians how privacy and security could be made compatible.

Approximately from 1987 on, Andreas Pfitzmann began to analyze the developed concepts and methods for privacy enhancing technologies in prototypical implementations and system concepts. Together with students in Karlsruhe and later in Hildesheim he developed the presumably first data protection practicum in Germany.

In 1988, the group around Andreas Pfitzmann developed and analyzed for the first time the concept of "ISDN-Mixes" – the first practically applicable method for anonymous communication in real time. With his method and many of his other ideas, Andreas Pfitzmann was ahead of the main stream by 5-10 years: What used to be labeled as utopian with regards to ISDN, proved to be visionary and groundbreaking with the success of the internet in the mid-90s.

In 1989 Andreas Pfitzmann earned his Ph.D. for his dissertation: "Services Integrating Communication Networks with Participant-verifiable Privacy" and in 1991, he moved on as an assistant professor to the chair of Prof. Joachim Biskup at the University of Hildesheim. Together with David Chaum he applied for the EU

project “CAFÉ“, which implemented and demonstrated the practical application of the first secure and anonymous smart card based payment system.

In 1993, Andreas Pfitzmann received a professorship at the Technical University of Dresden. With his promotion to professor he began his scientific work at the TU Dresden. His article on the protection of mobile participants from monitoring and localization published in 1993 in the German journal “Datenschutz und Datensicherheit“ (= Data Protection and Data Security) was trendsetting for his work at the TU Dresden within the first four years. In the beginning he dealt with the application and adaption of “ISDN-Mixes“ to GSM-based mobile networks. With research funds from the German Research Foundation and the Gottlieb-Daimler- and Karl-Benz Foundation, the newly founded working group around Andreas Pfitzmann developed methods for mobile networks that contrasted the popular acceptance that mobile network operators had to know the constant geographical locations of its users, with new solutions regarding the protection of confidentiality. Suddenly it was possible to be available by mobile phone without the network operator always knowing ones current whereabouts.

Within the context of the Daimler-Benz Kolleg „Security in Communication Technology“ the terms “Technical Privacy“ and “Multilateral Security“ were developed further in the years 1993-1999 by him and other scientists, mainly the head of the Kolleg, Prof. Günter Müller, and the Kolleg coordinator, Kai Rannenberg. With regard to “Multilateral Security“ the protection interests of all participants had to be embraced as well as the resulting protection conflicts at the time of establishment of any communication connection.

Andreas Pfitzmann received great recognition from science, industry and politics. The Alcatel SEL Foundation awarded him with the research prize “Technical Communication 1998“, which was a milestone in the public perception and general acceptance of his works. Among his great political successes was his work during the crypto-debate of the 90s. When, around 1997, the experience of governmental powerlessness with regard to surveilling internet communication assumed grotesque shapes, the scientist and citizen Andreas Pfitzmann unremittingly fought for the free und unlimited application of cryptography in the internet. One of his essential messages was that with a ban on crypto, criminals could use unobservable technical concealment possibilities, while innocent citizens became transparent persons for the state.

From 2000 on, important works of Andreas Pfitzmann and his group concentrated on the area of anonymous communication in the internet. Together with Hannes Federrath and Marit Hansen, he successfully requested adequate research projects from the German Research Foundation and the Federal Ministry of Economics. With the internet anonymization service AN.ON he produced one of the first self-protection tools for citizens and companies alike, which made the early theoretical works for the internet practically applicable.

His teaching and students were most important to him. In 2001, he was the first to receive the Best Course Award of the Department of Computer Science at the TU Dresden for the best course in the graduate study programme. As a long-standing dean of the Department of Computer Science, he lived and cultivated the unity - and freedom - of research and teaching.

With his expert report on the "Modernization of Privacy", commissioned by the Federal Ministry of the Interior in 2001, which he co-edited with Prof. Hansjürgen Garstka, he hoped that his ideas of technical privacy protection would also be reflected in legislation. The upcoming amendment of the Data Protection Act can make this wish finally – almost a decade later – come true. Again, it becomes apparent that Andreas Pfitzmann was ahead of his time. In any case, his latest works on the extension of the classical protection goals (confidentiality, integrity and availability) by special privacy protection goals such as transparency and unlinkability will have an impact on legislation. Federal data protection commissioners have referred to them in their current discussion.

Andreas Pfitzmann was invited as an expert to the political debate as well as requested by different courts, among others on issues like the application of biometry, on data retention and on online investigation. He particularly received considerable attention as an active expert for the Federal Constitutional Court on online investigation in 2007. Hence, he contributed to the phrasing of a new "Computer Constitutional Right" through the Federal Constitutional Court in February 2008 for the "Guaranty of Confidentiality and Integrity in IT-Systems".

The topic of "Anonymity" in its diverse facets formed a big part of his research works. During his "Workshops on Design Issues in Anonymity and Unobservability", organized in 2000, from which the yearly „Privacy Enhancing Technologies Symposium" (PETS) developed, he started the attempt to systematically edit the terminology of Anonymity and related terms. Presented by Andreas Pfitzmann and Marit Hansen, the „Terminology-Paper" was improved with the help of contributions from the community over the last 10 years [http://dud.inf.tu-dresden.de/Anon_Terminology.shtml].

In the early days, Andreas Pfitzmann's view on privacy protection was dominated by the concept of data minimisation: If there are no personal data, there is no risk that they will be misused. As in many cases absolute data avoidance is impossible, he expanded his view on privacy protection by the principle of control through the individual concerned – this fits in well with the right to informational self-determination and the concept of multilateral security. His research works - since 2000 - on the issue of identity management also emphasized this. From 2004 until recently, he and his research group published within the scope of the EU-funded projects "PRIME – Privacy and Identity Management for Europe" and "PrimeLife" important contributions in the area of "Privacy Enhancing Identity Management" in the online world. Furthermore, he was significantly involved in the European Network of Excellence "FIDIS – Future of Identity in the Information Society" (2004-2009). He was able to sketch his latest suggestions on privacy concepts, which

on the one hand should enable life-long privacy and on the other hand should provide a contextual binding of personal data, at the IFIP/PrimeLife Summer School in August 2010- therewith giving new impulses to the PrimeLife Project.

Visionary and Pioneer

Andreas Pfitzmann was a visionary and a pioneer. With his distinctive observation skills, his deep understanding of details, his high intelligence and determination to bring together people with similar – as well as different – interests, he contributed invaluably as a scientist and human being to improving our world.