Trends of Privacy and Surveillance in the Information Society

Klaus Brunnstein

Trends of Privacy and Surveillance in the Information Society

Extended Abstract

Klaus Brunnstein
(invited lecturer)
Department for Informatics, University of Hamburg, Germany
brunnstein@informatik.uni-hamburg.de

In the late 1980s, when large computers still dominated the application of Information Technologies to enterprise, industrial development and university research, and when small computers and networks had only begun to develop, some experts (mainly from the USA) predicted that future IT could be applied to government agencies as "Community Information Utilities (CIUs)". As contemporary IT was regarded inadequate (insufficient process and storage capacities, no remote access, missing system and software application), a moratorium for applications was suggested until the adequate IT would be available. Visions included many advantages for the citizen, such as availability and accessibility of public information and direct access for citizens to services from governments and agencies, to support "Free Flow of Information (FFO)" (as enshrined in the constitution of the USA). Experts suggested developments to related software, but technical matters concerning protection in hardware, systems and application programs were not addressed, and protection of the citizens private information – aka privacy – was not sufficiently discussed.

Indeed, both the technical capacities of small, distributed and connected computers and manifold applications, developed much faster than anticipated. These developments were governed by the principle "Enable Global Free Flow of Information", which has been realized in contemporary Internet services, social networks and mobile technologies. As provisions for protection of information (both data representing possibly sensitive information, as well as methods to work with such data) were not sufficiently designed and implemented into systems and applications. Service providers (e.g. in telecom and communication industries and social networks) today use available data without reference to the needs and interests of customers who use "their" data. Not surprisingly, customers begin to adapt their understanding to technical options: although a user "profile" contains potentially sensitive data that may be used against the respective person at some later stage, many users don't use minimal measures to inhibit illicit usage of related data (e.g. by using protective options), and worse, customers use methods of remote surveillance inherent in their personal IT (mobile search for "friends").

As in the past, technical developments will continue to shape the usage of IT in the future, following the principle: "All that is technically possible, will also be realized and used". Technical trends will support the storage and processing of much larger amounts of data, globally accessible and consequently stored in globally available storage ("clouds"). Significant growth of data streams and storages will essentially

come from enabling physical actors (from sensors to multiple devices, including heartbeat controllers, machines and factories) to communicate over global communication lines, for example: a suitably (e.g. IP3 protocol) equipped Internet/Web 3.0 interface. With the demand to remotely control processes (thus enhancing possibilities for surveillance) and to store growing masses of data, system and application software will become more complex and more difficult to analyse (including certification). With equally growing opportunities for new kinds of applications and services, the demand for more specific data will also lead to less control by users and customers and therefore to less protection of sensitive data. As data and processes will also be sensitive for enterprises, there is some hope that their interest and request for data protection will also help users and customers to protect sensitive personal information (aka “privacy”).