

Matthias Kaiserswerth
IBM Zurich Research Laboratory
Säumerstrasse 4
CH-8803 Rüschlikon

THE THIRD MILLENIUM -- OR -- THE TECHNOLOGICAL ODYSSEY

PRIVACY AND THE CONTINUING EVOLUTION OF INFORMATION TECHNOLOGY

EXTENDED ABSTRACT

The presentation explores where information technology will take us in the next ten years. We attempt to identify the privacy implications that this technology evolution will bring with it and briefly present some research ideas and projects for privacy enhancing technologies to cope with the increasing challenges to privacy.

Information Technology Evolution

For the future of information technology we can identify five major trends which all have implications to privacy:

THE FIRST TREND: In the next ten years computing will continue to become more and more powerful as far as speed, density of packing, bandwidth, and storage are concerned. There are some fundamental limits to certain technologies, but at the same time we know from past experience that there has always been some invention or disruptive technology that allowed computing power to remain on its exponential growth curve. For a given performance point, this trend also implies that computers will become cheaper and cheaper or smaller and smaller.

From a privacy point of view this tremendous growth will allow us to build PCs that might recognize emotions and talk like human beings. A multi-media telephone might record each conversation, and automatically identify the caller using voice recognition and provide all the information about the caller it can find on the Internet. Everything one ever communicated electronically or did or said in a public place, might be recorded. Information once collected will never disappear. Anything can be observed - nothing remains local anymore. Even non-digital transactions will leave digital traces.

THE SECOND TREND: Everything is going online. Whereas in the past the world was modeled in large computers, today computers and intelligent sensors are deployed throughout the world. Microprocessors are everywhere, everything - not only PCs - is getting connected to the Internet. Mobile phones can be located within a few hundred meters, and can automatically make an emergency call if needed, cars communicate their position, speed, how they're driven etc. Jewelry will be intelligent bio sensors, connected with doctor's offices over the net, and with myriads of bio sensors and actors flowing through peoples bodies.

THE THIRD TREND: A utility-like model for value delivery through IT is emerging. This trend is driven through the fact that we all use a common shared infrastructure, the Internet, and that there are powerful economic incentives to provide ever more complex IT services electronically. We are seeing the first examples of this in the nascent xSP (Application Service Providers, Storage Service Providers, ...) industry. Personally identifiable information (PII) is pushed into the network, onto edge servers: the servers collect, manage and disclose PII on behalf of individuals. Servers operate on PII on behalf of providers of end services.

This e-utility model is made possible through standardization and the increasing reuse of software building blocks, which is described by THE FOURTH TREND: As computers become more and more powerful, software also becomes increasingly more capable. Newer software development techniques, such as object-oriented programming, and environments such as Java have increased programmer productivity by an order of magnitude and have led to an environment where software building blocks have become the business. People no longer argue about whether they use Linux, Windows 2000 or some other operating system, but rather ask what business level objects are deployed and whether they are compatible with each other. This compatibility leads again to being able to set up electronic business relations with suppliers and customers quickly to move into a world of dynamic e-business. Such software standardization without enough focus on methods to assure the security of information handling systems leads to a situation where attacks can be written once and applied everywhere. We observe that on average 2-3 new vulnerabilities are discovered daily, well-known vulnerabilities do not get fixed and the continuing focus on features and functions leads to an extremely fragile infrastructure. Using exploits such as buffer overflows permits the large scale theft of PII with consequences yet unknown.

THE FIFTH AND FINAL TREND IS CALLED "Optimize to Survive". It says that in the future, computing in an enterprise will be used not only for traditional process automation and internal efficiencies (ERP, accounting, ...) but primarily to reinvent businesses. We are already seeing examples of pharmaceutical companies, financial institutions, etc. that use high-performance computing to invent new products or to redefine their value chain in ways impossible until now. PII is an important ingredient for optimizing many businesses, for example in merging and mining the data collected in customer relationship management systems or in the future to customize medication to an individual genetic profile.

Privacy Enhancing Technology Requirements

From the examples presented, one might get the impression that these trends inevitably lead to a world without privacy. But technology can also solve, or at least alleviate the problem. Identity management systems and intelligent tools for blocking, filtering and customization will help individuals to limit the amount of personal information released to what is really necessary and intended. Of course, once released, personal information can never be taken back. Therefore, creating awareness will be key to privacy protection.

Enterprises need specific privacy enhancing technologies, ranging from tools for the design of privacy enhancing business processes to tools supporting the creation, management and enforcement of privacy policies. New customer privacy services will be offered, giving individuals access to their personal information.

The infrastructure will provide some privacy enhancing services, like confidential or even privacy protecting communication and all types of trust enablement. Following the general trend, more services will be taken over by the infrastructure. It is important to ensure that such infrastructure services are provided in a secure and dependable way: there must be a variety of independent service providers giving individuals some choice, and their services must be based on open standards that have been carefully evaluated by the scientific community.

Privacy Research at IBM

IBM Research has created a global research program to develop new privacy enhancing services and technologies. Some sample projects will be briefly presented below. We primarily focus on enterprise and infrastructure aspects. All technology is designed to satisfy both the need for privacy protection and the need for safety, i.e., whenever a technology provides anonymity any misuse is prevented: anonymity can always be revoked by a trusted agent.

One of our projects is developing a privacy enhancing, pseudonym-based public key infrastructure. Like in an ordinary PKI, individuals receive certificates and can use them in e-business transactions. Using an normal certificate typically releases much additional information about the certificate owner. By employing modern cryptographic techniques we enable an individual to just prove a certain fact, e.g., that the owner is a citizen of Zurich. No other information is revealed.

Together with IBM's Global Services organization IBM Research developed a comprehensive, flexible Enterprise Privacy Architecture that allows an enterprise to define and implement an enterprise-wide privacy program.

One novel concept of this architecture is the Sticky Policy Paradigm: At least conceptually, personal information always comes with a specific privacy policy, agreed to by the enterprise and the individual. The architecture ensures that this link is never broken, not even when personal information is disclosed to another enterprise. This is in contrast to ordinary security policies that are defined just by the enterprise, and where policies are rather attached to types of information but not to individual pieces. In general, authorization due to a privacy policy is significantly more complex than one due to a security policy.

Several components are needed in an enterprise to manage and implement such privacy policies. Besides components implementing authorization and audit, the Enterprise Privacy Architecture also supports customer privacy services, like access to personal information, the use of privacy enhancing authentication like the privacy enhancing PKI, and generation and use of depersonalized data, e.g., for data mining.

Data mining is often considered as the "worst case" in privacy. One of our projects investigates how statistics can be precisely computed from truly depersonalized data: Data are depersonalized by stripping off all identifying information and by randomizing all numerical data so that they do not contain any information about the individual anymore. The project has shown that if this randomization is done in a specific way, then nevertheless certain statistics, like averages or correlations, can be precisely computed. Thus privacy and statistical data mining can actually be combined.