Designing databases that enhance people's privacy without hindering organizations

Article *in* Ethics and Information Technology · March 2006

DOI: 10.1007/s10676-006-9105-3

1 author:

Thomas Hodel
Bern University of Applied Sciences
33 PUBLICATIONS **163** CITATIONS

SEE PROFILE

Designing databases that enhance people's privacy without hindering organizations

Thomas B. Hodel, Niklas Auerbach, Alma Schütter, Klaus R. Dittrich
University of Zurich, Department of Information Technology
Winterthurerstr. 190, CH-8057 Zürich, Switzerland
{hodel, auerbach, dittrich} @ifi.unizh.ch, alma.schuetter@iew.unizh.ch, http://www.ifi.unizh.ch/

Abstract
Heteronomy – the lack of self-determination - expresses exactly how our personal data are often treated by organizations. Inspired by the tenet of autonomy from Immanuel Kant, we argue that future database systems must provide autonomy for individuals regarding the privacy of their data. We identify privacy invasive technology and existing privacy enhancing technology. We argue that despite the existence of a variety of privacy-enhancing technologies, there is still need for new approaches to data processing in systems that process personal data of identified individuals. We enunciate the reasons for ending heteronomic database systems, which include legal, organizational and technical issues. Finally, we propose a design for an autonomic database management system, identify challenges and problems, and suggest some approaches to these. Our main goal is to achieve a widely-accepted realistic and practical solution in order to ensure privacy for individuals in our future world, yet without hindering business and security.

1 Introduction

The explosive development of privacy-invasive technology like *identifying technologies* [Covell 1998] [Warwick 2002] (biometric technologies, radio frequency identification, bio-implants, DNA sniffers), *location based services* (cellular systems, wireless local area networks, bluetooth, ultrawide band) and *ambient intelligence* [Ducatel 2001] [Weiser 1991] shifts privacy issues onto a global level.
In this paper- also in the context of a digitalized world - we interpret privacy as the right of individuals to exercise autonomy in controlling their personal data. In order counter privacy-threats resulting from today's information systems, privacy-enhancing technologies such as *digital identity managers* [Registratiekamer 1995] [Gabber 1997] [Köhntopp 2000] [Jendricke 2003], *pseudonymous credentials* [Chaum 1985] [Camenisch 2001], *anonymous communication technology for the internet* [Goldschlag 1999] [Reiter 1998] [Berthold 2001] [Chaum 1981], and the *platform for privacy preferences* or *privacy-protection systems at the enterprise level* [Karjoth 2003] [Agrawal 2002] [Westin 1967] were developed. All these systems contribute valuable solutions for enhancing privacy.
We are inspired by the tenet of autonomy from Immanuel Kant, and promulgate the end of heteronomic database systems. It is time for individuals to regain control over their private data, and that people get control over their virtual shadows, which are spread over a number of information systems in different organizations. We argue that future database systems must provide autonomy with regard to data processing. We will enunciate the key principles for data processing systems that pertain to autonomy in data processing. Our principles are built on current privacy legislations and guidelines, and do not only address technical issues, but also include legal and organizational points. We propose a design based on our principles, identify privacy and security challenges, and suggest some approaches to solving these problems. Our main goal is to find a realistic and practical solution to return the control and autonomy over personal data to private individuals. Such an approach can increase privacy and end the current heteronomic approach, in which organizations handle private data - hopefully in accordance with existing data protection laws – but often without a person's knowledge or consent.
If such an approach should be widely accepted, its impact dare not hinder business and/or national security. Therefore we do not claim that our system guarantees complete privacy but we believe that this concept can influence people's awareness about their personal data. We do not intend our proposal as a replacement for

existing privacy-enhancing technologies (see part 3) but rather as an additional concept which could be used within these technologies. We also recognize that not all data live in database systems. We hope that the use of heteronomic databases will soon come to an end and that our concept will provide additional inducement for personal data to be sent back to where it belongs. If nothing else, our concept of a user-controlled Personal Data Identification System may provide guidance for similar structures in other types of data repositories.
In the next part we present a summary of privacy-affecting technologies and discuss privacy and security issues. Following this we describe state-of-the-art privacy enhancing technology, whereby a comparison emphasizes lacks and outlines potential for new technologies. We motivate the concept of heteronomic databases in this section. Our privacy enhancing data processing concept (see part 4), which separates business data from personal data, so that matching data can be controlled by the person involved, will build up trust and confidence in Information Society services. It empowers people by strengthening a user's control over its own data and the kind of processes he or she allows.

2 Privacy invasive technology: an overview

This chapter examines new and emerging technologies which can compromise individual privacy, based on their usage. These are identity-related technologies, location-based services and ambient intelligence technologies. However this chapter does not claim to cover the topic in full.

2.1 Identity-related technologies

The characteristics of identity may be described as follows: "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (EU Directive 95/46/CE on data protection, Article 2). Identifying people is a critical issue; it encompasses the citizen's privacy and security concerns. The identity-building process includes unity, permanence, and physical characteristics. The identification process itself, includes proof of true identity, verification, recognition, and authentication of identity. This process can be represented by four questions: What are you, what do you know, what do you have and what do you do. The final question is based on data mining and data processing results.
New tools, challenging proof, theft, loss of identity and multiple identities, have to manage the identification. Digital identity [Covell 1998], with digitized human characteristics such as identity, behavior, biological features, etc., will replace today's indicators like, for example, name, telephone number, etc. This new form of identity enables new digital services but brings new risks. A uniform system to identify users in cyberspace would have dramatic consequences. An **identity management system** [IMS 2003] enables new services, reduces the level of risk and therefore creates a trustworthy environment; it can also help in finding an acceptable balance between privacy and security needs.
Under **biometric technologies** we understand a genetic characteristic of people using technology for identification. Using biometrics for authentication is itself not new, but that machines are able to process biometrics is a new dimension. This technology, using unique human components such as fingerprints, iris, face, voice and DNA, is the quasi-perfect solution for identification. Some methods, like iris scan and face recognition, are contact-less biometrics technologies. Several biometric data can be merged to try to reach a higher level of protection. In addition to this, the risk of loss generated by using biometrics is very low, or in other words, it is very difficult to change biometrics for the user.
Radio frequency identification (RFID) technology is a wireless system for identification.
It allows remote non-contact or the automatic reading of RFID-enabled objects. These objects are built-in 'active' and 'passive' tags. Active tags, powered by an incorporated energy supply, offer a permanent connection and a long distance communication. Passive tags are energized by an antenna emitting radio signals. They just have a short-distance communication, up to about four meters. These tags can be embedded in nearly any object, such as bank notes, clothes or even razor blades, because they are almost invisible.
Future identification technologies are bio-implants and DNA sniffers. A **bio-implant** is a tiny implanted chip which has communication capability. This could be management of access levels, location data,

personalization of the nearby environment, or communication with other chips (e.g. bio-sensors) or with real-time medical systems, for example. Bio-implants can build an 'augmented' human body [Warwick 2002] and can therefore also be used in creating an identification process. **DNA sniffers** work on the basis of DNA fingerprints, a far simpler method than DNA sequencing. It can be compared with RFID, because identification also occurs without direct contact. The sniffer correspond to the RFID reader and human cells act as the equivalent of tags. This technology is the leading candidate for future identification systems.

2.2 Location based services

Location based services (LBS) claim to be accurate in physically locating users. Therefore wireless communication and location computation technologies can be used. LBS could be targeted at a variety of areas: commercial, location-specific content, accurate geographic information or even at health administration and entertainment.

Wireless communication technologies, providing location services, close the gap between the physical and the virtual world by delivering related virtual information to the other side. Examples of LBS, such as cellular systems, wireless local area networks, bluetooth and ultrawide band are discussed more precisely in the next section.

Cellular systems are the most common type. The European standard GSM (Global System for Mobile communications) has become the main mobile system world-wide with about 909 million subscribers across 200 countries (September 2003) [Gsmworld 2003]. The successors of GSM are HSCSD, GPRS and UMTS (Universal Mobile Telecommunications System). All of them increased the speed of transmission step-by-step, while UMTS reached broadband technology.

Wireless local area networks (WLAN) is another wireless technology with a connectivity range of about 100 meters, more commonly known as 'hot spots' (physical locations where WLAN access is provided). It is often used in train stations, airports, city halls, hotels, business centers, university campus, enterprise premises, as well as in private homes.

Bluetooth was developed to replace cables with devices up to a range of about 10 meters, but can be extended to more than 100 meters.

Ultrawide band technology enables the reuse of frequencies already assigned to wireless services and is therefore an alternative to cellular systems.

Different location computation technologies exist, based on the available possibilities and the target service. They may also be computed for a specific location-based service such as emergency-, in-car-, location information services, and for tracking and tracing. These services can be controlled by the user (explicit request from the user) or by the operator (without any control from the user). Satellite techniques (Navstar, Glonass, GNSS) are controlled entirely by the user, whereas terrestrial techniques (Cell id, observed time difference, Bluetooth and WLAN) are normally processed by the operators.

The geographic coverage is mapped by **cells** in a cellular system. User equipments run in a specific cell, which can always be determined by the operator. By means of **enhanced observed time difference** and **observed time difference of arrival** techniques, measurements from a pair of downlink transmissions, the position of an electronic device can be located with an accuracy of around a hundred meters. **Bluetooth** and **WLAN** are able to compute any user location from the position of the fixed access points. WLAN can do this with an accuracy of about 100 meters, and Bluetooth, with the additional possibility of getting their positions from other recently located users, to within about 30 meters. Using the signals transmitted from a satellite constellation, **global positioning systems** (GPS) can compute their position. Such satellite techniques are accurate up to half a meter. Further advantages of GPS are its global coverage and low impact on existing communication networks; its disadvantage is the signal's weakness indoors. A major impact on the performance of location technologies is achieved via the combination of the different terrestrial and satellite techniques.

2.3 Ambient intelligence space

Ambient intelligence and virtual residence provide a vision of the future. Humans will be surrounded by intelligent interfaces supported by computing and networking technology which will be embedded in everything. These objects, such as paper, roads, vehicles, furniture, clothes and smart materials are ubiquitously connected and always "on". Computing capabilities enable interaction with each other and with the environment. These devices will become increasingly smaller and cheaper and will be able to sense, think and communicate [Ducatel 2001]. Several terms reflect this vision: **ubiquitous computing, pervasive computing, disappearing computing, proactive computing, sentient computing, affective computing, wearable computing and ambient intelligence**. The term 'ubiquitous computing' is coined by [Weiser 1991] "the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it". While the terms ubiquitous and pervasive computing are predominant in the US, ambient intelligence is clearly more prevalent in Europe. Three key technologies will denote our future: intelligent user-friendly interfaces, ubiquitous computing and ubiquitous communication, realized by interconnected, invisible, intelligent and ubiquitous computing. This vision carries with it a high risk of losing one's privacy. Therefore the Information Society Advisory Group stresses the importance of giving control over ambient intelligence services and interfaces to ordinary people. Ambient intelligence is a vision which would have tremendous social implications, yet despite this the academia and industry investments in research and technological development within this field are enormous.

2.4 Privacy issues

The above-mentioned technologies certainly risk the loss of anonymity and raise a number of privacy concerns. Only remarkable points are extract in this parts.

Identity management systems could play a critical tool for the citizen, based on the growing number of services. A unique access tool creates an 'electronic' witness of a major part of the citizen's online life. Furthermore these technologies have to comply with the regulatory framework concerning privacy rights. To manage and control these data is very difficult, especially if the entities are not from the same regulatory territory. Such a system could be organized centrally or decentrally. The advantages and disadvantages of it are discussed in part 4.6.

Biometric data are sensitive and of a personal nature. Therefore even if it is forbidden by law, the risk of being disclosed to a third party is high. Numerous privacy concerns are raised within this topic. Biometric data fully identify a person and provide additional and sensitive information. Medical specificity can be found in fingerprints, iris image, and retina scan, for example. Iris scan and face recognition do not require contact therefore they are more risky for privacy, because they can be diffused or hidden in the local environment.

RFID tags can be accessed as well 'contact less' since they are also invisible. Therefore RFID tags raise specific privacy concerns such as user awareness and empowerment. RFID tags represent a sort of identity management system, as soon as the tags are linked to the owner of an object, thus defining the extent of privacy compromise.

In the near future, cellular system and WLAN technologies will diffuse mobile broadband services. Wireless communication increases privacy concerns regarding personal data, traffic data and location data. Negative consequences may arise for users when databases are mined.

Location based services raise important privacy questions. All citizens will have a shadow in the virtual world. Physical location and movements will be stored as personal, traffic and location data within the virtual world. Different parties are involved in the value chain of a location based service, therefore there is an even higher risk with regard to respecting and protecting privacy rules.

Monitoring and surveillance capabilities, using ambient intelligence, will emerge on a large scale. This kind of technology constantly detects and monitors what people are doing, both offline and online. Some argue that this represents the end of privacy [Garfinkel 2001]. "The right to be left alone" [Warren 1890] would not exist any more. Furthermore these technologies create the opportunity to 'cross the border' [Marx 2001]. Crossing borders usually implies a privacy-invaded feeling. These borders have natural (walls, doors, clothes), social (family, doctors, judges, work colleagues), spatial , temporal, (different parts of a persons life is conveyed to different target groups), ephemeral or transitory (information may get lost and have to be deleted) characteristics. Ambient intelligence makes the crossing of these borders easier and more likely, even

although the borders are always fluid, relative, multi-dimensional, and dependant on context, culture and personal preferences. This new world of interconnected objects creating smart environments could become an Orwellian nightmare without privacy and data protection laws, organizations and technology [Mattern 2003]. The 'smart home' [Gooley 2003] and 'virtual residence'[Benson 2003] concepts are just two examples of visions within this field.

2.5 Security issues

Privacy concerns are deeply intertwined with security requirements. Within the information society, identity management systems represent sensitive and necessary tools. Their level of security, control and access environment has absolute priority. No attack, misuse or identity theft can be tolerated.

It is important to realize that biometric data cannot be used as a key, based of their uniqueness [Schneier 1999]. The ability to update or destroy such a key is not given and other characteristics of a key like secrecy and randomness are missing too. Nevertheless, these data are a useful replacement for a personal identification number or signature.

Most RFID tags only deliver a unique identification number and the corresponding information is stored in a database. This offers an easy way of accessing tags, thus raising the risk of unauthorized access to the database by, for example, a hacker, who may check, modify or even erase certain information. At this particular point, the development of RFID tags takes the opposite direction to that of smartcard.

Cellular systems from the 2G digital network communication are rather insecure while 3G security features tend to be more efficient. The GSM encryption is fairly easy to break and the lack of strong security in GSM cellular networks allows for a wide range of fraud [Third Generation Partnership 1999]. WLAN security is even less efficient. 802.1x, 802.11b and 802,1i standards offer strong authentication between access points and wireless LAN cards. Wired equivalent privacy (WEP), dynamic WEP and WiFi protected access (WPA) provide a better layer of armour against hackers.

Location data, including where and who the user is, can improve security based on locations: for example, a witness at the scene of a crime, a criminal at the time a crime was perpetrated, and triggered electronic transactions. The main drawback is certainly the increasing surveillance in the information society. The collection of location data is made possible and provides interesting information regarding users habits. This situation easily leads to data mining, discrimination and surveillance, even if the data is only processed by machines. These data might be stolen and could therefore threaten personal security.

The scale of ambient intelligence, its mobility requirements, its heterogeneity, the complexity of its hardware and software, and its distribution of knowledge and resources increase security concerns in matters of trust and dependability. Paradoxically, ambient intelligence best reflects our real world interactions. This paradigm can be described with attributes such as flexibility, mobility, temporality, context dependency, heterogeneity, de-centralization, dynamism and change. Interactions will be based on trust and confidence

2.6 Conclusion

Though many benefits could be gained from identity-related technologies, local based services and ambient intelligence space, the potential for monitoring, surveillance, data searches and mining cannot be ignored. At the very least, protection of citizens from various types of intrusion and law enforcement must be ensured when using these technologies.

Balancing security and privacy in the information society [Maghiros 2003] [Walters 2001] will be a tough task. Respecting somebody's private life has to be weighed up against issues of national security, public safety, economic wellbeing, prevention of disorder and crime, protection of health and rights and freedom of others. It is impossible to make a prediction as to which side the future will lie on, but the risk of losing privacy, the "right to be left alone" [Warren 1890], "the right to select what personal information about me is known to what people" [Westin 1967], in the information society is rather high.

From our point of view, citizens will lose their entire privacy, if nothing is done against current developments. To strengthen privacy and security, actions on legal, organizational and technical issues are required [Lessig 1999]. These three elements are included in our principles which we explain in part 4. In the following section we summarize what has already been done in the field of privacy-enhancing technology in order to combat the afore-mentioned risks within this area.

3 State-of-the-art privacy enhancing technology

In this section, we consider the concept of privacy-enhancing technologies. We will discuss the PETs that are available today and illustrate their benefits and shortcomings. We will consider identity management, P3P, digital credentials, anonymisers and privacy-enhanced database systems.
The term Privacy-Enhancing Technology (PET) originated in the mid-nineties from a study that investigated technological measures to curb the use of identifying data in information systems [Registratiekamer 1995]. Nowadays the term PET is widely used, and refers to technologies which aim to eliminate the use of personal data in information systems or to restore the user's control over the revelation of personal data [Burkert 1997]. In a wider sense, one could say that the term PET represents all technologies which pertain to protecting an individual's privacy.

3.1 Identity management

Identity management (compare part 3.1 and 2.2) aims at giving users of electronic services the power to determine for themselves which data concerning their identity should be disclosed to other parties in the course of an electronic transaction. It intends to restore the power of informational self-determination to the user. For that purpose, an electronic identity manager is installed on the user's machine that assists the user in all electronic transactions. Such a software lets the user create several profiles for transactions on the Web that each contain different amounts of personal data. Furthermore, an identity manager supports the user in the creation and management of pseudonymous identities. Such identities may be realized with the help of pseudonymous credentials.
The identity protector as proposed in [Registratiekamer 1995] was the first proposal for an identity manager. A Web-based identity manager was developed by Bell Laboratories [Gabber 1997]. Identity managers were also proposed on the basis of PDAs (Personal Digital Assistants), which the user can carry along with him at all times [Köhntopp 2000] [Jendricke 2003]. Users conduct all electronic transactions with the help of a PDA, on which the identity manager is installed.
The use of identity management solutions alone is not effective enough to prevent the creation of personal data. Nowadays, most higher value transactions require the disclosure of an identity. In such settings, identity management is hardly efficient. Therefore pseudonymous credentials (see below) must be combined with the approach of identity management to allow for anonymous transactions which provide security to service providers (e.g. by guaranteeing that users who engage in unlawful behavior can be traced). Another problem is that users can't control how their data is processed once they have released it. We see the potential of identity management solutions in the context that they may help users to manage pseudonymous identity while at the same time hiding the complexity of credential systems from them.
[Chaum 1985] introduced pseudonymous **digital credentials** as a building block for an electronic transaction system which lets users conduct anonymous, unlinkable transactions. Users set-up a different pseudonym with every organisation they deal with and conduct all transactions under pseudonyms. Since several pseudonyms of the same user can't be linked, transactions can't be traced beyond organizational boundaries. Users can obtain credentials from organizations which are used to prove statements about the holder and thus serve the purpose of establishing trust. Pseudonymous credentials also incorporate a mechanism to hold users accountable for their actions. This may, perhaps, be a trusted third party who can divulge the identity behind a pseudonym in case of unlawful behavior.
Pseudonymous credentials can be used to achieve anonymous electronic transactions while maintaining security. Anonymous transactions are clearly the most effective way of avoiding the creation of personal data records. Since statements in credentials can be disclosed selectively, they also pertain to the privacy goal of data minimization [Westin 1967]. Currently, the most advanced implementation of a pseudonymous credential system is the one by [Camenisch 2001].
Although credentials afford users the possibility of anonymous transactions, it has to said that these technologies are rather complex and may be difficult for users to understand. Anecdotal evidence suggests that many users even find the handling of X.509 certificates, which have been around for much longer, rather cumbersome. Some of the complexity of these systems can be hidden from the user via measures taken at the level of interaction design. Identity management solutions can make such systems manageable even for the

average user. Deploying such systems at the current point in time may be difficult, as there are not yet any official standards regarding algorithms, key and message formats.

Anonymous communications and transactions in the Internet can only be achieved if the underlying network allows for the creation of anonymous communication channels. Several proxy services exist that afford anonymous Internet communication to users and enable users to surf the Web anonymously: examples include onion routing [Goldschlag 1999], crowds [Reiter 1998] or the Java Anonymity Proxy (JAP) [Berthold 2001]. Onion routing and JAP make use of the mix approach, a technique proposed by [Chaum 1981] to enable anonymous untraceable email communications.

There are also tools for anonymous email communication. Such tools enable users to send and receive email under pseudonymous addresses. Two types of systems exist: The first type removes identifying information in a message and forwards it. The second type uses mix networks to anonymize messages. A very well-known remailer service was anon.penet.fi, which was closed down by its owner after Finnish police demanded the disclosure of a user's identity.

On a political level, giving users the possibility to use Internet-based services in a fully anonymous manner is often perceived as a danger to society. Anonymity makes it more difficult to pursue offenders who use the Internet to access illegal content. In the current political climate, it is more difficult than ever to argue for fully anonymous communications in the Internet.

3.2 Privacy in ubiquitous computing

The vision of disappearing, **pervasive computers** in combination with powerful, new sensor technology poses a threat to an individual's privacy (see part 2.3). This vision creates a need for technology to counteract the negative effects on privacy in ubiquitous computing environments. However, sensors such as DNA sniffers, surveillance cameras or RFID tag readers make it difficult to come up with technological solutions that protect an individual when privacy is wanted but let an individual use service involving these sensors when desired.

Researchers have proposed approaches that center around a declaration of data collection practices and the possibility for individuals to consent to these practices. If users do not express consent, they can have services deactivated. Such an approach would again rely on machine-readable privacy policies such as P3P. Users must trust service providers that data collected from sensors is indeed processed as promised. Thus, such an approach still requires users to put a fair amount of trust in service providers.

3.3 Privacy enabled data processing

The **Platform for Privacy Preferences** (P3P) is a W3C standard which enables users to inform themselves about a Web site's privacy policy and to discover potential discrepancies with their own privacy preferences. Organizations declare their privacy practices in a machine-readable format which, with the help of a P3P-enabled Web-browser, can be compared with the user's own privacy settings. Depending on the browser's comparison, a user can choose not to visit a site, or to 'opt-in' to or 'opt-out' of a specific use of data.

P3P is useful for warning users about sites that engage in privacy-invasive data processing. It also helps users to discover sites which offer them a higher level of privacy. There has also been some criticism of P3P however: first and foremost, users have no way of telling whether service providers really adhere to the principles stated in P3P policies. Unless sites are audited and certified with regard to policy implementation, users do not know whether policies are really implemented. It is also debatable whether P3P really empowers the user. In many cases, a user does not have the option of selecting a site and will just have to accept the data processing practices of a given site. In the opinion of the authors, P3P won't dramatically change the power balance between organizations and consumers.

Privacy-protection at the enterprise level as well as privacy policies which are published on Web sites are essentially promises made by organizations that they will adhere to certain data processing practices. Users have no way of verifying whether these promises are kept. The Platform for Enterprise Privacy Policies (E-P3P) is an approach to privacy enable the processing of personal data. Privacy policies are formalized and are then automatically enforced throughout an enterprise [Karjoth 2003].

Users are presented with privacy policies at the time of data collection and can consent to a specific use of data. The consent of the user to a given purpose is stored along with all data items which were collected from

a user. Whenever personal data is to be processed for a given purpose, the system consults the policy attached to the data and denies an operation if it is not in line with the practices stated in the policy. This leads to a system that effectively prevents the misuse (including unauthorized disclosure) of personal data.
Such a system can guarantee that a user's data can only be processed in accordance with a published policy – provided the system is administered correctly. However, existing systems need to be modified in order to support this approach.
[Agrawal 2002] propose a new category of **privacy enabled database systems** called 'Hippocratic Databases'; these include responsibility for the privacy of data as a central design goal. The name is inspired by the Hippocratic Oath, which has guided the professional conduct of physicians for centuries. The founding principles for these databases mostly stem from privacy legislation and guidelines, such as the Fair Informational Practices [Westin 1967].
When data is collected, users express consent to the processing of specific data items for a specific purpose. A Hippocratic Database keeps privacy metadata which records for every data item: the agreed processing purpose, external recipients (if any), authorized users and the retention period. Based on this meta-data, the system checks every query and only executes queries that are compatible with these policies. Further components include a data retention manager that deletes data when no longer needed and a query intrusion detector that flags suspicious queries based on heuristics.

3.4 Conclusion and motivation for autonomic databases

Many privacy enhancing technologies aim to allow anonymous transactions and anonymous communication in the Internet. While this is clearly the most effective approach to avoid the creation of personal data, it remains to be seen whether service providers are willing to embrace these technologies. The approach of enterprise-level privacy policies promises to guarantee that enterprises do indeed process data according to their declared policy.
We propose autonomic databases as a technology that complements existing privacy-enhancing technologies. The approach is different from existing technologies. Autonomic databases are intended for settings in which personal data is processed and in which an individual's identity is stored in the database. We perceive that transactions should be conducted anonymous wherever possible and perceive pseudonymous credentials as the most effective technological means to support a migration towards anonymous transactions.
The approach of autonomic databases further develops existing approaches to privacy-enabled data processing. We envision a data processing system that guarantees by technological measures that data is processed in line with polices. The approach of autonomic databases has this characteristic in common with the approach of [Agarwal 2002] and also with the approach of [Karjoth 2003] for privacy in data processing at the enterprise level. However, we see further need to tailor data processing to the needs of the individual if privacy is to be maintained.
Our approach comprises new legislative measures to complement the existing legal framework on data protection. On the one hand, we propose a differentiation between personal data and transactional data. Individuals are to be given full access to personal data, but not to transactional data (which is thought to be owned by the company rather than by the individual). Furthermore, we aim to bring more transparency to data processing: through a structure of portal services, an individual can monitor data processing in two ways: First, an individual can view all personal data that is stored about him or her, and second, for every data item, an organization must state how this item of personal data was acquired.
The portal aggregates views on all organization who store data concerning this individual. Through the use of a portal service, individuals do not have to manage accounts with several organizations who store data about that individual. Instead, all data can be accessed through a single point of entry.
The approach of autonomic databases thus aims to give users more control in wettings where identified transactions take place. In the next section, the design goals for such a system are stated.

4 Founding principles to end heteronomic database systems

Privacy enhancement can be understood as an increase in the control which each customer has regarding personal data which is shared with organizations. In this section, we introduce our concept for privacy enhancement and point out the key principles on which our system design is based.
Our founding principles are motivated by the value of privacy itself. These principles are rooted in existing data protection laws. They articulate what it means for a personal data collection system to responsibly manage private information. We argue for the following six 'new' principles, in addition to the several privacy regulations which already exist. In a few aspects some of the principles are related to but not similar to [Westin 1967] and [Agrawal 2002].

Consent: People know when their personal data are stored and have to consent this storage.
Purpose: Persons affected (see consent) must have the possibility to specify the purpose and usage of their data.
Separation: Personal data and any other business data have to be stored separately.
Audit: Transactions involving personal data must be recorded in transactional logs. Persons affected can then follow executed transactions and retrace usage of their personal data.
Participation: Persons affected have access to their personal data, its usage and purpose specification. They can choose where and how to manage their personal data.
Ease of use: Persons affected have the choice to bundle access to personal and audit data through portals and can define automatically applied patterns.

4.1 Consent

Nowadays almost any transaction, regardless of what it represents, is recorded. As long as no exact identification of a specific person can be made by using these data, no privacy issues are involved and there is no need for us to care about it. As soon these data are linked to personal data, however, privacy could be jeopardized as described in section 2.
The first principle is that people, whose private data are stored, must give their consent for this storage, and the specified organization is obliged to inform these individuals 'where and what' data are stored. In most cases, people do not remember which companies store their data; they often have no chance to know this because in many cases they are completely unaware of such a data collection.
Personal data can be used for evaluations and for marketing purposes. It may be sold to other companies without the customer's consent or knowledge and as well as that, such data could even be stolen. Generally people do not pay attention to who manages or what happens with their data, but as soon as they are harassed with spam, telemarketing calls or advertising mails they want to know how this problem has arisen. On the other hand, it is important that organizations are not able to refuse services to any individual on the grounds of an eventual risk. Excluding customers from setting up a life insurance policy, denying access to buildings or generally concealing information are just a few examples of this. The importance of giving customers more information about data storage and the necessity of the customer's consent for further usage of that data is evident. At the same time, organizations gain competitiveness while data management transparency is offered to customers.

4.2 Purpose

The first principle illustrates the importance of customers being informed where and what personal data is stored. Now we outline why it's important to specify the purpose as to how personal data can be used.
Personal data can be used for different purposes and it is often used against people's intentions. This data-misuse problem can be solved if organizations put the people affected in a position from which they can influence the further data management. Each organization defines its own purposes which determine the intended use of personal data. Individuals are then able to decide how these settings should be applied to their personal data. For example, a purpose specification may be to receive special offers by e-mail. Organizations can distinguish themselves from competitors and at the same time enhance trust and confidence in their services. This method of participation naturally varies from organization to organization. The only exceptions

when peoples personal data is passed without their consent are defined by legal regulations or occur during criminal investigations.

4.3 Separation

An area which urgently requires more attention with respect to privacy and security, is the stage at which business data is separated from personal data. During such a separation, business data, which contains sensitive information (e.g. about executed transactions), can be used for data mining without any need for the person's consent. Only an identifier indicates that these data belong to a specific person, so the data are anonymous as long as no connection to personal data can be made. As soon as personal data are requested for a specific purpose by linking to these data, this process must be permitted by the person affected and subsequently recorded in the audit trail.

4.4 Audit

Both people and organizations must have the possibility to understand and detect unauthorized uses of personal data. This leads us to the need for audit information where all executed transactions which accessed personal data can be traced. Such information should contain all of the following: who had when with which purpose access to what kind of personal data. This knowledge provides more security to individuals and organizations. This audit information simultaneously supports data protection and helps to minimize fraud. Usually these data are stored at the organizational side, but should be readily accessible to the persons affected.

4.5 Participation

While discussing the principles above, we saw why it is so important for people to manage and control the usage of their data. On the one hand, customers must be informed about further utilization of personal data, and on the other hand, they must be able to give their consent for any usage purpose.
To fulfill these requirements, customers need access to personal data which is stored on the organizational side. This participation can be realized in different ways, such as per telephone, forms or internet.

4.6 Ease of use

A possibility for accessing personal data is realized via web portals. The central idea is to aggregate the information shared with all the organizations we are dealing with, and to create one personal portal. This provides people with a better overview and ensures that organizations know where users are managing their data and that they are informed of any changes. The resulting benefit for organizations is improved customer contact, enhanced trustworthiness and a higher level of confidence.
This kind of information aggregation results in a possible security gap. Each person can minimize this problem by depositing their personal data on different web portals. Each portal is physically separated, certificated and protected by a password.
This solution encompasses good standards, open interfaces and the possibility for organizations to buy these systems out of the box, its main objective being to enhance the ease of use by offering standardized interfaces and always adhering to the security requirements.

5 Design

In this part of the paper, we discuss the design aspect. We study a scenario and visualize the idea of purpose specification with the help of two examples. Furthermore, we outline the structure to indicate the direction in which the set-up of such databases could be preceded, however we are unable to provide a full implementation guide.

5.1 A use scenario

Avatara and Belios are two on-line booksellers who want to enhance customers' confidence in their company by implementing an autonomic database system. The main idea is to provide a service which gives customers the possibility to define what happens after personal data is entrusted to their companies. Basically, customers set purposes for their personal data usage. During the process in which business data is separated from a customer's personal data, this anonymous business data can be used for data mining and data analysis. References from business to personal data always need a customers' consent.
Additionally, customers are able to see and verify all executed transactions in a transactional list (audit trail), which is automatically updated each time the personal data is accessed.
In this section, we look at examples revealing how the two booksellers handle this requirement and what purpose specifications they define.

5.1.1 Purpose Specification Belios

Avantara and Belios must observe legal regulations and inform customers about these exceptions. For example, in the case of criminal investigations, personal data may be handed over to public agencies without the customer's consent.

Fig. 1: Privacy Control Settings for customers of Belios

Avantara and Belios have different opinions about how much information and customer's cooperation is necessary. Belios defines only a few settings (see Fig. 1) for purpose specifications of personal data, and only asks general questions, for example, if the customer would like to receive advertisements.

5.1.2 Purpose Specification Avantara

Avantara, on the other hand, gives customers various possibilities to define purpose specifications regarding the use of their personal information. For instance, Avantara assumes that customers have preferences as to which information should come via which channel. Hence Avantara offers various channels for communication and makes distinctions between private and business phone numbers. Furthermore, customers can classify how they prefer to be contacted. These options are contracted under the tab "Contact". Under "Order", general order properties are defined, such as whether or not customers wish to be informed about their order status. Other companies and individuals are also employed to perform functions on Avantara's behalf. Examples include fulfilling orders and delivering packages, sending postal mail and emails, etc. They require access to personal information which is necessary in order to perform their functions, but they are not permitted to use it for any other purpose. Avantara guarantees that business or personal data is never passed to third parties without the customer's prior agreement, and that customers are always asked if data may be used for purposes other than those defined at the beginning. For customers who don't want to answer each single question under the "Defaults" tab, Avantara defines settings-categories for data usage. The data usage allowance can be set on "Minimum" or "Maximum". Last but not least, Avantara gives customers the chance to define the intensity of advertisement. These predefinitions are visualized in Fig. 2.

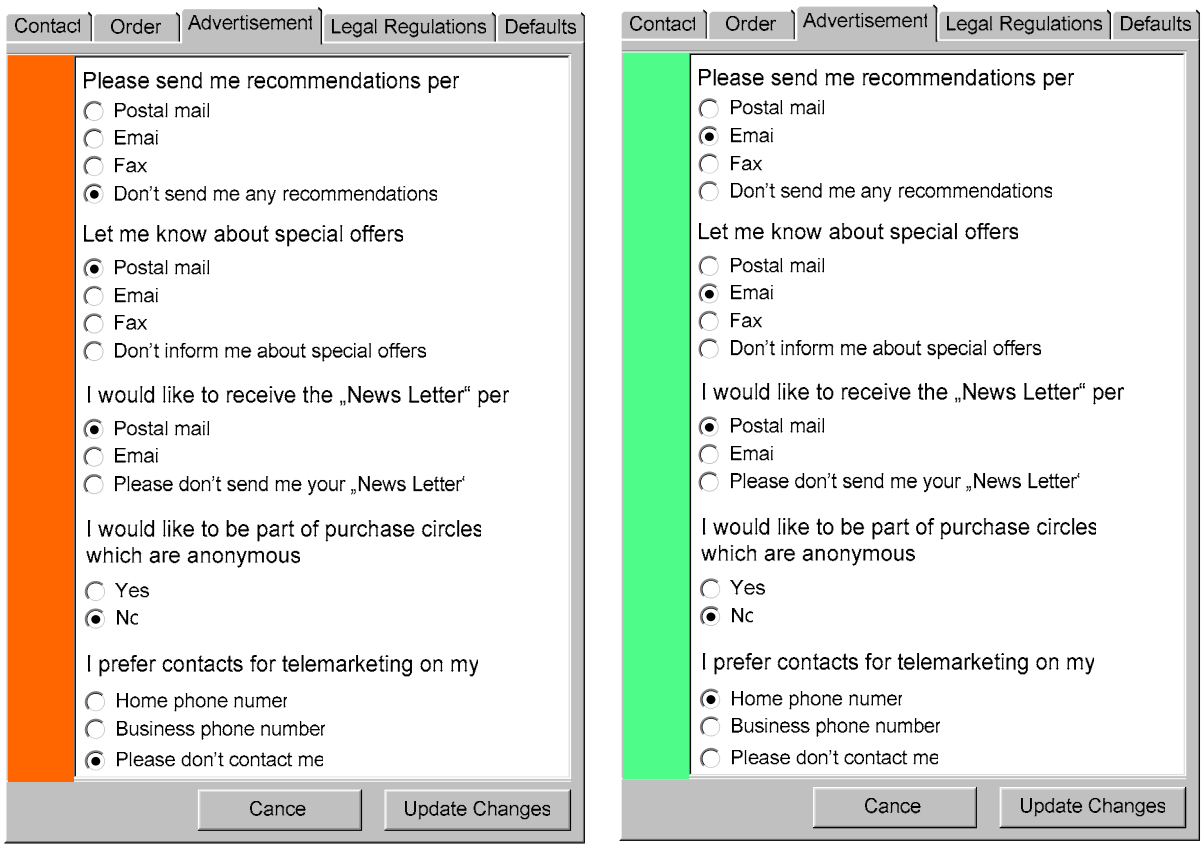

Fig. 2: Privacy Control Settings of Alice Privacy Control Settings of Bob

Alice and Bob (compare [Agrawal 2002]) are looking for a skilled online bookseller, whereby Avantara and Belios are short-listed. Alice is a privacy fundamentalist who normally doesn't want companies to retain any information once her purchase transaction is complete. However she is willing to commit her personal data in order to receive some specific information if she can be certain that her data will be handled confidentially and only for the chosen purposes. For this reason, Alice decides to buy her books at Avantara since there she has the best overview of her personal data usage. Bob, in contrast, is a privacy pragmatist. He appreciates the convenience of only having to provide his email and postal address once when registering with organizations. He likes to receive new recommendations, but does not want to be part of purchase circles. He also chooses Avantara but his reasons are different from Alice's. The different "Privacy Control Settings" of Alice and Bob are illustrated in Fig. 2.
Tent is Avantara's privacy officer. He is responsible that the information system complies with the company's privacy policies. Mallory is an employee and he has questionable ethics.

5.2 Architecture

Finally, we present the architecture of an autonomic database. Central to the design is the active participation of customers in providing specific information within the organizational systems.

5.2.1 Components

Customers Data Requestor is responsible for opening a communication channel to the Request Handling Agent, which is located on the Customers Data System side.
Request Handling Agent only accepts properly formulated requests from the corresponding Customer Data Requestor.
Privacy Settings Rule Model covers rules which determine for which purposes customers' personal data can be accessed. These rules are constituted in the Privacy Control Settings. Trent designs these privacy

definitions with regards to the company's privacy policy. For instance, he determines the purposes as to when a customer's email address can be used.

Rule Compliance Validator examines whether or not a personal data request complies with the Privacy Control Settings of each user.

Access Control takes care of accesses before and during query execution. Access Control is carried out on both the Business and Personal Data Identification System.

Query Intrusion Detection checks the accuracy of accesses after the queries by comparing the access with the usual access patterns for queries with that purpose and by that user. For example, Mallory decides to steal all email addresses of Avantara's registered users and to sell them to Avantara's competitors. Normally customers' email addresses can only be accessed for sending them recommendations or offers, or to enable order status tracking etc., as defined in the Privacy Settings Rule Model. Before the query results are returned, the Query Intrusion Detection matches these queries with the usual access patterns and detects the fraud.

Audit Trail records all possible queries for privacy audits and addresses challenges regarding compliance. Furthermore, this is where the customer's personal preferences as well as any changes to the Privacy Control Settings are maintained. Since customers have access to audit information, they are in a position to view all transactions and to detect any fraud.

5.2.2 Privacy Policy

Fig. 3 illustrates the separation of customers' personal and business data. The privacy policies of the two systems therefore differ in certain aspects, as explained in the following section.

5.2.2.1 Business Data System

Authorized users and applications of the Business Data System are specified in the privacy policy. These are the set of Avantara's employees and applications who, or respectively which, can access particular information. The anonymous business data is accessible for purposes such as data maintenance, data mining and data analysis. As a result of the data separation, Avantara doesn't require a customer's personal information for most data mining and analysis activities - that is, not until Avantara addresses its customers directly.

5.2.2.2 Personal Data Identification System

The privacy policy for the Personal Data Identification System is more sophisticated and consists of three main parts.

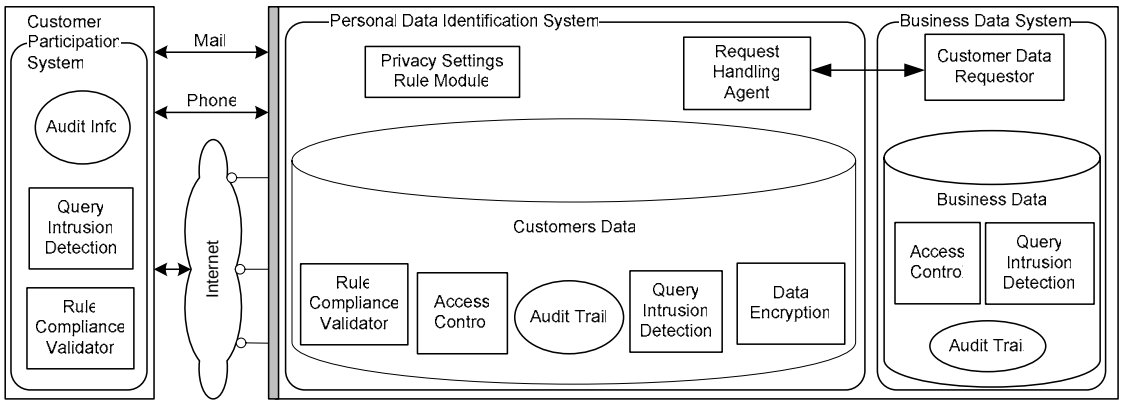

Fig. 3: Architecture

Authorized users This is a group of employees, customers and applications. Employees and applications access this data for maintenance purposes only. Customers, in comparison, access the Privacy Control Settings to assign their preferences and restrictions with regard to data usage. Moreover, customers access Audit Trail information to view and verify the suitability of the use of their personal data. Returning to our example case, Mallory is employed by Avantara to maintain customers' business data, therefore he has no authorization to access customers' personal data.

Rule Mechanism Privacy rules are defined in the Privacy Settings Rule Model. This model covers rules which determine the general purposes for which customers' personal data can be accessed. The Rule Compliance Validator checks customers' Privacy Control Settings to examine if specific accesses should be allowed.

Request / Reply Mechanism The only way of connecting anonymous business data to customers' personal data is via a communication channel between the Customer Data Requestor and the Request Handling Agent. The Customer Data Requestor asks for information from the Request Handling Agent, which handles these requests and sends back a reply verified by the rule mechanism.

5.3 Queries

Avantara decides to launch a new marketing promotion, and therefore selects 500 records from the Business Data, with the intention of sending these customers specific recommendations per post or per email. In order to do so, Avantara needs to access the Personal Data Identification System where customers' addresses are stored. The access from the Business Data System to the Customers Data System is only possible via a controlled channel. All queries for customers' personal data are first sent to the Customer Data Requestor. The Customers Data Requestor forwards these queries to the Request Handling Agent, which is located in the Personal Data Identification System. The Request Handling Agent passes all properly formulated queries it receives to the Rule Compliance Validator. The query for customers' postal or email addresses with the purpose "recommendation" was sent by an authorized employee at Avantara. The Rule Compliance Validator now checks, in accordance with the Privacy Settings Rule Model, if this query can be accepted. After the commit, customers' Privacy Control Settings are checked. Alice stipulated in her Privacy Control Settings that she doesn't want to receive any recommendation whilst Bob would like to be sent recommendations per email. Therefore only Bob's email address is sent back to the Customer Data Requestor.

Let's suppose that Alice unexpectedly receives a recommendation from Avantara, despite having told them that she doesn't want this. Since Alice has access to the Audit Info where all transactions are recorded, she can verify the permission of the received email and complain to Avantara about the mistreatment of her personal data.

6 New Challenges

Now we describe some interesting problems which we identified in our principles and design. This list is by no means complete; its purpose is to initiate discussions.

6.1 Consent

The cornerstone for ending heteronomic databases would be a new international data protection law, which requests the explicit consent of a person before personal data can be stored. Furthermore, the law stipulates that this person must have access to their data, to specify purposes and to control audit information.

Within this law, several questions are raised. There will be a certain amount of administrative work and it will not always be clear how to set the process up. For instance, the user must first give his / her consent, before his / her personal data is stored, and not the other way around. How can organizations which do not care about this law be identified? Are normal individuals qualified to handle their personal data or instead to instruct a company specialised for this purpose?

However - and this is a crucial point – at least a person knows which databases store information about him / her.

6.2 Purpose

At a first glance, purpose specification may appear easy. However selecting what kind of usage from personal data a person allows depends heavily on the way in which this can be achieved and how these usages can be presented and categorized. No one is willing to spend several minutes specifying purposes, therefore a low amount of fixed categorizations have to be defined in which each category includes several purpose

specifications. Then people can choose to make settings either only on the category level and / or for each purpose. The categorization must also be independent of the branch or industry. To set-up, define and become widely accepted, such a general categorization of purposes is essential and its development may be a tough task.

6.3 Separation

Business data and personal data are often already separated in large-sized companies. Different applications use these data. On the other hand, in small and middle-sized companies these data are normally stored together and are only used by one main application. A physical or logical separation is necessary according to the principle of separation. This makes any IT-architecture more complicated. In addition, the architecture has to be extended with a strong identification functionality. To increase trust and confidentiality, the 'Personal Data Identification System' (see Fig. 3) should be certified by a third party.

6.4 Audit

Generating audit trails that are in the hands of the people affected could provide a strong and powerful tool for protecting privacy. First of all, these audit trails can be investigated by the organizations themselves in order to detect internal misuse. Secondly, each person can scan these data and convince himself / herself in compliance with the audit trail of his / her personal data, or in the case of misuse, can place a complaint. Last but not least, a person can engage external software agents to monitor his / her audit information and to be automatically informed if a violation is detected. Within this scenario, three main questions arise. How can an individual set up his / her complaint and who will receive this message? What kind of competence or interest could such a 'compliance office' persecutes? What kind of consequences may occur for the principal offender? Furthermore, 'Rule Compliance Validator' agents activated by the customer represent several security and privacy risks, despite being convenient for the customer.

6.5 Participation

Participation requests a certain kind of connection to the control equipment of the purpose specification and audit information. This communication and requested identification must be secure. Misuse cannot be tolerated.

6.6 Ease of use

We propose a hybrid solution. Each person can decide how centralized he / she would like to treat his / her personal data. A centralized system is quicker and easier to handle but encompasses more privacy risks than a decentralized system; however they could both provide a higher level of security. A centralized system is a far more attractive target for illegal transactions, because full data profiles related to specific users are available. The system's structure should at least be digitally secured against possible misuse and should guarantee the respect of a citizen's privacy.

7 Closing remarks

Organizations collect large amounts of personal data about their customers. Even although they promise privacy to their customers by means of privacy statements, there is no methodology to enforce these promises throughout and across multiple organizations. This paper illustrates the way in which the abolition of heteronomic databases can be achieved; it also defines legal and organizational principles as well as technical privacy-enabled database management systems for increasing personal privacy. Inspired by Kant, we present a vision of a system that takes responsibility for the privacy of the data which it manages. Its comprehensive privacy-specific approach expresses how individuals regain control over their own personal data. From a user's point of view, this will incline towards 'autonomic database' systems. Our approach offers a realistic, practical and pragmatic solution for enhancing peoples' privacy, without hindering organizations' business.

8 References

[Agrawal 2002] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, Hippocratic databases, VLDB, 2002.
[Benson 2003] D. Benson, "Distributed identities: Managing privacy in pervasive computing," Explored Viewpoints, SRI Consulting Business Intelligence, 2003.
[Berthold 2001] O. Berthold, H. Federrath and S. Köpsel, "Web mixes: A system for anonymous and unobservable internet access," Designing privacy enhancing technologies. International workshop on design issues in anonymity and unobservability, H. Federrath (Editor), vol. 2009, Springer, 2001, 113-129.
[Burkert 1997] H. Burkert, "Privacy-enhancing technologies: Typology, critique, vision," Technology and privacy - the new landscape, P. Agre and M. Rotenberg (Editors), 1997.
[Camenisch 2001] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," Advances in cryptology - eurocrypt 2001, international conference on the theory and application of cryptographic techniques, innsbruck, proceedings, B. Pfitzmann (Editor), vol. 2045, Springer Verlag, Berlin, 2001, 93-118.
[Chaum 1981] D. L. Chaum, Untraceable electronic mail, return addresses and digital pseudonyms, Communications of the ACM 24 (1981), no. 2, 84-88.
[Chaum 1985] D. Chaum, Security without identification: Transaction systems to make big brother obsolete, Communications of the ACM 28 (1985), no. 10, 1030-1044.
[Covell 1998] P. Covell, S. Gordon, A. Hochberger, J. Kovacs, R. Krikorian and M. Schneck, Digital identity in cyberspace, Conference on Legal/Technical Architectures of Cyberspace, 1998.
[Ducatel 2001] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leitjen and J. C. Burgelman "Scenarios for ambient intelligence in 2010," IPTS Publications, 2001.
[Gabber 1997] E. Gabber and P. B. Gibbons, How to make personalized web browising simple, secure, and anonymous, First International Conferenceon Financial Cryptography, 1997, 17-32.
[Garfinkel 2001] S. Garfinkel, Database nation, the death of privacy in the 21st century, O'Reilly, 2001.
[Goldschlag 1999] D. Goldschlag, M. Reed and P. Syverson, Onion routing for anonymous and private internet communications, Communications of the ACM 42 (1999), no. 2.
[Gooley 2003] C. Gooley and T. Saponas, "Privacy issues of the aware home," Paper on the Georgia Tech Aware Home project, 2003.
[Gsmworld 2003] http://www.gsmworld.com/news/press_2003/press_25.shtml
[IMS 2003] "Identity management systems (IMS): Identification and comparison study," IPTS Publications, 2003.
[Jendricke 2003] . Jendricke, Sichere kommunikation zum schutz der privatsphäre durch identitätsmanagement, vol. Rhombos, Berlin, 2003.
[Karjoth 2003] G. Karjoth, M. Schunter and M. Widner, "Platform for enterprise privacy practices: Privacy-enabled management of customer data," Privacy enhancing technologies, R. Dingledine and P. Syverson (Editors), Springer, 2003.
[Köhntopp 2000] M. Köhntopp, "Generisches identitätsmanagement im endgerät," Gi workshop sicherheit und electronic commerce - wssec 2000', R. Grimm and A. Röhm (Editors), Köllen Verlag, Bonn, 2000.
[Lessig 1999] L. Lessig, Code and other laws of cyberspace, Basic Books, 1999.
[Maghiros 2003] I. Maghiros, C. Centeno and C. Rodríguez, "Security and privacy for the citizen in the post-september 11 digital age: A prospective overview," IPTS Publications, 2003.
[Marx 2001] G. T. Marx, Murky conceptual waters: The public and the private, Ethics and Information Technology **3** (2001), no. 3, 157-169.
[Mattern 2003] F. Mattern, "Ubiquitous computing: Scenarios for an informatized world," ETH Zurich, 2003.
[Pfitzmann 2001] A. Pfitzmann and M. Köhntopp, Anonymity, unobservability, and pseudonymity - a proposal for terminology, Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability, Springer-Verlag, 2001, 1-9.
[Registratiekamer 1995] T. N. Registratiekamer, "Privacy-enhancing technologies: The path to anonymity," vol. 2002, 1995.
[Reiter 1998] M. K. Reiter and A. D. Rubin, Crowds: Anonymity for web transactions., ACM Transactions on Information and System Security 1 (1998), no. 1, 66-92.
[Schneier 1999] B. Schneier, Communication of the ACM, **42** (1999), no. 8.
[Third Generation Partnership 1999] T. G. Partnership, "Technical specification group services and system aspects 3g security; security principles and objectives (3g ts 33.120 version 3.0.0)," 1999.
[Walters 2001] G. J. Walters, Privacy and security: An ethical analysis, ACM SIGCAS Computers and Society 31 (2001), no. 2.
[Warren 1890] S. Warren and L. Brandies, The right to privacy, Harvard Law Review **IV** (1890), no. 5.
[Warwick 2002] K. Warwick, "Identity and privacy issues raised by biomedical implants," IPTS Publications, 2002.
[Weiser 1991] M. Weiser, The computer of the 21st century, Scientific American (1991), 94-101.
[Westin 1967] A. F. Westin, Privacy and freedom, Atheneum, New York NY, 1967.