Marrying Transparency Tools with User-Controlled Identity Management

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein, Germany

Abstract. User-controlled identity management systems assist individuals in managing their private sphere. An individual's privacy can be supported by transparency on processing of personal data. After giving an overview on transparency properties as well as its relation to privacy and data protection regulation, this text introduces different transparency tools: Prior to an interaction, information on the interacting party should be made transparent. During the interaction, privacy policies have to be communicated. Afterwards, users should be helped in exercising their privacy rights such as, among others, the right to access own personal data. In addition information on security and privacy incidents provides complementary data for the user's perception of the level of privacy. Although transparency tools alone are no panacea for maintaining the private sphere, the combination of transparency tools and user-controlled identity management systems yields viable functionality to empower users to protect their privacy.

1 Introduction

The world we live in becomes more and more complex. This is also true for data protection:

- In former times, personal information on individuals, so-called data subjects, were stored in few central databases. It was pretty much clear who processed personal data.
- The current situation is characterized by storage of personal data in many centralized and decentralized databases from various organizations in all sectors, often processing the data in a globalized context. In particular in the digital world, users accidentally or intentionally disclose a huge amount of personal data to others. Most people have difficulties to track who is processing what personal data.
- In the emerging world, not only organizations store, possibly link and analyze personal data of individuals, but also peers, e.g., in their e-mail folders or via social networks. In ubiquitous computing, sensors and thereby data processing can be everywhere. Every user may turn into a fully equipped data processing entity for own personal data and for those from others. The computing power in the hand of users can be used to assist them in maintaining their privacy.

Please use the following format when citing this chapter:

Hansen, M., 2008, in IFIP International Federation for Information Processing, Volume 262; The Future of Identity in the Information Society; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci; (Boston: Springer), pp. 199–220.

The underlying challenge for privacy in a democratic information society is to prevent steep rugged power imbalances. In fact, society needs a fair balance of power (which is not equivalent with evenly distributed power). Transparency is a well-known necessary, yet not sufficient mechanism for achieving fair balances because it enables to discuss openly the power distribution [6]. Power balance is not only relevant on the societal or political level on a large scale, but also in each privacy-related transaction.

Since several years, in many areas of life there are increasing demands for transparency so that individuals are empowered to take appropriate action, cf. Table 1. While areas such as food, cosmetics or pharmaceuticals in industrialized countries have to comply with manifold regulations and standards concerning transparency, the current practice for handling personal data and privacy issues still seems to be underdeveloped.

Table 1: Trend towards transparency in various application areas

	Throughout processing	**For individuals**
Food	Coloring rotten meat; thaw checks for frozen food	Nutrition overview
Cosmetic care products	Tests	Indication of ingredients and important properties
Pharmaceuticals	Marking components; tests	Patient Information Leaflet
Personal data and privacy issues	Today: mainly internally handled	Today: partially via privacy policies

This text is organized as follows: Section 2 introduces identity management, focusing on the user's perspective. The next section concentrates on transparency and transparency tools, setting the scene by illustrating the scope when considering privacy-relevant issues as well as the legal background. Section 4 explains how user-controlled identity management can be enhanced by transparency tools. Further, Section 5 discusses limitations of transparency tools and ways to deal with them. Finally, Section 6 concludes the text and gives an outlook.

2 Identity Management

This section introduces the concept of partial identities and identity management. Taking the user's perspective, a focus is put on user-controlled and privacy-enhancing features of user-centric identity management. Important mechanisms of user-controlled identity management systems are outlined for the example of the project "PRIME – Privacy and Identity Management for Europe".

2.1 The manifold facets of identity

"Who are you?" the border guard asks me. It is a difficult question – it is probably not appropriate to inform him that I am a caring parent traveling without my kids, a person who seems to be creditworthy enough to get a loan to buy a house, an employee of a big company, a person open to new challenges, a jazz fan (in particular of Louis Armstrong's songs), a former resident of a quaint village near a national park who is now used to living in a big city, the best runner in the ninth grade at school, the treasurer of the district sports club, a lover of hot spicy meals. ... He interrupts my chain of thought: "Please show your ID. I need to see your passport." Sure, he is not interested in me as a person, but as – right now – an international traveler. He checks my citizenship as well as the validity of my passport and estimates the risk of me being a terrorist by looking at me and searching for my name in a database. "Okay, please proceed to the gate."

Indeed, the identity of an individual is a complex entity with many facets. In each situation only a subset of this complete identity is needed – in essence, a **partial identity** [11]. Individuals learn to manage their partial identities intuitively, telling others only what they are willing to disclose and separating contexts from each other where appropriate. Some people have nicknames which are only used within a specific scope: at the sports club or in their personal relationship, for example. It would be out of place to be called by that nickname in a business meeting. Nobody gets to know the complete identity of a person – instead, only specific partial identities can be perceived.

Digital representations of partial identities are data sets comprised of attributes and identifiers. In our information society, organizations and individuals are working with those digital partial identities in all areas of life. Identity management means managing various partial identities (usually denoted by identifiers such as pseudonyms), developing and choosing partial identities and pseudonyms appropriate to specific contexts, and administering identity attributes. Figure 1 illustrates some of the partial identities that an individual may employ in daily life.

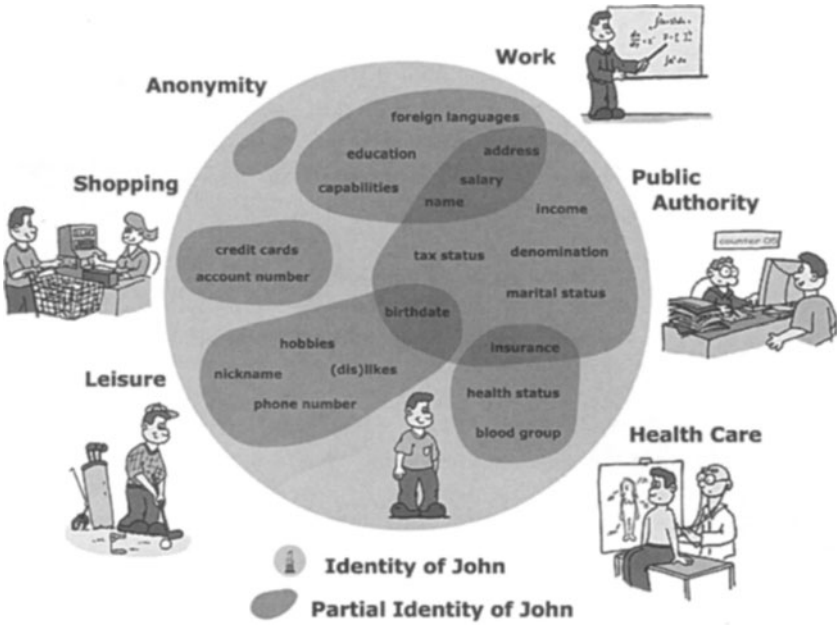

Fig. 1: John's partial identities (as shown in the PRIME tutorials [29])

2.2 Identity management: user-controlled and privacy-enhancing

Identity management is an overloaded term, associating various meanings. Starting from the notion of partial identities, "**identity management** means managing various partial identities (usually denoted by pseudonyms) of an individual, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role" [28].

From the service's perspective, account management systems and profiling systems are typical types of identity management [4].

Here we take the user's perspective and limit our view to **user-centric identity management** "that focuses on usability and cost effectiveness from the user's point of view" [21]. We highlight two main properties of user-centric identity management systems:

1. A **user-controlled** identity management system makes the flow of identity attributes explicit and gives its user a large degree of control [13]. The guiding principle is "notice and choice". These systems support users "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent that information is communicated to others" [31]. This is also the essence of the "right to informational self-determination" which stems from the ruling of the German Federal Constitutional Court on the 1983 census and demands that each person can at any time ascertain who knows what about him or her.

2. A **privacy-enhancing** identity management system aims at data minimization, in particular unlinkability [28]. Preservation of unlinkability can be achieved by choosing the pseudonyms (and their authorizations such as private credentials [8]) denoting the partial identities carefully, especially by keeping discrete contexts separate over the course of time.

The combination of these two properties yields **user-controlled privacy-enhancing identity management** which strives for user-controlled linkability of personal data, i.e., accomplishing control by the user based on thorough data minimization [28].

2.3 The prototype of PRIME – Privacy and Identity Management for Europe

The EU-funded FP6 project "PRIME – Privacy and Identity Management for Europe" aims at developing solutions for both user-controlled and privacy-enhancing identity management that supports individuals' sovereignty over their private sphere and enterprises' privacy-compliant data processing.

The guiding principle of PRIME is to put individuals in control of their personal data, based on three main components which are explained in the following subsections: pseudonyms and private credentials, enforcement of privacy policies, and a history function for transactions (cf. also [23]).

2.3.1 Pseudonyms and private credentials

In interactions with others, often the real name of a user is not required. Instead, distinct identifiers, i.e., pseudonyms, could be used to prevent undesired context-spanning linkage and profiling by unauthorized parties. Organizations can support this by skillful design of their workflows, separating different tasks – and the corresponding databases – from each other.

As a special feature, PRIME's approach uses "private credentials" which enable proving one's authorization (e.g., to be over 18 years old) without revealing information that may identify the individual [8]. These private credentials are derived from certificates issued on different pseudonyms of the same person. Multiple private credentials can be created from a single certificate that are neither linkable to each other nor to the issuance interaction in which the master certificate was obtained. Private credentials provide accountability combined with data minimization – only in the case of misuse the user's anonymity can be revoked.

2.3.2 Enforcing privacy policies at all times

For an organization, presenting a privacy policy on its website is usual practice. But providing privacy policies which are really understood by users and at the same time serve as rules for the automated data processing within the organization is a challenge tackled by the PRIME project. Its work encompasses both "before" and "after": the provision of privacy policies before a transaction takes place, e.g., in a stage when the user has to give consent to data processing, and after the transaction when the policy still sticks to the data disclosed. These so-called "sticky policies" enforce the rules

how the data may be processed even after they have been disclosed and thereby have left the user's area [22, 9].

2.3.3 Logging transactions in the "Data Track"

The right to informational self-determination demands the knowledge who knows what about oneself. This is supported by a history function of the user's online transactions. In principle this "Data Track" – as it is called within PRIME's Internet browsing prototype (cf. Figure 2) – stores in the user's trusted area which personal data the user has disclosed to whom at what time. Currently the "Data Track" is limited to structured information being disclosed, e.g., forms filled in or identifiers such as pseudonyms [27]. In addition to the personal information the conditions for the disclosure are being stored. This comprises also the privacy policy of a service requesting data. Further, it could cover additional obligations the service promises to fulfill. The "Data Track" helps to (re-)use the appropriate accounts – pseudonymous and passwords – in different contexts, keeping them apart unless otherwise desired.

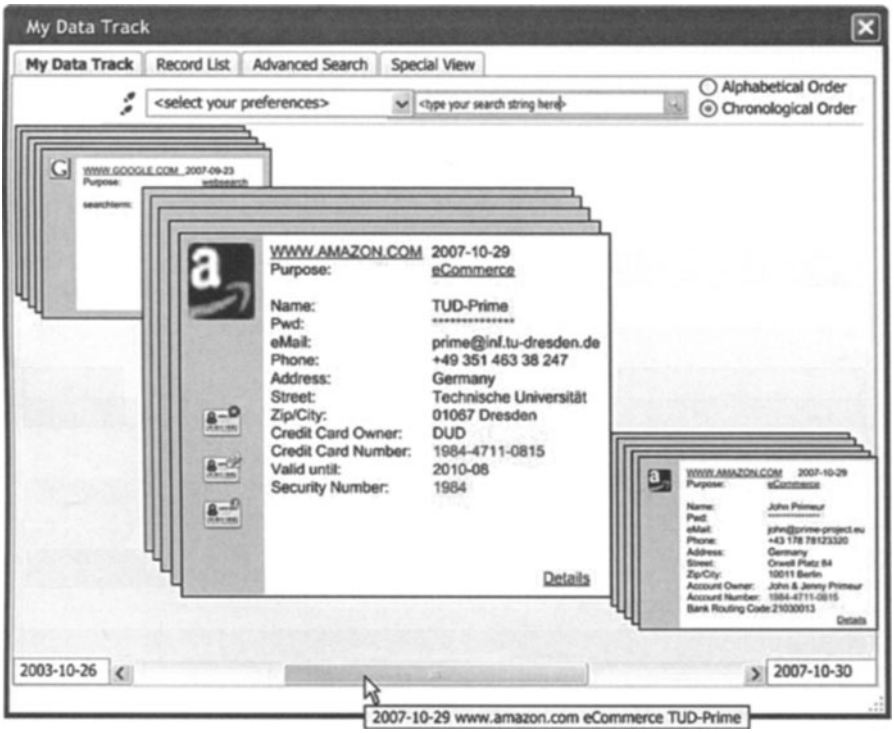

Fig. 2: The "Data Track" in the PRIME prototype

2.4 Other prototypes for user-controlled identity management

Various approaches have been studied for user-controlled identity management (beginning with [10]) and – at least partially – implemented in a prototype, e.g.,

"Dresden Identity Management (DRIM)" [12] focusing on role management, "iJournal" keeping track of transactions as part of MozPETs (Mozilla Privacy Enhancement Technologies) [7], "iManager" which is designed for mobile use via a PDA or mobile phone [20], and the "Personal Identity Assistant" for managing authorized access to user profiles [32].

As pointed out in [25], history functionality for logging transactions is an essential feature in DRIM, in the "iJournal" and – as presenting the most sophisticated concept – in the PRIME prototypes. For those user-controlled identity management systems without a history function, this transparency-enhancing feature could be added. As we will see later in Section 4.5, PRIME's "Data Track" plays a central role for integrating and orchestrating other transparency tools.

3 Transparency

In this section, basing on the definition of transparency different kinds of related tools are briefly introduced. The scope of transparency with respect to an individual's private sphere is illustrated. Finally the current legal baseline in the European Union for transparency issues with respect to privacy is outlined.

3.1 Defining transparency and transparency tools

Transparency is an ambiguous term: Especially in computing it depends on the context whether it should express that *all details* of a system or a process are being shown or on the contrary *none at all*. Indeed if transparency is meant to enhance understanding of a person, the amount of given information as well as the way of presenting it are important – if this is not performed appropriately, the level of understanding may even decrease, and in addition the person may even be demotivated to deal with the given information.

> ***Transparency***
> *From Wikipedia, the free encyclopedia (2007)*
> "Transparency is the property of allowing transmission of light through a material. It is the noun form of the word *transparent* (for example, glass is usually transparent.)
> Metaphorical meanings can amount to clear visibility, but also the opposite, invisibility (in particular of irrelevant details)."

When dealing with personal data and privacy, **transparency tools** are tools which can provide to the individual concerned clear visibility of aspects relevant to these data and the individual's privacy. This comprises, among others, the data flow, the privacy policy, actual methods of data processing, offered services, used software, reputation of interaction partners, guarantees of trustworthiness and security of all data processing and also all actual or possible vulnerabilities and security breaches.

The objective of transparency tools in this context is to empower users to act in an appropriate way on this information which requires understanding as well as the possibility to take action.

When discussing transparency tools, it has to be clear *what* should be *transparent* (or the other way round: *not transparent*) to *whom* [6]. Table 2 shows what a person typically favors considering transparency in the relation of oneself to others, distinguishing **transparency-supporting** and **transparency-preventing tools**. The presented dichotomy is shown from a personal perspective, not the perspective from society. In any case transparency and its inverse, opacity, are possible properties for personal data or actions of an individual (which should be opaque against unauthorized parties from the privacy point of view) as well as for data processing mechanisms used by the data controller (which should be transparent for data subjects concerned).

Table 2: Categorization of tools concerning their effect on transparency (based on [6])

	Supporting tools	**Preventing tools**
Favorable from the personal perspective	Tools that help *ME* see what *OTHERS* are up to	Tools that prevent *OTHERS* from seeing what *I* am up to
Unfavorable from the personal perspective	Tools that help *OTHERS* see what *I* am up to	Tools that prevent *ME* from seeing what *OTHERS* are up to

In the context of profiling – in particular in the "Ambient Intelligence world" – **transparency-enhancing technologies (TETs)** are being discussed:

"TETs (transparency enhancing technologies) anticipate profiles that may be applied to a particular data subject. This concerns personalized profiles as well as distributive or non-distributive group profiles, possibly constructed out of anonymous data. The point would be to have some idea of the selection mechanisms (application of profiles) that may be applied, allowing a person adequate anticipation. To be able to achieve this, the data subject needs access – in addition to his own personal data and a profiling / reporting tool – to additional external data sources, allowing some insight in the activities of the data controller. Based on this additional information the data subject could perform a kind of counterprofiling." [18]

We do not build our discussion on the concept of transparency-enhancing technologies defined in [18] because we consider it too focused on counterprofiling. On the one hand this approach seems too narrow compared with the various flavors of transparency mechanisms. On the other hand it is problematic to rely on counterprofiling on the user's side only because it can (probably) never give an accurate estimation of what the other parties can or will do with personal data being processed. In particular this is the case in a potentially "hostile" environment refusing to disclose information on data processing to the data subject [17].

3.2 The scope of transparency tools concerning privacy

According to [5] transparency is an important privacy principle: "The design principles should ensure that the individual may check at any desired moment regarding what personal data he/she has given to the data systems, with the possibility to peruse, supplement, alter and delete personal data. … Control empowers people to stipulate the information they project and who can get hold of it, while feedback informs people when and what information about them is being captured, and to whom it is being made available."

Transparency is not only an important prerequisite for the users' control over their private spheres. Also for enhancing trust in privacy-enhancing technologies, users should feel in control of the technologies concerning them, which can be achieved if procedures are transparent and reversible [1].

When discussing transparency of privacy issues, it is necessary to explore different stages of the typical workflow for observing, linking, and analyzing personal data, cf. Figure 3. This generic workflow illustrates different actors in different stages of the information gathering and linking process. This process can lead to decisions about, e.g., receptiveness to marketing information, creditworthiness, suitability for a specific job, or probability of contracting a particular disease in the next decade. The decisions made on the basis of these analyses may affect a group of people or a single individual.

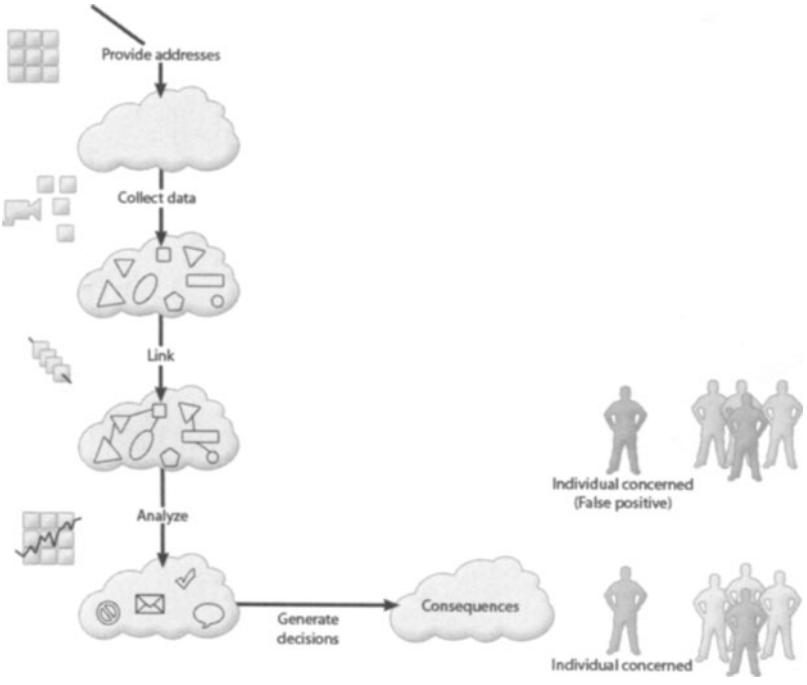

Fig. 3: Workflow of data enrichment influencing an individual's privacy [16]

As Figure 3 demonstrates, the individual whose information is processed is not necessarily well-equipped to either find errors in the case of wrong inferences or to ensure that corrective measures are applied [16]. Here, the power distribution obviously adversely affects the individual. Thus, considering the level of an individual's privacy, transparency would be needed in all these stages, about all data processing involved, about the responsible actors performing data processing, and about used algorithms and tools when enriching personal data. This would demand "transparency throughout processing" as well as "transparency for individuals" (cf. Table 1 in Section 1) and shows the wide scope of transparency tools.

3.3 Legal background on the EU level

The privacy principle of transparency of personal data processing is a key to informational self-determination. For this reason, the EU Data Protection Directive 95/46/EC guarantees individuals extensive information and access rights:

According to Art. 10 of the Directive, individuals from whom personal data will be collected have to be informed at least about the identity of the controller, the purposes of the data processing, and possible recipients or categories of recipients. In addition, a clear indication must be given as to how the individual can access additional information.

Under the terms of Art. 12 of Directive 95/46/EC, every individual has the right to access, i.e. the right to obtain from the controller a confirmation whether data relating to him are being processed and information at least as to the purposes of the processing, the data concerned, and possible recipients or categories of recipients. In addition, Art. 12 grants every individual the right to obtain from the controller the rectification, erasure, or blocking of data concerning him as far as the processing does not comply with the requirements of the Directive, in particular when the data at issue are incomplete or inaccurate.

Further, Art. 14 ensures that individuals are aware of the existence of the right to object, e.g., to processing of personal data for direct marketing.

In specific application contexts there may be other transparency and information obligations. Moreover there are proposals to change the EU electronic communications regulatory framework including improving transparency and publication of information for users and the introduction of security breach notification [19]. These recommendations are currently taken up in a proposal for amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on consumer protection cooperation.

4 Enhancing identity management by transparency tools

After having seen already the history function as one potentially integrated transparency tool for user-controlled identity management, this section explains four main areas of related transparency tools: information on interaction partners, understanding privacy policies, exercising privacy rights online, and a news feed on security and privacy incidents. Further, the orchestration of the described transparency functions is sketched.

4.1 Information on interaction partners

For users in the digital world, trustworthiness and reliability of potential interaction partners are important not only when commercial transactions take place, but also when other processing of personal data is involved. Having this information at hand, a user may decide beforehand not to interact with the other party at all.

In principle there can be two different sources for information on potentially interacting parties: the party itself or some third party, such as an organization, a peer or a group of peers. In most cases statements from the party itself will neither be considered impartial nor comprehensive, so only self-statements may be not sufficient to convince users that a party can be trusted. However, a big organization such as a company with long history, no known scandals and the aim of staying in the market may be considered trustworthy because of a famous and widely acknowledged brand. In addition, with cryptographic trusted computing chips servers may prove to the client that they fulfill certain security requirements and give guarantees for enforcement of policies.

In any case the judgment from third parties will also play a major role when estimating trustworthiness and reliability, in particular if those third parties are independent and avow for the party under consideration with their own name or base the judgment on transparent processes. Positive information statements on the data handling of an interacting party may be audit certificates, privacy seals or other trust marks which could be issued by a data protection authority (DPA)[1]. An example for a negative statement is the blacklisting of that party, such as the blacklist from the Swedish consumer protection organization Konsumentverket[2].

Further, reputation systems can be used which inform on experiences from peers with the party to interact with[3]. However, many reputation systems do not enable a reliable judgment because the descriptions of experiences from other peers may not be accurate – i.e., too positive or overcritical – and usually cannot be considered

[1] E.g., the established privacy seal "ULD-Datenschutz-Gütesiegel", https://www.datenschutzzentrum.de/guetesiegel/, or in the European context the project EuroPriSe, https://www.european-privacy-seal.eu/.

[2] "Svarta listan" from Konsumentverket Sweden, http://www.radron.se/templates/ blacklist____1936.asp.

[3] E.g., the reputation system used in eBay.

impartial. In addition, in most cases it cannot be excluded that the rating peers have been invented or bribed by the party itself.

4.2 Understanding privacy policies

Users are often not aware of their privacy rights [14]. But even if they are, it is not easy for them as lay people to understand privacy policies provided by services. There are different proposals to enhance the transparency of what is expressed in the privacy policy, as shown below.

The Article 29 Working Party has recommended a multi-layered format of privacy policies to improve the readability and focus on what users need in different steps to make decisions [2]. Further they propose to use language and layout that is easy to understand.

With development of P3P – Platform for Privacy Preferences[4], the World Wide Web Consortium aimed at machine-readability of privacy policies. This requires a harmonization of what can and should be expressed and how it should be interpreted. As a global harmonization of diverse privacy concepts is currently out of reach, the P3P vocabulary can only be a simplified compromise. Still even this less-than-ideal solution can help users understand privacy policies in foreign languages which have been expressed in P3P because their client can transform the machine syntax into their mother tongue. Further, parties such as data protection authorities could provide configuration files or wizards which express the national law both to users and service providers. If it turns out that the service does not work with a legally compliant configuration, users or supervisory authorities could make a complaint.

In a multimedia environment, a restriction to textual privacy policies seems to be old-fashioned and more difficult to grasp. In the complex world with information and communication technologies (ICT) we need short cuts for common concepts. The simplification as attempted in P3P could also be performed for audio- or video-enhanced privacy statements. In particular icons expressing data protection-relevant issues (as shown in Figure 4 [24, 30]) are currently under discussion.

[4] http://www.w3.org/P3P/.

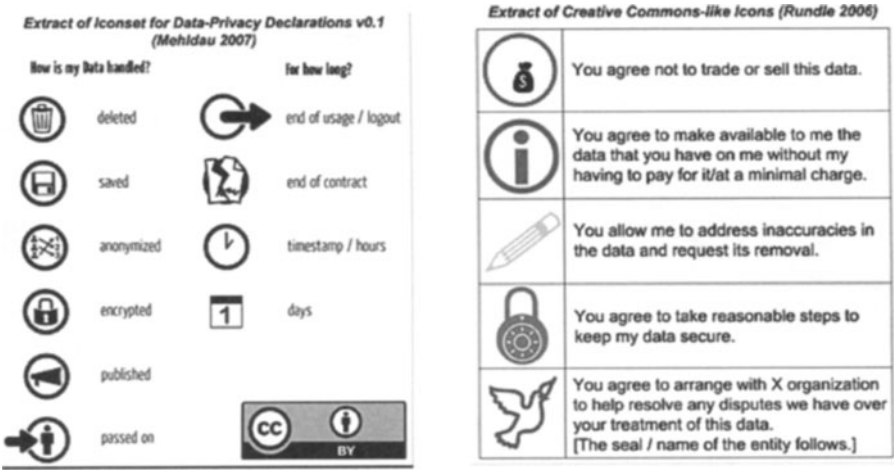

Fig. 4: Excerpts from proposed icon sets to express privacy statements (left: [24], right: [30])

4.3 Exercising privacy rights online

Whenever personal data of users are processed, they have specific rights in the European jurisdiction, as depicted in Section 3.3: Users have the right to request access to their personal data, rectification of inaccurate personal data and erasure of illegally stored data. In addition they can withdraw a formerly given consent.

Currently most services do not offer an interface to assert one's privacy rights online even if all other user communication takes place in digital networks. These days, providers usually offer users the possibility to access and correct data only for the benefit of the data controllers, e.g., to change the address after having moved. As a rule, users do not get online access to personal data processed by profiling, scoring or data mining systems.

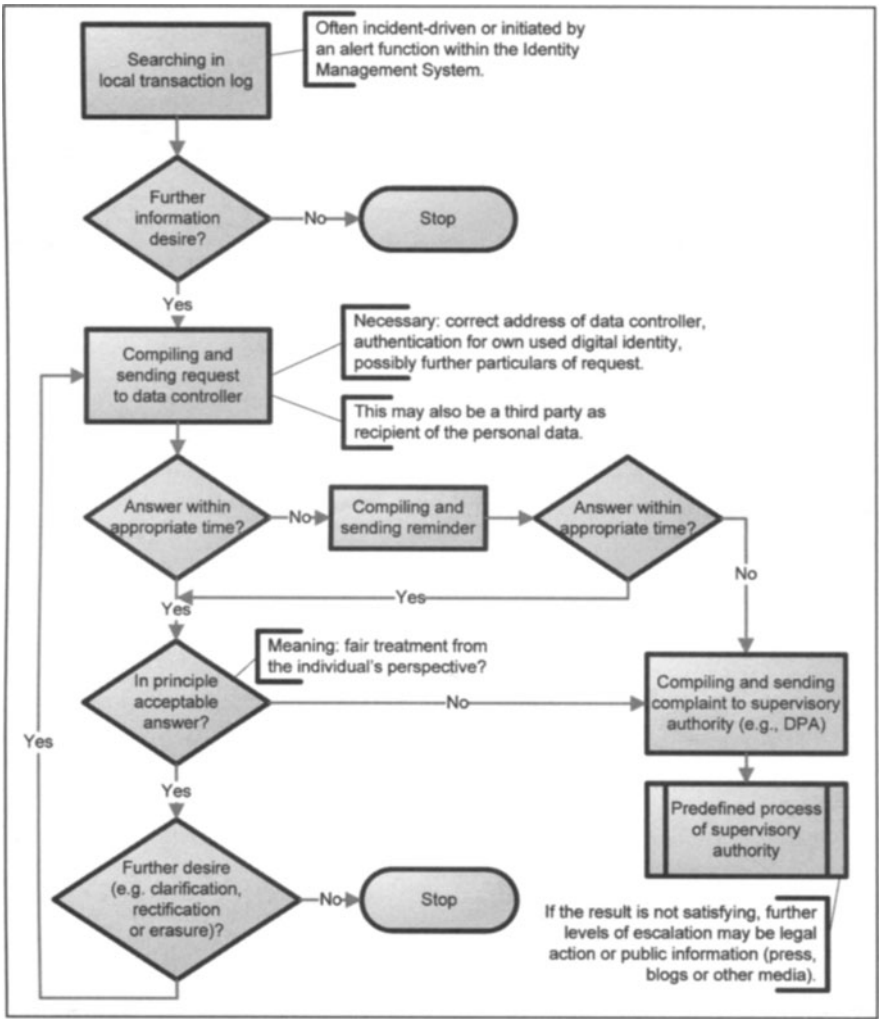

Fig. 5: Workflow for exercising privacy rights [15]

There are two ways to support users in exercising their rights: The service provider lowers the threshold for this by offering easy and convenient ways to access own data and request changes or erasure of data. Or the user gets tools which assist them to send requests to the data controller or – if necessary – complaints to a supervisory authority. An online function for requesting information related to one's personal data should help the user to specify all information needed for a data access request, which comprises:

- The contact address of the recipient.
- The personal data requested: Even though every individual has the right to request access to all information that can be linked to oneself, one might often only be interested in data that were released or collected about oneself in a

specific context. Hence, the online function should help the user to specify that context, which might also make it easier for the service's side to retrieve the data in its databases. If a user has released data under a certain pseudonym, a proof has to be given that the requesting user is actually the right holder of this pseudonym.

Additional information revealed by the request should be minimized; e.g., if the user's e-mail address has not been released yet, the user may choose another channel instead of e-mail communication or make use of one-time e-mail addresses or other anonymizing services.

The flow chart in Figure 5 gives an overview of essential steps to be taken into account when implementing an assisting function [15]. If the data controller offers a direct interface instead of posting letters, the process may be run through much faster. If no or only an incomplete answer is received from the service's side, a reminder process should start which may end in compiling a complaint mail to be sent to the supervisory authority in charge.

Meanwhile some public services, in particular citizen portals as gateway to the public sector, consider offering online access for citizens. In a few countries it is already possible for citizens to see their own profile data from the national register file, including the logfile containing who has accessed their data (except for law enforcement and other security agencies). This is implemented in, e.g., Belgium ("mijndossier/mondossier"[5]) and Norway ("minside"[6]), and a kind of "transparency portal" is planned in Germany as well[7].

4.4 News feed on security and privacy incidents

The user's privacy depends on security and data protection guarantees for all ICT systems involved in processing the user's personal data as well as organizational processes. This means that especially all information on security and privacy threats or incidents concerning the user's data is relevant. This comprises all mechanisms and implementations in use such as protocols, applications, cryptographic algorithms, or also the identity management system software itself. In particular users have to be informed about the risk to their private sphere, i.e., who definitely or potentially has unauthorized access to personal data, and about the consequences, e.g., options to take action.

In case of security breaches, transparency is legally demanded by Security Breach Notification Acts in several jurisdictions, in particular in the USA. Here any business that releases accidentally or otherwise personal information of any resident must

[5] https://www.mijndossier.rrn.fgov.be / https://www.mondossier.rrn.fgov.be / https://www.meindossier. rrn.fgov.be.

[6] http://www.norge.no/minside/.

[7] Information from the German Federal Ministry of the Interior, 16 March 2007: "IT-Projekte im Überblick: Bundesmelderegister" and the presentation from M. Schallbruch on 19 March 2007: "Das Deutschland Online-Vorhaben – Meldewesen", both available via http://www.deutschland-online.de/.

disclose such within a reasonable period. The intention of this obligation to notify residents is to ensure they are made aware when their data is received by unauthorized persons.

Today, security breaches and vulnerabilities are reported by a variety of providers, such as national Computer Emergency Response Teams (CERTs) or manufacturers of security tools. As in many cases vulnerabilities are only announced when there is already a patch available (which means that a certain percentage of vulnerabilities remains unreported), services such as VulnWatch inform on all threats submitted by security researchers or product vendors to alert the Internet community of security issues that may effect them[8].

Currently, comparable information in the area of privacy risks, e.g., relating to what can be observed or linked by others, is not available, or at least not in a structured way. This kind of information comprises, among others, the possible linkage of personal information by joining two formerly separated databases (e.g., if one company takes over another company), the possible linkage with other (publicly) available data, or the possible analysis of personal data according to other (publicly) available rules or knowledge (cf. Figure 3 in Section 3.2).

Feeding information on security and privacy threats or incidents directly into an identity management system can support the user to take action related to, e.g., configuring the system beforehand, administering the partial identities, using the identity management system within a transaction, or asserting privacy rights afterwards. The potentially presented options for users' activities comprise, e.g.,

- "Don't use that partial identity anymore."
- "Don't establish further communications or perform further transactions concerning this mechanism / party."
- "Patch the system (the identity management system itself or the environment, e.g., operating system)."
- "Don't use mechanism <mechanism_name> anymore."
- "Tag related transactions in the history logfile that there may has happened an incident (if possible: describe consequences)."
- "Assert right to access to own personal data or information on the data processing ICT system with respect to party <party_name>."
- "Assert right to delete personal data."
- "Revoke consent."
- "Inform peers."

In a prototype for PRIME, an RSS feed was designed to transport information on security incidents [26]. This feed is regularly polled by the user's system. For convenience reasons related warnings are grouped, and priorities assigned to the feed items are evaluated together with the user's estimation of reliability of the respective feed provider (i.e., a "trust level" "low", "medium" or "high", cf. Figure 6).

[8] http://www.vulnwatch.org/.

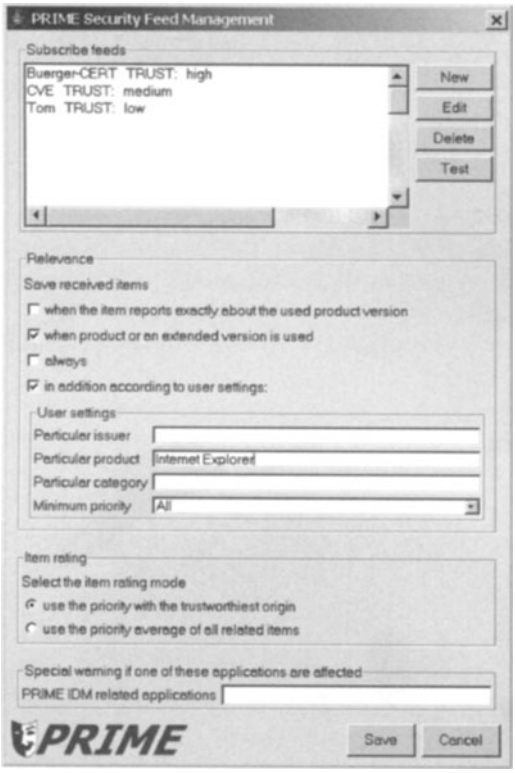

Fig. 6: Security feed in a PRIME prototype

The news items are formatted in XML, containing among others data on

- Product concerned (incl. version) and its issuer;
- Description of the vulnerability (incl. priority), since when it exists and the date of its detection;
- Recommendation for action (e.g., countermeasures or specific checks) with information on the effectiveness of the proposed solution;
- Digital signature for authenticity check.

For a wide use and the possibility of machine interpretation, e.g., by identity management systems, the format of news items and the way for interpretation by the user's system should be standardized. This is especially important when extending the information scope to data protection issues, leaving the traditional area of security vulnerabilities from CERTs and others which already base on structured formats.

4.5 "Data Track" as control center

The transparency tools showed in the previous sections can be used within any ICT system, but they are especially interesting in combination with a user-controlled identity management system.

In PRIME the main control center which can orchestrate the different transparency tools is the "Data Track" (cf. Section 2.3.3) together with the function to check which personal data to disclose in a specific context. Here the information on potential interaction partners and the privacy policy information can be shown even prior to the interaction or any disclosure of personal data. In addition, the "Data Track" would not only serve as a history function for user-side logging of data transaction records, but also would enable users to ask data controllers later on whether they really treated the data as promised. Moreover, information from security and privacy news feeds which is relevant for the user could be stored at the user's side and displayed when the user is going to disclose personal data. This information is also valuable for investigating potential risks related to former transactions in the "Data Track".

5 Limitations of transparency tools

The value of transparency tools depends on how accurate, comprehensive and understandable the information is. Obviously this is a challenge especially in a hostile environment where the reliability of available information is questionable and where adversaries would not make attacks transparent. In particular breaches of confidentiality can hardly be noticed. Hidden spying technologies are meanwhile available for everybody [16]. Partial remedy can be achieved by integrating findings of third parties or other peers on possible surveillance, linkage or profiling. People should be able to choose from a plurality of information providers whom to trust that they offer reliable information.

Without standardization, information being made transparent often is hard to understand for humans and cannot easily be interpreted by machines. In a globalized world this would require hard-to-achieve international harmonization, at least with respect to important aspects. Again, peers or organizations trusted by the individual can be of help when deciding on proper actions.

Providing transparency by offering information bears a great responsibility as inaccurate information may be harmful. In particular if news feeds for security and privacy information are automatically interpreted, rumors may lead to build-up processes with undesired consequences which are hard to revoke. Related are liability issues.

Transparency is not sufficient for achieving a high level of privacy: Giving all necessary information to individuals does not mean that they have a real and fair choice to maintain their privacy. In fact, data minimization with minimal disclosure of personal data is usually more effective than relying on "notice and choice". Also transparent privacy-invasive processes are still privacy-invasive. In this case, people concerned should be empowered to complain via other ways, as offered by today's democratic state mechanisms, e.g., informing supervisory authorities, bringing the case to court, or using political influence.

Further, transparency tools may be privacy-invasive themselves, in particular when they require to process personal data themselves. This is especially true if personal data from others are involved. But also a huge storage of own personal

information is a risk as it represents yet another data silo which would have to be safeguarded against unauthorized access.

Finally, companies may not be willing to provide more information and enhance transparency because they would have to reorganize internal processes. In addition, this information would have to be kept apart from potential trade secrets or personal data from others. However, the people interested in transparency may be an own customer segment which could be attracted. Here it should be taken into account that according to a study, consumers who desire greater information transparency are less willing to be profiled, i.e., the demand for transparency and the need of privacy seem to be correlated [3].

6 Conclusion and outlook

In many areas of life in our increasingly complex world there is a trend towards transparency. Similar approaches are needed for privacy-related issues as well. Transparency is a precondition for an informed decision on aspects related with processing of personal data, e.g., which data to disclose, which data processing methods to allow and which additional conditions to demand. Not only in the European regulatory context it is legally required to offer data subjects transparency on processing of their personal data.

As user-controlled identity management systems assist individuals to manage their privacy, they can function as a perfect basis for transparency tools which pursue the same objective. In particular this means giving information to individuals in an understandable way and empowering them to act accordingly.

Transparency tools can enhance user-controlled identity management in many facets. Users can profit from their use at all times: before an interaction when checking the other party's trustworthiness and reliability, during an interaction when policies are being displayed and consent has to be given, and also after an interaction to control. The information can either be displayed directly on the spot or asynchronously, depending on the context.

Transparency can help users to get an idea which knowledge on the own person other parties may have gained. This is important to support them in determining (re-) use of partial identities, taking into account, e.g., the assumed or stated trustworthiness of the service and its already compiled knowledge. Moreover, it may provide information for deciding whether and how to act after data have been disclosed.

However, transparency tools are no panacea for achieving a high level of privacy. As a matter of fact, they may convey privacy problems, e.g., if the information to be made transparent to an individual belongs to other persons. Even in workflows which separate data from different persons, sometimes intermingling of multiple data subjects' personal data cannot be fully excluded, e.g., in interactions between natural persons or in reputation systems which base on linking ratings from others on former interactions.

Implementing transparency tools bears several challenges. In particular it is challenging to provide understandable information, not too little and not too much, otherwise individuals will be overwhelmed by the complexity of data processing and privacy. Also, precaution should be taken that individuals neither overestimate nor underestimate security and privacy risks. Further, if transparency information is sensitive itself, it is a challenge to protect these data silos which are set up for transparency purposes against unauthorized access.

The "marriage" of transparency tools with user-controlled identity management can result in a full "privacy suit" for users, providing only one user interface and gateway to the outside world. We do not have to start from scratch – information and services out there can be integrated to a certain extent. Standardization and harmonization of transparency tools and their interpretation is needed so that transparency-enhanced user-controlled identity management can come into full blossom – provided that interaction partners and parties within the infrastructure are also able and willing to support both identity management and transparency demands. For the sake of privacy and sovereignty of every user, transparency tools should be implemented on top of data minimizing functions and be combined with possibilities for users to track back data processing involving multiple parties to be able to find errors in the case of wrong inferences and to ensure that all necessary corrective measures are applied.

Thereby increased transparency will enable a further societal discussion on how to shape privacy and data processing on individuals in our information society, aiming at a fair power balance between individuals, companies and States.

Acknowledgments

This work was partially done within the context of two European research projects: the Network of Excellence FIDIS – Future of Identity in the Information Society (http://www.fidis.net/) which works among others on identity, identity management and transparency enhancing tools and the Integrated Project PRIME – Privacy and Identity Management for Europe (https://www.prime-project.eu/) where concepts and prototypes for user-controlled identity management are being developed. I am grateful for helpful comments on this topic and related issues from and constructive discussions with Mike Bergmann, Laurent Beslay, Katrin Borcea-Pfitzmann, Caspar Bowden, David Brin, Sebastian Clauß, Stephen Crane, Simone Fischer-Hübner, Riccardo Genghini, Markus Hansen, Mireille Hildebrandt, Xavier Huysmans, Katja Liesebach, Christian Krause, Holger Krekel, Martin Meints, Sebastian Meissner, Jan Möller, Antje Nageler, John Sören Pettersson, Andreas Pfitzmann, Stefanie Poetzsch, Thomas Probst, Hartmut Pohl, Charles Raab, Maren Raguse, Martin Rost, Jan Schallaböck, Sandra Steinbrecher, and Stefan Weiss. The FIDIS Network of Excellence and the PRIME project receive research funding from the European Union's Sixth Framework Programme and the Swiss Federal Office for Education and Science.

References

1. Andersson C, Camenisch J, Crane S, Fischer-Hübner S, Leenes R, Pearson S, Pettersson, JS, Sommer, D (2005) Trust in PRIME. In: Proceedings of the 5th IEEE Int. Symposium on Signal Processing and Information Technology. Athens, Greece, 552-559
2. Article 29 Working Party (2004) Opinion on More Harmonised Information Provisions. WP 100, 11987/04/EN. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf. Accessed 2 Dec 2007
3. Awad, NF, Krishnan, MS (2006) The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Quarterly 30 (1): 13-28
4. Bauer M, Meints M, Hansen M (eds) (2005) Structured Overview on Prototypes and Concepts of Identity Management Systems. FIDIS Deliverable D3.1. Frankfurt am Main, Germany. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf. Accessed 2 Dec 2007
5. Borking JJ, Raab CD (2001) Law, PETs and Other Technologies for Privacy Protection. In: Journal of Information, Law and Technology, Vol. 1. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking. Accessed 2 Dec 2007
6. Brin D (1998) The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? Addison-Wesley, Reading, Mass.
7. Brückner L, Voss M (2005) MozPETs – a Privacy Enhanced Web Browser. In: Proceedings of the Third Annual Conference on Privacy, Security and Trust (PST05), Canada. http://www.ito.tu-darmstadt.de/publs/pdf/BrueckнerVoss_Mozpets.pdf. Accessed 2 Dec 2007
8. Camenisch J, Lysyanskaya A (2000) Efficient Non-Transferable Anonymous Multi-Show Credential System With Optional Anonymity Revocation. IBM Research Report RZ 3295 (# 93341), extended abstract in: Advances in Cryptology – Eurocrypt 2001, revised full version available at http://eprint.iacr.org/2001/019. Accessed 2 Dec 2007
9. Casassa Mont M, Pearson S, Bramhall P (2003) Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. Trusted Systems Laboratory, HP Laboratories Bristol, HPL-2003-49. http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf. Accessed 2 Dec 2007
10. Chaum D (1985) Security without Identification: Transaction Systems to Make Big Brother Obsolete. CACM 28 (10): 1030-1044
11. Clauß S, Köhntopp M (2001) Identity Management and Its Support of Multilateral Security. Computer Networks, 37 (2): 205-219
12. Clauß S, Kriegelstein K (2003) Datenschutzfreundliches Identitätsmanagement. Datenschutz und Datensicherheit 27 (5): 297
13. Clauß S, Pfitzmann A, Hansen M, Van Herreweghen E (2002) Privacy-Enhancing Identity Management. The IPTS Report 67: 8-16. http://www.jrc.es/home/report/english/articles/vol67/IPT2E676.htm. Accessed 2 Dec 2007
14. Eurobarometer (2003) Data Protection. http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_data_protection.pdf. Accessed 2 Dec 2007
15. Fischer-Hübner S, Pettersson JS, Bergmann M, Hansen M, Pearson S, Casassa Mont M (2007) HCI Designs for Privacy-Enhancing Identity Management. In: Acquisti A, Gritzalis S, Lambrinoudakis C, Di Vimercati S (eds) Digital Privacy: Theory, Technologies, and Practices, Auerbach, in press

16. Hansen M, Meissner S (eds) (2007) Verkettung digitaler Identitäten. Report commissioned by the German Federal Ministry of Education and Research. https://www.datenschutzzentrum.de/projekte/verkettung/. Accessed 2 Dec 2007
17. Hildebrandt M, Koops B-J (eds) (2007) A Vision of Ambient Law. FIDIS Deliverable D7.9. Frankfurt am Main, Germany. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf. Accessed 2 Dec 2007
18. Hildebrandt M, Meints M (eds) (2006) RFID, Profiling, and AmI. FIDIS Deliverable D7.7. Frankfurt am Main, Germany. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf. Accessed 2 Dec 2007
19. Hogan & Hartson, Analysys (2006) Preparing the Next Steps in Regulation of Electronic Communications – A Contribution to the Review of the Electronic Communications Regulatory Framework. http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/next_steps/regul_of_ecomm_july2006_final.pdf. Accessed 2 Dec 2007
20. Jendricke U, Gerd tom Markotten D (2000) Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet. In: Proceedings of the 16th Annual Computer Security Applications Conference, 344-353
21. Jøsang A, Pope S (2005) User Centric Identity Management. In: Proceedings of AusCERT, Australia. http://sky.fit.qut.edu.au/~josang/papers/JP2005-AusCERT.pdf. Accessed 2 Dec 2007
22. Karjoth G, Schunter M, Waidner M (2002) Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. In: Proceedings of 2nd Workshop on Privacy Enhancing Technologies (PET 2002), LNCS 2482, Springer, 69-84
23. Leenes R, Schallaböck J, Hansen M (eds) (2007) Privacy and Identity Management for Europe – PRIME White Paper V2. https://www.prime-project.eu/prime_products/whitepaper/. Accessed 2 Dec 2007
24. Mehldau M (2007) Iconset for Data-Privacy Declarations v0.1. http://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf. Accessed 2 Dec 2007
25. Meints M (2006) Protokollierung bei Identitätsmanagementsystemen – Anforderungen und Lösungsansätze. Datenschutz und Datensicherheit 30 (5): 304-307
26. Nageler A (2006) Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem. Diploma Thesis, Christian-Albrechts-Universität zu Kiel
27. Pettersson JS, Fischer-Hübner S, Bergmann M (2006) Outlining "Data Track": Privacy-Friendly Data Maintenance for End-Users. In: Advances in Information Systems Development – New Methods and Practice for the Networked Society, Proceedings of the 15th International Conference on Information Systems Development (ISD 2006), Springer US, 215-226
28. Pfitzmann A, Hansen M (2007) Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology v0.30. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Accessed 2 Dec 2007
29. PRIME Tutorials (2007). https://www.prime-project.eu/tutorials/. Accessed 2 Dec 2007
30. Rundle M (2006) International Data Protection and Digital Identity Management Tools. Presentation at Internet Governance Forum 2006, October 2006, Athens. http://identityproject.lse.ac.uk/mary.pdf. Accessed 2 Dec 2007
31. Westin AF (1967) Privacy and Freedom. Atheneum, New York
32. Wörndl W (2003) Privatheit bei dezentraler Verwaltung von Benutzerprofilen (Privacy in Decentral Management of User Profiles). PhD Thesis at Technische Universität München. http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2003/woerndl.pdf. Accessed 2 Dec 2007