Making PRIME Usable

John Sören Pettersson
Simone Fischer-Hübner
Ninni Danielsson
Jenny Nilsson
Karlstad University
651 88 Karlstad, Sweden
{john_soren.pettersson,
simone.fischer-huebner,
ninni.danielsson}@kau.se

Mike Bergmann
Sebastian Clauss
Thomas Kriegelstein
TU Dresden
010 62 Dresden, Germany
{mb41, sc2, tk4 }@ inf.tu-dresden.de

Henry Krasemann
Independent Centre for Privacy
Protection (ICPP)
24103 Kiel, Germany

ld101@datenschutzzentrum.de

ABSTRACT
Privacy-enhanced Identity Management can enable users to retain and maintain informational self-determination in our networked society. This paper describes the usability research work that has been done within the first year of the European Union project on "Privacy and Identity Management for Europe" (PRIME). It primarily discusses and compares three alternative UI paradigms for privacy-enhanced Identity Management, and presents how important legal privacy principles derived from the European Union Directives have been mapped into suggestions of user interface solutions for PRIME. Besides, it discusses results and encountered problems from conducted usability tests on mock-ups implementing the different UI paradigms and proposes means for addressing those problems. The paper concludes with remarks on the characteristics of usability work for privacy-enhancing technologies.

Categories and Subject Descriptors
H.5.2 [**Information Interfaces and presentation**]: User Interfaces – *evaluation/methodology, interaction styles*

General Terms
Security, Human Factors, Legal Aspects.

Keywords
HCI, Privacy-Enhancing Technologies, Identity Management

1. INTRODUCTION
In today's information society, users have lost effective control over their personal spheres. The promotion of Ambient Intelligence applications, where individuals are mostly unaware of a constant data collection and processing in their surroundings, will even sharpen this problem. It is however critical to our society and to democracy to retain and maintain individual's autonomy and thus to protect privacy and particularly the individual's right to informational self-determination. Powerful tools for technically enforcing user control and informational self-determination as well as pseudonymity and anonymity can be provided by privacy-enhanced Identity Management systems, as currently developed within the EU FP6 integrated project PRIME ("Privacy and Identity Management for Europe"[1]). However, PRIME technologies will only be successful if they are accepted and applied by the end users. For this reason, the PRIME project has also put an emphasis on human-computer interaction (HCI) research on new user interface (UI) solutions and paradigms for privacy-enhancing identity management. This paper will present the first results from the PRIME HCI research activity. It will first present the aims and scope of the PRIME project and related work, on which we have partly based our research for PRIME UI solutions. It will then discuss paradigms for privacy-enhanced Identity Management (IDM) control elaborated within PRIME and furthermore the mapping of related legal privacy principles to specific design solutions for HCI. Some pertinent results from usability evaluations are reported. Finally we reflect on characteristics of usability work within the IDM sphere.

Symposium On Usable Privacy and Security (SOUPS) 2005, July 6-8, 2005, Pittsburgh, PA, USA.

2. PRIME – AIMS AND SCOPE
The PRIME project can be described and motivated as follows: In everyday life, individuals are frequently and naturally playing different roles, for example as family members, citizens or patients, and are participating in different communication relations. Typically, when individuals are performing a certain role or are participating in a certain communication relationship, they do not reveal all personal data about themselves but only parts of their personal data (i.e. parts of their identities). Hence, each role or communication relationship could be associated with a partial identity of this person. For example in Figure 1, Alice reveals different partial identities to different communication partners. In the non-electronic world, individuals naturally had control over the releases of partial identities to other parties. In our modern age of electronic communication, an Identity Management System can help the user to manage all her/his partial identities, i.e. depending on the user's current role or communication partner, the Identity Management System supports the user to control what personal information about him is revealed to others.

Identity Management subsumes all functionalities that support the use of multiple identities by the identity owner (user-side IDM) and by those parties with whom the owner interact (services-side IDM). The PRIME project addresses privacy-enhancing IDM to support strong privacy by particularly avoiding or reducing

[1] http://www.prime-project.eu.org/

identification and by technically enforcing informational self-determination.

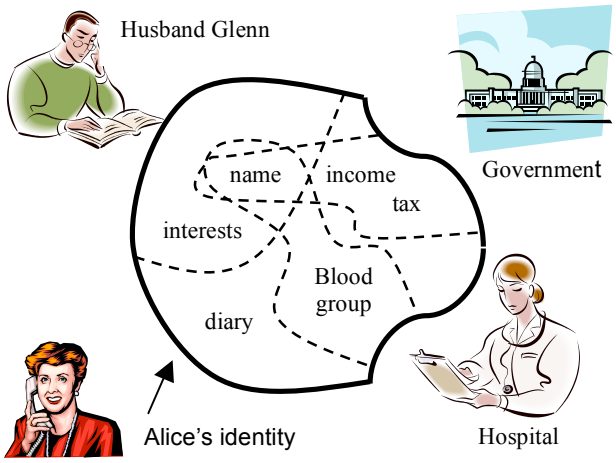

Figure 1. Partial identities of a person for different roles and relationships.

PRIME is based on the principle that design must start from maximum privacy. This means that a priori all interactions are anonymous, and individuals can chose pseudonyms to link different interactions to each other, bind attributes and capabilities to pseudonyms and can establish end-to-end secure channels between pseudonyms. Whether or not interactions are linked to each other or to a certain pseudonym is under the individual's control. Hence, PRIME tools that are developed allow individuals to act under different pseudonyms with respect to communication partners, roles or activities and at the same time provide them control over the release of their personal data including transparency about who has received what personal data related to them and possibilities to trace personal data being passed on. Besides, PRIME tools include policy handling and management tools helping them to define who has the right to do what with one's personal data under which circumstances, online functions for exercising their rights to object to data processing or to rectify, block, delete data as well as tools allowing them to define and switch identities, pseudonyms and related profiles.

3. RELATED WORK

Some previous work has been done in the area of usability and privacy, especially on user perception and trust issues, UI paradigms for Privacy-Enhancing Technologies (PETs), usability of security systems, the mapping of legal privacy requirements to HCI requirements, privacy UI vocabularies and information structuring (see discussion on related work in [15]).

In the following subsections, we briefly summarize some research results of the EU FP5 PISA ("Privacy Incorporated Software Agent") project [12][13] and recommendations of the Art. 29 Working Party concerning the content and structuring of information to be provided to users [1], which we used as a basis for our HCI design proposals and research in the PRIME project.

3.1 The PISA Project

Important domain-specific HCI requirements can be derived from privacy legislation. In the PISA project, it has been studied in detail how privacy principles derived from the EU Data Protection Directive 95/46/EC [5] can be translated into HCI requirements and what are possible design solutions to meet those requirements [12][13]. The derived HCI requirements were grouped into the four categories comprehension (to understand, or know), consciousness (be aware or informed), control (to manipulate, or be empowered) and consent (to agree).

In the PRIME project, we have used these privacy principles and HCI requirements from the PISA project to derive proposed UI design solutions for PRIME. In addition we have added further legal privacy principles that were not considered or not analyzed in detail in the PISA project, for which we also derived HCI requirements and proposed UI solutions. These additional privacy principles were derived from the EU Directive 2002/58/EC [4] on privacy and electronic communications and from Art. 25-26 of the general EU Data Protection Directive 95/46/EC regulating the data transfers to sites in countries outside the European Union with no appropriate level of data protection.

The PISA project also investigated user agreements for obtaining informed user consent. The common method of "click-through agreements" were users must click on a text expressing agreement to get the software or service being offered, often contain long and complex legal statements that are difficult to read and/or understand by many users. In order to avoid "a large, cumbersome, complicated User Agreement presented to the user only when they begin to use a product or service", the concept of 'Just-In-Time-Click-Through Agreements' (JITCTAs) was introduced. "The main feature of a JITCTA is not to provide a large, complete list of service terms but instead to confirm the understanding or consent on an as-needed basis. These small agreements are easier for the user to read and process, and facilitate a better understanding of the decision being made in-context. Also, the JITCTAs can be customized for the user depending on the features that they actually use, and the user will be able to specify what terms they agree with, and those they do not. It is hoped that the users will actually read these small agreements, instead of ignoring the large agreements that they receive today."[12].

The concept of a JITCTA was also used for the PRIME HCI proposals for the design of the "Send Data?" dialogue boxes (see [15] and below). However, a problem with click-throughs including JITCTAs is that users have the tendency to automate behaviors so that the individual parts of an action are executed without conscious reflection [19]. Thus, too many click-throughs in a row should be avoided. The PRIME HCI work package has therefore also developed the alternative concept of Drag-And-Drop-Agreements (DADAs), which, of course, can also appear 'just in time' (see below).

3.2 Art. 29 Working Party Recommendations

The Article 29 Data Protection Working Party has recently investigated what information should be provided in what form to users in order to fulfil all legal provisions of the EU Data Protection Directive 95/46/EC for ensuring that data subjects are informed of their rights to data protection [5]. The Art.29 Working Party recommends providing information in a "multi-layered format under which each layer should offer individuals

the information needed to understand their position and make decisions". They suggest three layers of information provided to individuals, which include the short privacy notice, the condensed notice and the full privacy notice. The short notice (layer 1) must offer individuals the core information required under Article 10 of the Directive 95/46/EC, which includes at least the identity of the controller and the purpose of processing. In addition, a clear indication must be given as to how the individual can access additional information." The condensed notice (layer 2), which must be available at all times online but also in hard copy via written or phone request, includes in addition all other relevant information required under Art. 10 of the Data Protection Directive, such as the recipients or categories of recipients, whether replies to questions are obligatory or voluntary and information about the data subject's rights. The full notice (layer 3) includes in addition to layers 1 and 2 also "national legal requirements and specificities."

The Art. 29 Working Party sees short privacy notices as legally acceptable within a multi-layered structure that, in its totality, offers compliance. JITCTAs as defined in the PISA project are in fact corresponding to such short privacy notices. The PRIME project has also followed the Working Party's recommendations to use multi-layered privacy notices in its design proposals (see [15] and below). It can however be noted that the layered principle does not in itself provide the means to fully readable comprehensive notices when mobile devices with small screens are used (see 5.3.3 below).

4. PRIME UI PARADIGMS

In this section, we will present the main characteristics of alternative UI paradigms for identity management that have been elaborated and tested by the PRIME partners within the PRIME HCI work package.

A particular feature prominent in all these attempts was the bundling of personal data with different pseudonyms. The bundles were called *roles* or *areas* in the three main UI paradigms represented among the user interfaces, namely the role-centred, the relationship-centred and the TownMap-based UI paradigms.

The first two paradigms are traditionally styled while the third one is an attempt to make preference settings more accessible and, hopefully, understandable to users. On the other hand, the two latter ones share a common approach to the use of preference settings, namely that the selection among the different preference settings (roles and areas, respectively) is implicit when connecting to each service provider. A user has different privacy needs as regards different communication partners and pre-defined selection of roles should facilitate a lot.

The three paradigms are presented in the three following subsections. The UI paradigms have been embodied in an early prototype for IDM [2] and in some mock-ups produced for the PRIME project.

4.1 Role-centred Paradigm

Role-centred means that user control of data disclosure is primarily done via the 'roles' described above. Within a role, the user can set and utilise different disclosure preferences for different data types. The user then has to select the role he will be acting under when contacting service providers, and whenever he thinks that this role is inappropriate, he has to select one of his other roles. The UI paradigm was embodied in an early user-side prototype called DRIM (Dresden Identity Management [2]) where the IDM functions were displayed in side bars of an ordinary Internet browser (Mozilla Firefox). This UI paradigm also figures in one of the PRIME mock-ups where the IDM functions were integrated in an ordinary browser (MS Internet Explorer) to explore toolbar designs (this mock-up was never tested with users).

4.2 Relationship-centred Paradigm

An alternative approach could be to define different privacy preferences in relation to each communication partner. In the *relationship-centred* UI paradigm embodied in PRIME mock-ups, the identity management controls are integrated in the same way as in the role-centred mock-up, but in addition, the ordinary bookmarks ("Favorites" in Explorer) have roles attached to them. By default, a predefined role based on transactional pseudonyms[2] called "Anonymous" is activated. Further kinds of roles could be defined by the user and added as a start-role for any of the bookmarks. In this way there is during ordinary web browsing no extra step of selecting roles. By using transactional pseudonyms as default, the relationship-centred approach allows the privacy-enhancing functions to be switched on from start even if the user is not prepared to actively select among them.

In fact, in the PRIME mock-ups, we decided to always have the icon for the anonymous role ready in the bookmark list, so that anonymous 'entrance' to all bookmarked web sites could always be made – one can hypothesise that even a user, who sets the role of a "registered customer" as the default for a specific web site, does not always want to be recognised when visiting that web site. In Figure 2, the anonymous role is selected by clicking the masked man for each bookmark while the two other icons stand for roles that might be recognizable by the service provider via the pseudonym that the role is acting under and/or by some automatically released personal data (if the service provider requests such). Clicking on the name of a bookmark implies selecting the left most role if there are more than one icon.

Figure 2. Bookmark list with role icons

The solution described above works when a user accesses web sites via bookmarks. On the other hand, when the user enters a web address in the address field of his browser *the system should find* the default role for that site, if the user has defined one; otherwise the anonymous role should be used because this is the standard setting and applies to all web sites if nothing else has been set by the user. More problematic is that users might find it hard to easily select the anonymous role when it is not default; the "Go" button of the web browser could have alternatives as in Figure 3 even if users presumably would use the "Enter" key if

[2] I.e., when a new pseudonym is created for each transaction [18].

they have keyed in an address. The role icon to the left of the address field shows the current role.

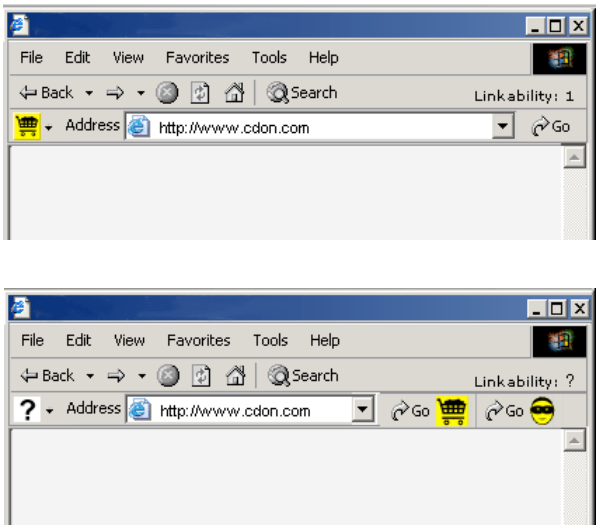

Figure 3. Traditional "Go" button and address field with two "Go"s

The role-centred and the relationship-centred approach differ by what is the primary action by the user: either selecting roles (and only secondly or implicitly communication partner) or selecting communication partner (and implicitly the role = privacy setting). Figure 2 and 3 indicate how the relationship-centred paradigm can be materialised in a UI. However, for both paradigms there has to be a role-list to select from: in the mock-ups the access to this list went via the icon showing current active role, which was placed to the left of the address field (see Figure 3, top).

The primary action of the relationship-centred UI supports the user's primary goals, namely accessing service providers. It should also be noted that while the user interface has to be somewhat more elaborated, this UI does not introduce any extra actions during ordninary browsing, while on the other hand a role-centred UI would force the user to repeatedly change roles (or change web sites if roles have default start sites, but making a role list with a lot of alternative start pages only begs the question of why re-inventing the ordinary bookmark list).

4.3 TownMap-based Paradigm

In the *TownMap-based* UI paradigm the roles are replaced by areas visualising privacy protection concepts with default privacy settings. Predefined areas were the Neighbourhood (where relationship pseudonymity[3] is used by default), the Public area (where transactional pseudonymity is used by default), and the Work area (where relationship pseudonymity is used) with different default privacy options for another set of personal data than for private use. The Work area in fact includes the role concept within the TownMap paradigm, because the user has to decide whether he acts as a private citizen or as an employee. A more explicit use of roles is also feasible but then the design will demand more from the user.

The approach to use different default 'roles' for different areas within a town should make it easier for a novice to see the options available once he has grasped the TownMap metaphor. Individual bookmarks or lists with bookmark menus are symbolized by houses. The user also has his own house in the map (a prominent house at the baseline). Of course, the map display has to vanish or be reduced when the user encounters one of the service providers.

In Figure 4 the user wants to add a shortcut link (similarly to dragging a websites icon from a present-day browsers' address field to the desktop). The user has clicked on the button "Show tools" and picked a house to place somewhere. This will make it possible not only to put a new bookmark in the TownMap but also to put an alternative privacy preference definition: if a web site is already listed in the public space, now the user adds an access point to the same site but in his neighbourhood to indicate that he should be recognized when accessing the web site this way.

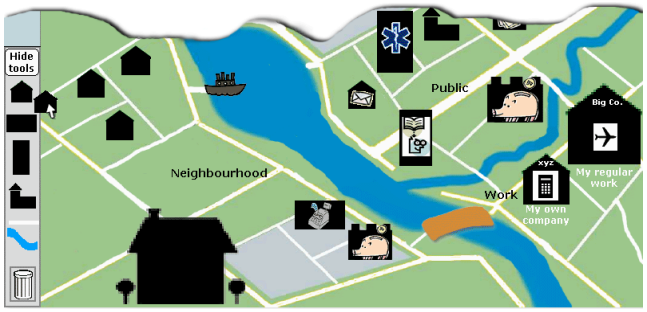

Figure 4. TownMap with building tools visible

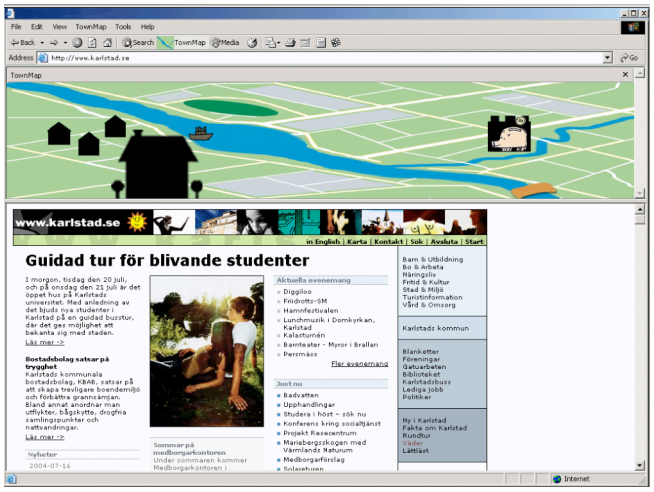

Figure 5. Tilted TownMap visible

Figure 5 shows a view when the user is browsing a site. The user has clicked on the TownMap symbol in the browser bar and can now see a tilted TownMap and all or some of his shortcut links (in this figure only five houses has been placed on the map). This could be refined – just compare the "Looking Glass" UI paradigm

[3] I.e., a pseudonym chosen in regard to a specific communication partner.

presented by SUN Microsystems[4] – but in any event, it allows using the spatial relationships which the user has become acquainted with: the way between the user's house and the bank for instance, can be used for indicating data flow and even for letting the user show preferred data flows; more on this topic in section 5.3.4.

4.4 Data Track

Data Track is a function available in all three alternative UI paradigms. This data tracing function is meant to give the user a possibility to check all the data disclosures that have been made. Also the linkability by the use of pseudonyms should be indicated. The design problems concern mainly the vocabulary including the categories behind (e.g. 'pseudonyms'), the representation of items within each category, and finally the arrangement for searching data. The function will not be explained in anymore detailed here, but it plays an important role as an adjunct to the other features and will be referred to in the following sections.

5. FROM LEGAL PRIVACY REQUIREMENTS TO PRIME UI PROPOSALS

As pointed out in section 3.1, the PISA project has conducted important research on how to map legal privacy principles to HCI requirements and possible HCI design solutions, which was presented in form of a table in [13]. The HCI research within the PRIME project has built on these PISA project results by using and extending the privacy principles and HCI requirements from the PISA table and proposing corresponding PRIME UI solutions (see chapter 4 in [15]). In this section we are only discussing the mapping of some important legal requirements to PRIME UI solutions, namely provisions for informing the data subjects, on rights of the data subjects to access/rectify/block/erase their data and consent as a legitimization for data processing. Finally, we will also discuss in this section legal privacy requirements that have to be considered for UI designs based on predefined roles and default privacy options as used in the PRIME UI paradigms.

5.1 Information to be provided to data subjects

Art. 10 of the EU Data Protection Directive 95/46/EC requires that data subjects from whom personal data will be collected have to be informed about the identity of the controller, the purposes of the data processing – except when individuals are already aware – and about further information in so far, as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair data processing. Web sites of data controllers within the EU have to provide privacy notices or links to privacy notices that display this information. This is, however, not necessarily required for non-European web sites. Besides, those privacy statements usually contain long texts that are usually not read or noticed by users.

As elaborated in [13], the legal privacy principles of information provision and transparency translate to the HCI requirement that users must *know* (i.e. comprehend) who is controlling their data and for what purposes.

We presume that each PRIME-enabled server side should make a complete privacy policy for that side available in computer-readable form (e.g. via ontologies in XML-format, i.e. using the eXtensible Markup Language). The server side's privacy policy will be retrievable from the PRIME application at any time.

In the PRIME HCI guidance and proposals [15], we suggest that the information contained in the server side's privacy policy should be displayed in the PRIME interface in the form of privacy notices by following an approach of multi-layered privacy notices as suggested by the Article 29 Data Protecting Working Party (see [1] and section 3.2 above). A link to the full privacy notice displaying all information required by EU Directive 95/46/EC and other applicable laws (such as Art.4 of Directive 97/7/EC on the protection of the consumers in respect to distance contracts) should be placed at a prominent place in the PRIME user interface (such as plug-in menus found in tool bars in a browser). The full privacy notice should also be retrievable by the user via the Data Track functions.

Figure 6 shows a dialogue box (the so-called "Send data?" dialogue) which is opened in the traditionally styled PRIME UIs because the current role setting of the user is such that all the requested data is not disclosed automatically[5]. Instead the user is required to agree to data disclosures. This "Send data?" dialogue window can be reduced to only contain short and easily comprehensible text but must contain the core information which is required under Art. 10 of EU Directive 95/46/EC. Besides, it must include a link to the full privacy notice (that is, to a condensed privacy notice if no national legal specificities are applicable).

5.2 Data subject's rights to access/rectify/ block/erase data and to object

According to Art.12 of EU Directive 95/46/EC, users have the right of access and under special circumstances the right to obtain from the controller the rectification, erasure or blocking of their personal data. Art. 14 (a) of the Directive also defines a right to object to the data processing, in particular if data are processed for the purpose of direct marketing.

Users must know what rights they have and understand them in order to exercise their rights. In the PISA project, these privacy principles were translated to the HCI requirements that users are *conscious* of their rights, and that they *understand* and can *exercise* their rights.

In the PRIME HCI guidance and proposals [15], we suggest that information about the data subject's rights has to appear in the

[4] "Project Looking Glass", www.sun.com/software/looking_glass

[5] The user can specify in the role settings that some data items may be automatically disclosed to specified parties and for specified purposes.

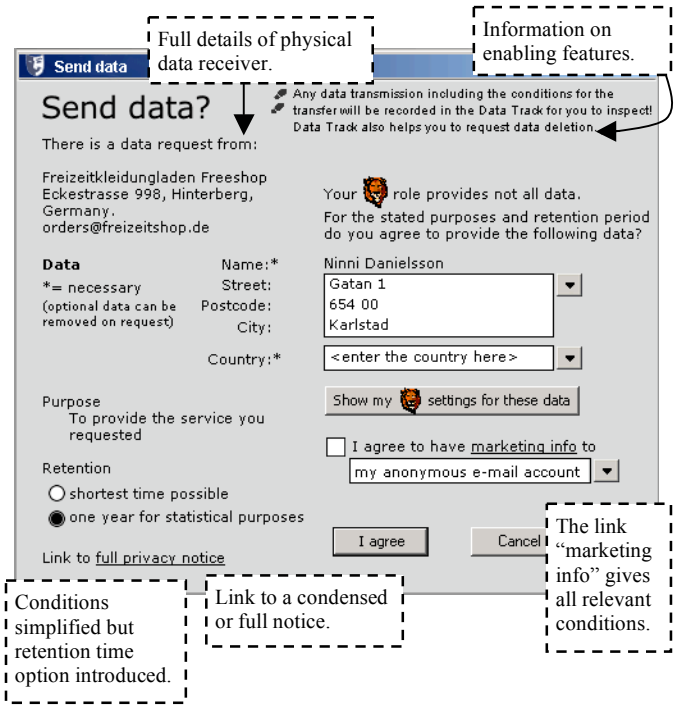

Figure 6. Send data?

privacy policy and in the privacy notices (i.e. if multi-layered notices are used, it should appear in the condensed privacy notice or in the short notice if this is necessary for guaranteeing a fair data processing). Besides, relevant information could, for instance, be provided through a click-through agreement at registration (as also suggested in [13]). Furthermore, the interface should provide obvious tools for exercising the data subject's rights.

Ideally it should be possible for the data subjects to exercise these rights both on-line and at the physical address of the controller (see also chapter 2 of [6]). Links to such online access functions could be provided in the Data Track window as an extension to the Data Track functions. Besides, email / snail address for requests to access/rectify/block/erase data or to object to data processing has to be provided in the privacy notices which can be used as a fall back solution in case that the online functions do not work.

5.3 Obtaining consent from data subjects

"Unambiguous", "explicit" or "informed" consent by the data subject is often a prerequisite for the lawful data processing (see for instance Art. 7.a EU Directive 95/46/C or Art. 9 EU Directive 2002/58/EC). Informed user consent is also seen as a HCI requirement in [13].

5.3.1 Consent to automatic disclosure settings

As mentioned above, the user can specify in the role settings that some data items may be automatically disclosed to specified parties and for specified purposes. By selecting the automatic disclosure option, the user implicitly gives his consent to data disclosures for purposes and types of data controllers that he selects in the automatic disclosure form. It should not be possible to set automatic disclosure for the special categories of data according to Art. 8 Directive 95/46/EC (i.e. data that are regarded as very sensitive such as health data or data about religious believes) for which an explicit consent is required. Besides, the user must always have the possibility to change or disable the automatic disclosure setting. Furthermore, the user should constantly be aware of these settings, and thus should be reminded about his automatic disclosure settings at the first time of use and at regular intervals.

5.3.2 A dialogue box for informed click-through

For data disclosure agreements that the user has to make while requesting a service, similar specifications need to be done. In this case, however, one has to consider that a user, who might welcome a detailed dialogue box in one situation, might find it superfluous and irritating in another situation. Furthermore, it is an open question to what extent this can be handed over from a user interface which the service provider is in control of (inside, e.g., the user's web browser) to the PRIME system at the user side.

JITCTAs as defined in the PISA project constitute a possible solution for obtaining consent by the user. Also two-clicks (i.e. one click to confirm that one is aware of the proposed processing, and a further one to consent to it) or ticking a box have been suggested by different European legal experts and data commissioners as a means for representing the data subject's consent (see also chapter 2 in [6]).

As discussed above, the "Send data?" window should correspond with its form and content to a JITCTA. If the approach of multi-layered privacy notices is implemented, the "Send data?" window should contain the core information to be displayed in short privacy notices.

The "Send data?" window shown in Figure 6 includes also some suggestions on how to provide options for data releases. There are non-mandatary data fields (street, postcode, city) which however the current role has filled in. Retention period is possibly not filled in by the role but suggested by the service provider. Opting in for marketing information is a third option. It is debatable whether non-necessary information should be included in a standard window like this. However, letting the user open sub-windows for such information might make it too complicated even if this allows for extensive user tailoring of the conditions. An alternative is that the service provider has several sets of data requests on his side which are opened only when the user calls for them.

Often the information stipulated by Article 10 (identity of data controller, purpose of processing, any particular circumstance needed for fair processing) is already known by the user/customer, and then it is not necessary to give it explicitly according to this Article (a reference to the full information must, however, always be given). The user can give his informed consent without having to read an elaborated "Send data?" dialogue box which only states the obvious. Especially for mobile phones this may be a very good solution. Two problems remain, however, in the mobile case as the following subsection reveals.

5.3.3 Informed consent mobile phone displays

As just noticed, in many cases the explicit agreement from the user may not need any elaborated information boxes to be read by the user.

However, there remains the question of how to deal with the full information in small-display units. Article 29 Data Protection

Working Party, mentioned in section 3.2, suggests that a longer text is not broken up into consecutive parts but rather condensed in one or two steps giving a hierarchical link structure such as Short notice → Condensed notice → Full notice [1]. This principle may have little to offer users of small mobile phones if they want to go beyond the short notice. The screen will not get bigger the deeper into this structure the user comes, so some way of handling the full text will have to be provided at the end, such as dividing the text by hyperlinking or making it scrollable. The suggestion from the Working Party mentions the possibility to use a common format. This would enhance the possibility to automatically indexing the longer notices (i.e., the 'full' and the 'condensed') which would facilitate hyperlinking. User preference tests will have to be performed for the many solutions conceivable.

A second problem with the small devices, and possibly with many ordinary computer stations, is that a low bandwidth may make it hard for a user to access the condensed notice (or full notice) as quickly as supposed by the Article 29 Data Protection Working Party when it stresses that this notice should be accessible online "at all times". It is not unthinkable that service providers put inconsiderate heavy graphical adornment or privacy-policy illustrations on their web pages. If there are problems to download this notice, some users might start to skip reading such information and just click I agree in the agreements window (e.g. "Send data?"). Thus, the total system is not in the spirit of the EU Directive 95/46/EC [5]. A possible PRIME solution is to let the "Send data?" function have control over the whole process, downloading automatically the condensed notice and not showing the short notice until it is certain that it is possible to immediately show the condensed notice if the user requests so.

5.3.4 Consent by drag-and-drop actions

The problem of click-throughs however is that having to click *OK* or *Cancel* in the ever-present confirmation boxes of today's user interfaces makes most people react by automatised actions, often clicking the right alternative but sometimes getting it wrong. One of the basic premises of Raskin's, mentioned in section 3, is the observation well-known within psychology of the tendency of people to automate behaviours so that the individual parts of an action are executed without conscious reflection. "A set of action that forms a sequence also becomes clumped into a single action; once you start a sequence that takes less than 1 or 2 seconds to complete, you will not be able to stop the sequence but will continue executing the action until you complete that clump." ([19], p. 22)

Raskin uses this observation to argue against dialog-boxes asking for confirmation from users. Because such boxes pop up frequently in certain situations, users will become accustomed in such situations to simply click any *OK* button. The (alleged) confirmation is then executed subconsciously and is not really trustworthy.

Drag-and-drop actions could be a way to avoid such automation of behaviour. As mentioned in section 3, DADAs ("Drag-And-Drop Agreements") were introduced in the TownMap-based UI proposals as an alternative way for users to express consent by moving graphic representations of their data to receivers' locations on the TownMap. In such a construction, the user not only has to pick a set of predefined data (which would be much like clicking "Agree" on a pop-up window), but choose the right personal data symbol(s) and drop them on the right receiver symbol. Thereby, the system can to some extent check that the user has understood the request (in contrast to JITCTAs or two-clicks, where users are still tempted to automatically pressing buttons without clearly reading the text). So-called ToolTips, displaying the specific data content for each data icon, can accompany the drag-and-drop actions. The number of drag-and-drop operations needed to agree varies depending on how much information is contained in a symbol (e.g., a credit card icon could contain card number but also expiry date and holder's name).

The system's check mentioned in the last paragraph requires that the information is already requested by the service provider, so that the drag-and-drop action really is an act of *confirming*, and not an act of stating conditions (a text corresponding to a JITCTA is appearing and requesting the user to agree to the data transaction by drag and drop of the right personal data symbol to the right receiver symbol). Drag-and-drops can be mistakenly performed and would need a last confirmation if they are used to *state* the conditions of an agreement. In normal 'click-based' interactions a final confirmation is sought by requesting yet another click from the user. Hence, drag-and-drops for stating conditions are not as secure as drag-and-drops for agreements and would need a last confirmation click. For minor statements, one might avoid an extra agreement click, as in Figure 7 where the user has selected his VISA credit card rather than his MasterCard (he has also already dragged his name icon to the service provider).

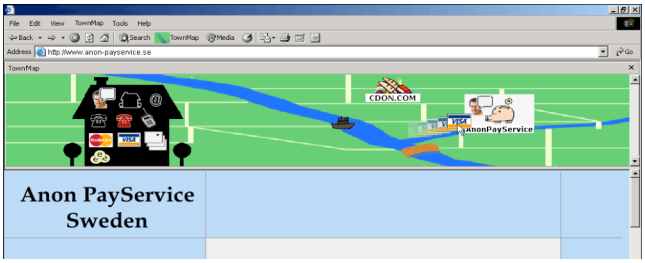

Figure 7. DADA to send credit card info (upper part of a screen shot).

From Figure 7 it should be obvious that this UI concept for providing user consent should work also as an alternative within a traditionally styled UI paradigm. From the TownMap point-of-view, one can say that the town map has been cleared of irrelevant entities when it reappears in the top of the browser's window during the user's interaction with a specific service provider's site (cf. Figure 5). The tilted view of Figure 7 has been evoked because some data are requested (only part of the browser window is visible in the figure). Alternatively, from the point-of-view of the relationship-centred design, a rudimentary town map is shown to provide some screen space for the three entities involved, namely the user, a shop, and a third party pay service.

Dragging and dropping an item on the computer desktop constitutes an action of the user that is similar to actions, such as ticking a box, that have been legally acknowledged as a way of expressing user consent. Hence, as discussed in [6], it can be assumed that also drag and drop can express a user's consent.

5.4 Legal requirements for predefined roles and default privacy options

In the relationship-centred UI paradigm, the so-called roles can be utilized to pre-define privacy preferences vis-à-vis individual service providers. Similarly, the TownMap-based UI paradigm uses default privacy settings for different areas of the TownMap. Predefining a role other than a totally anonymous one and predefined privacy options may prove problematic [6]. For instance, there could be a predefined role called "Registered customer" that a user can use with several service providers – his PRIME system (user-side IDM) then uses a special role-relationship pseudonym for each web site accessed by performing this role, but the data disclosure rules are the same for all these sites. "Even for "registered customers", the personal data required by a service provider may vary, depending on the type of the service offered or the payment methods accepted. For instance, providers of services which are delivered electronically (e.g. computer programs, e-books, music files, etc.) have no need to know the physical address of the customer. Similarly, those providers who offer an anonymous payment and/or delivery system need much less identifying information about their customers. Consequently, a single, fit-for-all pre-defined customer role may prove much more complicated in practice than we now assume." (chapter 2 in [6]).

Predefined roles or privacy settings may for these reasons not correspond to the privacy principle of data minimization derived from Art. 6 (1) c of the Directive 95/46/EC, unless users can, as in the PRIME UI proposals, define the pre-settings or else at least be aware of them and have the possibility to change them. As yet empirical data is lacking on how complicated it might be to really use several roles. The level of complication will depend in part on how users name roles they have created themselves; for instance, "Electronic delivery" and "My street address" may have privacy preferences that matches exactly what is required in some situations. Possibly, a set of pre-defined roles for common usage may be defined. Moreover, in order to make the use of pre-settings more transparent for users, they have to be reminded about them at regular intervals and at least before the first instance of an automatic data disclosure allowed by a role.

6. EVALUATION

The usability evaluation consisted mainly of several usability tests and some questionnaires. Also one preference test was conducted comparing the traditionally styled relationship-centred design with two TownMap designs. Except for this preference test, the TownMap paradigm did not figure in our tests. It was deemed too hard at the present stage to develop a convincing new graphical appearance. There was also the consideration of the mental effort for people to replace a more traditionally styled UI with a new one, if the focus is on people's ability to manage the interface.

At the project start, the role settings in the user side early prototype for identity management DRIM [2] were tested. Then we used interactive mock-ups based on the Karlstad University's Ozlab system [14][16] and also an up-dated version of the DRIM prototype. In this way several designs of the role-centred and relationship-centred paradigms were tested. The test tasks mainly focused on simple e-commerce via (faked) web sites. Interviews were made after every usability test session (only 1 participant per session) to capture more of the test user's impressions.

Our evaluation has been carried out both during the re-design of DRIM and during mock-up UI development rather than being performed to choose one among a few final designs. This approach excludes massive testing where a large number of test subjects are involved in a single test. Instead, a 'massive' number of tests have been performed as will be listed immediately below. One should note that before each test, pilot tests with between one to three test users were performed to find weak spots in test designs and to stabilize the tests. Where not otherwise stated the tests were performed in Sweden, mostly with texts in English.

- Initial tests of DRIM: three tests each with 5 test participants, and a fourth test in Germany and in German by the (German) developers with 6 test participants.
- Questionnaires on PRIME-related words: on linkability (use of pseudonyms), 12 participants; on other PRIME-related words (nine words and phrases), 12 participants; joint questionnaire on both PRIME-related words and linkability, however particpants were reluctant to do the second half on linkability which contained several texts, 36 participants (a class of psychology students). Joint questionnaire to 6 German participants.
- Disclosure icons short test: 18 participants (high school students) tested on two triplets for setting disclosure options for personal data.
- Usability test of redesigned role-setting in DRIM: 5 + 5 test participants (the latter half was confronted to new symbols for disclosure options for personal data, but did not have to do the whole test).
- Usability of browsing of the re-designed DRIM: 5 test participants.
- Relationship-centred e-shopping in the mock-ups: one whole-scenarios usability test with 7 test participants; a test including 10 test participants seeing a user interface animation and then answering questions or performing mouse movements on realistic screen-dumps on a laptop (the laptop solution made it possible to visit participants in their homes).
- TownMap preference test (briefly described in 6.2.5): 34 test participants.

In all, eight usability tests, one preference test, and two sets of questionnaires with, in total, 71, 34, and 66 participants, respectively.

6.1 Problems and Observations

The questionnaires and usability tests gave a lot of information on individual design details. The usefulness of such information is of course dependent on whether the details are included in a whole user interface or not. The present section tries to capture more general lessons. In particular, the following are worth highlighting:

- Users had diverse preferences for icons to symbolise roles
- Users had problems to mentally differentiate between user-side and services-side identity management
- There are problems to make people trust the claims about the system, although remedies to this problem based on the Data Track functions were derived from usability tests

- Unclear perception of interdependence between pseudonyms and "real-life" data
- Transaction animations with spatial metaphors "facilitate"

Other things of interest concern the difficulties non-English test subjects had with English phrases in the UI. This will not be dealt with in the present paper, but the results conform to earlier findings of the same research group [17]. It should also be noted that within the P3P project, research on lay users' understanding of privacy-related vocabulary has shown the need for specially designed phrases for the use in user interfaces [3].

6.2 Discussion and suggested solutions

6.2.1 Icons, especially role icons

Usability tests of icons for 'roles' showed that users may verbalise facial icons very differently even though they might understand how to use them.

In the DRIM user interfaces that were subject to our usability tests, users were able to select an icon and a name for each role they created to remind themselves of the particularities of that role. For pre-defined roles, the role icon and name could also be used by the system to indicate for the user in what form he appears to web services (see various figures in this article). For a role "Anonymous", the system suggested the masked man in Figure 8. Several test subjects thought that this man looked suspicious, but other subjects in other test rounds chose that icon even when the system did not provided it.

For the mock-ups we were elaborating with the anonymous concept as the significant characteristic of PRIME. However, one of the theatre masks in a PRIME leaflet has been selected as our "PRIME icon" to avoid bad connotations (Figure 8), while the "Anonymous" icon – the masked man – has been kept also in later tests for the default role "Anonymous" since it entailed no usability problems. Theatre masks are presently considered also for roles but the requirement will always be that it is easy to tell the difference between the role icon and the PRIME icon. An alternative design could use, e.g., a crowd of people as the icon for the "Anonymous" role – all persons outlined in that icon should look the same.

Figure 8. "Anonymous" and PRIME masks

As a conclusion for how to name and symbolise individual preference settings, it seems advisable to always leave the door open for the user to define name and icon, since these two identify data sets and privacy options belong to the user. One possible exception from this rule could be a pre-defined anonymous role based on transactional pseudonymity with no automatic disclosure of any data and a clear system-related name such as "PRIME Anonymous".

6.2.2 Differentiate user-side and services-side

Of particular importance is the finding that users do not really see the difference between 'their' PRIME-enabled browser and the web server side. This showed in various indirect ways. For instance, as a means to control disclosure of personal data several test subjects avoided to enter any data into the DRIM or the "PRIME system" of the mock-up. Another example is that in post-test interviews they talked about functions from the web site and the PRIME program as if these were one.

If the identity management at the user side is under the control of the user, as the PRIME prototype is meant to allow for, it is important that the user understands both the purely physical functions of anonymous e-services but also the difference between user-side and services-side IDM systems. It is important that users are aware that the technology is *their* technology, not just any Internet technology, that is, they must understand that they have control over the personal data stored at the user side. (Cf. the opinion of Kobsa's about personalization of web sites [8].)

Thus, a major HCI privacy principle should be: The user interface shall clearly distinguish between functions provided by services-side and functions provided by the user-side IDM system.

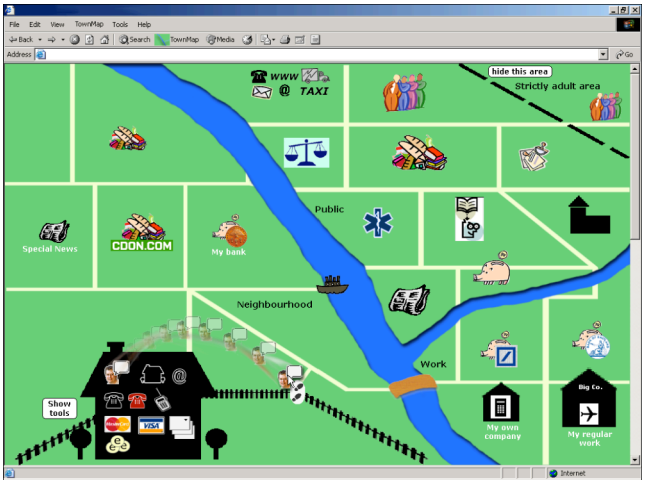

Figure 9. Dragging a name icon to see transmission history (foot print icon at the gate)

For example, in the TownMap design made for the evaluation, the user's 'home' contained the PII symbols that need to be moved to the right service provider or to a PRIME function as depicted in Figure 9. Spatial distance, as utilized in DADAs, between the user's home and symbols of communication partners may help users to differentiate between user side and services side. In contrast, a "Send data?" window with data-entering facility might be harder to make look uniquely the user's own property; moreover, an attacker might be able to create a similarly-looking window.

The DADAs could in principle appear in the traditionally designed user interfaces, but then the design could not be based on screen locations already present in the browser as is the case of the TownMap. Instead, location would have to be established for where the user "is" and where the service provider "is" in the dialogue box.

6.2.3 Trust

"Trust is important because if a person is to use a system to its full potential, be it an e-commerce site or a computer program, it is essential for him/her to trust the system" Johnston et al. asserts [7]. Many European user surveys show that people are not trusting networked data processing to preserve privacy; see e.g. surveys collected in [6]. For instance, in one of the surveys reviewed, 80% of the respondents were concerned about data processors "not keeping data secure at the risk of being stolen" and 72% about processor "not collecting information in a secure way" (p. 43; originally from Information Commissioner UK, 2004 [20], p. 6). Therefore the question of potential users' trust in a system such as the conceived PRIME identity manager is important. Below, factors promoting and preventing users to develop trust, especially legitimate trust, in an identity management system are discussed.

In spite of the introductory texts that our test users had to read and in spite of the presence of anonymous roles etc., some participants voiced complaints over the whole idea of attempting to stay private on the net. "Internet is insecure anyway because people must get information even if it is not" traceable by the IDM application, to partly quote one test participant interviewed after a PRIME usability test session. In fact, information about this person might be released by someone else, but this should not make this person feel that it is pointless to use PRIME client software that warns him for suspicious data receivers before data release. Even more motivating should be that the user-side PRIME system keeps a record of his data releases. This growing record of transmissions should make it possible for him to claim that a specific occurrence of his personal data has not been granted by him because it is not in his "Data Track" (as we have called the transaction database presented in section 4.4 – designing a usable interface to search and sort information from this database is a research task in itself).

To continue with user data and the trust problem, the above citation demonstrates that even if users understand that they have special software on 'their' side, they will not necessarily believe that it will be able to help them. Comments from test users indicate exactly where trust breaks down. It is at such points the UI development must focus on. Two more examples of this are given here.

A test subject said about the Data Track function, "Even if it is good to see what information has been sent it is too late anyway because you cannot undo it." This is only partly true. Possibly, one cannot always directly from the user-side IDM system withdraw information sent to a data processor, even if some 'PRIME-enabled' service providers might allow such actions (the user can be identified via the pseudonym he used when he disclosed his personal data). But a function such as the Data Track mentioned above should inform users about rights to actions such as rectification and erasure of their data. The Data Track should also help the user to, e.g., immediately write an e-mail letter to the data processor about this request, and should preferably contain online functions for exercising these rights (see 5.2).

At another occasion, one participant commented that it is very fine to see what information has been released but remarked that: "On the other hand, I don't know what I would have done if I had seen a list of strange places that had received my data – what I would have done then?" Indeed, what should or even could this person do then, one must ask. And further one must ask, what actions would the help function in the Data Track suggest to a worried user? Hopefully, the PRIME technology should prevent users from releasing data to 'strange places'. Nevertheless, because a prospective user is obviously able to conceive such a situation and to doubt that the system would help in such a case, there must be instructions to users on how to deal with deceptive receivers who have given the impression of being someone else than what the user's IDM system has actually recorded.

Thus, there must be conspicuously placed information ensuring worried users that they will find helpful instructions within the system.

Help functions could also inform about external help to enhance people's trust in PRIME. One could compare wishes surfacing in user studies that e-commerce companies should provide "Access to helpful people" (Nielsen et al., [11]). For a user-side PRIME system there could be up-dated information on consumers' organizations, data protection authorities, police, and possible pay-by-question or -minute helpdesks if it is made clear that they help with legal issues and not only with software support. For mobile PRIME use, telephone numbers for immediate contact in the language preferred by the user should be given. Future user testing will have to prove that no-one who sees a demonstration of the program thinks that they are left alone with the PRIME software system if they start to rely on it. They may doubt that the system per se can help them all the way through all conceivable situations and, therefore, the within-system help functions should also refer external help systems.

'Trust' is not part of the legal requirements for a privacy system, but the legal system is a part of the requirements for trustworthy privacy management.

6.2.4 Linkability vs. "real-life" data

When defining roles, users could choose whether actions and data should be linkable "by all web sites", "by each web site separately" or "never" (corresponding to different types of pseudonymity). Test users seemed to cope fairly well with these phrases. However, it is hard to measure how well they understood that there are implications of their data disclosures that surpass the definition of the linkability settings. For example, if a user decides to give away his telephone number to different places, he could be linkable by this number even if he has selected to be "never" linkable (i.e. transaction pseudonyms are used).

It is not clear how to deal with this problem, even if simulations based on people's own transmission records can enlighten users, as has been discussed within the PRIME project. Perhaps the system should prevent the user from ever enter data manually into web forms etc. but instead always letting everything go via the PRIME system so as to be forced to categorize all data before release. However, this might not be possible for swift chat and email use.

6.2.5 Animation of transactions "facilitates"

As mentioned, the TownMap paradigm was not used in the usability tests. It was deemed too hard at the present stage to develop a convincing new graphical appearance and there was the suspicion that people would prefer a design that they are used to no matter how well the TownMap was designed. Instead a preference test was designed in the following way. Three graphical designs were included. One was the alleged PRIME-enhanced Internet Explorer used for Ozlab-based usability tests.

The second one was the one shown in Figure 7 and Figure 9, while the third was a simplified TownMap called CrossRoad with two main "roads" dividing the screen into four parts – the fourth part being the home area of the user. The rationale behind this third design was to present the predefined areas without making a game-like design. Ozlab was used for making user interface animations of an e-shopping scenario in the traditionally styled browser and for the TownMap in Figure 7 and Figure 9 (but not of the CrossRoad since the interaction design was quite similar to the TownMap). Some speech comments were added to both films (the films were 7 and 5 minutes long).

The test was conducted in lecture halls with several participants at a time. The participants started by filling in a brief form about their age, Internet habits and attitudes. Then they read a 1-page introduction to privacy and PRIME, after which they saw the first film, which was followed by a second questionnaire, this time on their understanding of PRIME and their willingness to trust such solutions. Finally, they saw the animation of the TownMap and were afterwards shown six sample shots, two from each of the three designs, while they were filling in a third form where they were asked to give descriptions (using a few words only) of each design and then rate them according to their own preferences.

As expected, of 34 participants most preferred the traditional design, even if two fifths wanted to be able to switch between designs. The CrossRoad and especially the TownMap was considered cluttered – probably because a lot of "bookmarks" (houses) were already in place. The speaker voice of the films stressed the possibility for the user to build the content of the maps, but the impression was obviously that the design was jumbled.

The above account of this film-based preference test has been brief because the TownMap paradigm will be presented elsewhere. However, for the present paper, where the DADAs have been discussed, there is one result of this test that is of particular relevance. In the user animations, the possibility to utilise spatial relationships of the map was demonstrated. Drag-and-drop agreements were utilized when the "user" sent data to a receiver, a pay service (Figure 7). Similarly, after the DADA actions, the user interface animation shows money being transferred to the shop: a stylized Euro coin moves from the bank icon of the pay service to the icon of the web shop. Drag-and-drop was also utilised when the "user" wants to check transmission history at the end of the film: the "user" drags his name icon to the Data Track footprints icon at the gate of his garden (Figure 9).

Participants were asked about their impression of the demonstration of transmission of credit card details and money. They were instructed to circle one of three alternatives in two columns: *Hard to understand – Superfluous – Facilitates*; and *Childish – Corny – OK*. The interesting fact is that although only 10 of the 34 participants ranked one of the maps highest (7 for the TownMap and 3 for the CrossRoad), more than half of the participants circled "facilitates" when asked about their impression of the animations of transactions. Most of these also thought it looked "OK". It should be noted that these animations were performed manually by the assistant making the screen capture and could be expected to be regarded as amateurish and clumsy.

Naturally, it should be possible for users to switch off such demonstrations of ongoing transactions (e.g. of money transfer in the example above) if they do not want to see them, but such animations complement well the use of DADAs. The question is how well they work in traditional user interfaces where things are not already set in 2-dimentional locations (the test result does not cover this situation since it was only in the TownMap film that demonstrations of DADAs and transactions were shown). Possibly a reappearing diagram with fixed points for standard types of actors can serve to animate transactions. But in such a solution the positions will have to be explicitly labelled with the name of the actors for each new transaction (except, of course, the user). Keeping the user's position fixed may also help to overcome the difficulties test users seem to have to differentiate between user-side and services-side IDM functions.

As can be seen from this section, there are different ways of pursuing tests with users. This is a very important methodological consideration when dealing with identity management because most people are not aware of the complexities of privacy threats or of what are the right protection methods.

7. CONDLUDING REMARKS ON HCI-PRIVACY

In this section we reflect on the definition or at least the characteristics of usability work for privacy-enhancing technology.

The PISA project derived HCI requirements from legal principles. Such principles could be debated but have to be taken as necessities when designing or evaluating a real system. However, the "possible solutions" suggested in their table (cf. section 3.1 above) are always open for interpretation and, most importantly, the number of solutions will be higher if new interaction elements are introduced, such as the DADAs.

To compare, there is a paper by Johnston et al. where security HCI is defined: "HCI-S is human-computer interaction applied in the area of computer security". [7] The authors derive HCI criteria from Nielsen's ten usability heuristics [10]. The reason for this reliance is "the established nature of these criteria". The contribution by Johnston et al. consists in the introduction of some criteria and the reduction of the number of Nielsen's criteria. One principle of Johnston et al. that is of particular relevance to PET systems designers is the 'Convey features' principle – both security and privacy-enhancing features may go unnoticed if they are not readily presenting themselves since most people lack knowledge of such features.

However, for the present discussion of the foundation of privacy UI principles, one should note that Nielsen based his criteria on an analysis of 249 usability problems from which he distillated the most important factors. This empirical background is not mentioned in the paper by Johnston et al. Neither do they test their set of principles in any comparative analysis of usability evaluation by inspection and usability evaluation by user testing (such comparative studies exist; e.g. [9]). This is not to deny that the 'case study' presented in their paper – an analysis of Window XP's Internet Connection Firewall – highlight many usability weaknesses. But the credibility of the usability claims concerning their proposed altered system could be questioned, especially the evaluation according to their criterion User satisfaction. Probably, most designers would consider such a criterion fulfilled when inspecting their own proposals.

These examples show that a set of requirements cannot be the "final" methodological contribution to the area of security HCI

(HCI-S) or privacy HCI (HCI-P). It is not only that user testing will always have to be performed. User testing is not in itself an answer for avoiding biases because degrees of compliance to criteria must always be counted with. But there are more questions.

Above, the need to develop standards for how to introduce test users to the area of PET was mentioned. The problems depend on people's vague notion of privacy protection through identity management. The introductions that we have explored so far within the PRIME project varies from short texts over longer texts to user interface animations, as well as conducting specially designed short tests which do not need any introduction. In this way we are contributing to the methodology of privacy HCI. To this come the test set-ups themselves which have included not only prototype testing but also specific computer-based methods for testing with mock-ups (all these things are described, albeit somewhat cursory, in [6]).

The lesson for HCI-P is that user-test methodology is an important aspect of privacy HCI.

8. ACKNOWLEDGMENTS

We thank all our colleagues for helpful comments and inspiration, especially Anna Buchta, KU Leuven, and Christer Andersson, Karlstad University and the PRIME teams at TU Dresden and ICPP in Kiel.

The work reported in this paper was supported by the IST PRIME project. The PRIME project receives research funding from the Community's Sixth Framework Program (Contract No. 507591) and the Swiss Federal Office for Education and Science.

9. REFERENCES

[1] Article 29 Data Protection Working Party. *Opinion on More Harmonised Information provisions*. 11987/04/EN WP 100, November 25 2004. http://europa.eu.int/comm/internal_ market/privacy/workingroup/wp2004/wpdocs04_en.htm

[2] Clauß, S., Kriegelstein, T. Datenschutzfreunliches Identitätsmanagement, *DuD Datenschutz und Datensicherheit 27*, pp. 297, 2003.

[3] Cranor, L.F., Guduru, P., & Arjula, M. *User Interfaces for Privacy Agents* [forthcoming] ms 2004.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L No. 201, 31.07.2002.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L No. 281, 23.11.1995.

[6] Fischer-Hübner, S. & Pettersson, J. S. (Eds.). *Evaluation of early prototypes*, PRIME deliverable D6.1.b, 1 December 2004. http://www.prime-project.eu.org/public/prime_products/deliverables/

[7] Johnston, J., Eloff, J. H. P. & Labuschagne L. Security and human computer interfaces. *Computers & Security*, Vol. 22 (8), pp. 675, 2003.

[8] Kobsa, A. Personalized Hypermedia and International Privacy. *Comm. of the ACM* 45(5), pp. 64-67, 2002.

[9] Law, L-C. & Hvannberg, E. Analysis of strategies for improving and estimating the effectiveness of heuristic evaluation. In Hyrskykari, A. (Ed.) *Proceedings of the Third Nordic Conference on Human-Computer Interaction*, Tampere, Finland, October 23-27, 2004

[10] Nielsen, J. Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.) *Usability Inspection Methods*, John Wiley & Sons, New York, NY, 1994. Cf. also http://www.useit.com/papers/heuristic/heuristic_ list.html

[11] Nielsen, J., Molich, R., Snyder C. & Farell S. *E-commerce user experience: Trust*. Nielsen Norman Group, 2000.

[12] Patrick, A. S. & Kenny, S. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interaction. *Proceedings of the Privacy Enhancing Technologies Workshop* (PET2003), Dresden/Germany, 2003.

[13] Patrick, A. S., Kenny, S., Holmes C. & van Breukelen, M. Human Computer Interaction. Chapter 12 in *Handbook for Privacy and Privacy-Enhancing Technologies*. PISA project. Eds. van Blarkom, Borking, Olk, 2002. http://www.andrewpatrick.ca/pisa/handbook/handbook.html

[14] Pettersson, J. S. & Siponen, J. Ozlab – a Simple Demonstration Tool for Prototyping Interactivity. *Proceedings of the Second Nordic Conference on Human-Computer Interaction*, Demonstration session, October 19-23, 2002, Aarhus, Denmark. Pp. 293-294, 2002.

[15] Pettersson, J. S. (Ed.). *HCI guidance and proposals*, PRIME deliverable D6.1.c, 11 February 2005. http://www.prime-project.eu.org/public/prime_products/deliverables/

[16] Pettersson, J. S. Ozlab – a Systems Overview with an Account of Two Years of Experiences. Chapter 10 in Pettersson, J. S. (Ed.) *HumanIT 2003*, Karlstad University Studies, 26, 2003. http://www.cs.kau.se/~jsp/ozlab

[17] Pettersson, J. S. P3P and Usability – the Mobile Case. In Duquennoy, P., Fischer-Hübner, S., Holvast J. & Zuccato A., (Eds.) *Risk and challenges of the network society*, Karlstad University Studies 2004:35, 2004.

[18] Pfitzmann, A. & Hansen, M. *Anonymity, Unobservability, Pseudonymity, and Idenity Management – A Proposal for Terminology*, v0.21, 3. September 2004, http://dud.inf.tu-dresden.de/Literatur_V1.shtml

[19] Raskin, J. *The Humane Interface - New Directions for Designing Interactive Systems*. ACM Press, New York, 2000.

[20] UK Information Commissioner. *Annual Track Research Findings. Individuals*. 2004. http://www.informationcommissioner.gov.uk/eventual.aspx