End User Transparency Tools: UI Prototypes

Editors:	Erik Wästlund, (KAU)
	Simone Fischer Hübner, (KAU)
Reviewers:	Bibi van den Berg, (TILT)
	Katrin Borcea-Pfitzmann, (TUD)

Identifier:	D4.2.2
Type:	Deliverable
Class:	Public
Date:	June 29, 2010

Abstract

The Data Track is a user-side transparency-enhancing tool developed in PrimeLife, which provides the users with a history function documenting what personal data the user has revealed to whom under which conditions. Besides, it provides online functions to access the user's personal data at the remote services side.

This deliverable documents PrimeLife work package 4.2's work on a usable Data Track. After introducing into the Data Track functionalities and the technical background, we will present the results of five iterations of user interface developments and usability testing, which we performed at Karlstad University and at CURE. We also present our initial work on a Data Track for social communities as well as on a Data Track for lifelong privacy.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483 for the project PrimeLife.

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe – Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

List of Contributors

This deliverable has been jointly authored by multiple PrimeLife partner organizations. The following list presents the contributors for the individual parts of this deliverable.

Chapter	Author(s)
Executive Summary	Erik Wästlund (KAU) & Simone Fischer-Hübner (KAU)
1. Introduction	Simone Fischer Hübner (KAU)
2. Basic Functionality of the Data Track	Hans Hedbom (KAU)
3. Technical Background	Hans Hedbom (KAU)
4. Usability Tests at Karlstad University	Erik Wästlund (KAU), Staffan Gustafsson (KAU) & Peter Wolkerstorfer (CURE)
5. Usability Tests at CURE	Peter Wolkerstorfer (CURE), Cornelia Graf (CURE) & Erik Wästlund (KAU)
6. Data Track for Social Communities: the Tagging Management System	Tobias Pulls (KAU), Hans Hedbom (KAU) & Simone Fischer Hübner (KAU)
7. Lifelong Data Track	Marit Hansen (ULD)
8. Conclusions & Outlook	Erik Wästlund (KAU) & Simone Fischer Hübner (KAU)

Executive Summary

Within the PrimeLife project, Privacy-enhancing Identity Management Systems and Tools are researched and developed, which aim at enhancing the individuals' control over their personal spheres. The set of PrimeLife tools includes the Data Track, which is a transparency-enhancing tool providing the user with a history function, which documents what personal data the user has disclosed to whom under which conditions, as well as with functions for accessing her personal data at remote services sides online. The objective of this deliverable is the presentation of the research and development work by PrimeLife work package 4.2 on a usable Data Track with a focus on HCI (Human Computer Interaction) aspects of the application.

The first Chapter of this deliverable briefly describes the legal background and social trust factors which have motivated the development of the DataTrack within PrimeLife. This chapter also outlines the deliverable itself and provides a short overview of related work.

The second Chapter describes the history functions and the online access function which are the two main functions of the Data Track. The objective of the history functions is to provide the user with a view of what data she has released to various data controllers under which conditions (i.e. under which negotiated or accepted privacy policy) and to enable her to perform granular searches within these listings. The objective of the online access function is to allow the user to examine what data a given data controller have stored about her and also allow to change these data if they are no longer accurate or even delete them if the user no longer wishes the data controller to store the data (if the data controller permits data modifications or deletion). In Chapter three an overview of the technical details of the Data Track is provided.

Chapters four and five both present usability tests performed on the Data Track. All in all, five iteration rounds of user tests have been performed at Karlstad University and at CURE's usability lab in Vienna. Although the objectives of the tests are to investigate the users understanding of the Data Track, an additional objective of these two chapters are to describe the interface solutions proposed by Activity 4. The main results of the user tests are that the Data Track has reached a rather mature state, but that there are still issues that warrant further attention.

In addition to investigating the developed and tested Data Track described above, this deliverable also describes future directions of research that are about to be undertaken.

As more and more personal information is published and distributed by users to other users in web 2.0 settings, such information also needs to be incorporated within the Data Track. The reason for this is not only a matter of history but also a matter of legality and transparency as users broadly publishing information about others should be made aware of that informed consent by the individuals concerned is required. Furthermore, the individuals concerned should have the possibility to either give or deny consent to the publication of personal information relating to them and any consent given or denied by them to the publication of their personal data by others should be documented in their data tracks. Therefore, in Chapter six, a first possible solution of a tagging management system, which can assist users to obtain informed consent before they are publishing data about others, is presented that can work as the foundations for a Data Track for social communities.

Chapter seven deals with a lifelong perspective on the Data Track and the issues that have to be considered in order create a system for privacy and identity management throughout life. The main objective here is not to present technical solutions but rather to understand the implications of key concepts such as privacy and identity management covering all *areas of life*, *the full lifespan*¸ and *all stages of life*.

Finally, in Chapter eight, we summarize the main findings of the deliverable and point out directions for our future work.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation and Background

Privacy-enhancing Identity Management Systems and Technologies, which are researched and developed within the PrimeLife project, aim at enhancing the individual's right to informational self-determination by providing tools, which allow them to better control what personal data are released to which data controllers under which conditions and how these data are processed. For making well-informed decisions on personal data disclosures and for controlling that personal data which were once disclosed are processed according to legal privacy provisions and negotiated privacy policies, the transparency of personal data processing plays a key role.

Moreover, transparency is not only an important principle for protecting the individual's privacy, but is also essential for a democratic society. A society, in which citizens could not know any longer who knows who knows what about them in any given situation, would be contradictory to the right of informational self-determination. Hence, the privacy principle of transparency of personal data processing is enforced by most western privacy laws, including the EU Data Protection Directive 95/46/EC, which provides data subjects extensive information and access rights.

Pursuant to Art.10 EU Directive 95/46/EC, individuals about whom personal data are obtained have the right to information about at least the identity of the controller, data processing purposes and any further information necessary for guaranteeing fair data processing. If the data are not obtained from the data subject, the data subjects have the right to be notified about these details pursuant to Art.11. Further rights of the data subjects include the right of access to data, the right to obtain from the data controller knowledge of the logic involved in any automatic processing of data concerning them at least in the case of the automated decisions (Art. 12 a), the right to object to the processing of personal data (Art.14), and the right to correction, erasure or blocking of incorrect or illegally stored data (Art.12 (b)).

Transparency is also an important means for enhancing end user trust in applications. As discussed by Leenes et al. [Leenes et al. 05], trust in an application can be enhanced if procedures are clear, transparent and reversible, so that users feel in control. This also corresponds to the findings of Trustguide [Trustguide 06], which provides guidelines on how cybertrust can be enhanced.

With the advance of modern communication technology including sensor networks and ambient computing technology, transparency is, however, increasingly at stake. Transparency-enhancing

technologies can help users to enhance transparency of data processing by providing tools to users, or their proxies acting on behalf of the user's interests (such as data protection commissioners), for making personal data processing more transparent to them.

A transparency-enhancing technology for privacy purposes can be defined as a technical tool that has one or more of the following characteristics (see also [Hedbom 09]):

1. it provides information about the intended collection, storage and/or data processing to the data subject, or a proxy acting on behalf of the data subject, in order to enhance the data subject's privacy;
2. it provides the data subject with an overview of what personal data have been disclosed to which data controller under which policies;
3. it provides the data subject, or her proxy, online access to her personal data, to information on how her data have been processed and whether this was in line with privacy laws and/or negotiated policies, and/or to the logic of data processing in order to enhance the data subject's privacy;
4. it provides "counter profiling" capabilities to the data subject, or her proxy, helping her to "guess" how her data match relevant group profiles, which may affect her future opportunities or risks;

A key success factor for the employment of transparency-enhancing tools is usability. The transparency-enhancing tools and their user interfaces should be intuitive and easy to learn, efficient to be used, and they should be pleasant to use and thus be valuated by the end users. This also means that transparency-enhancing tools should provide an optimum of relevant information without overloading her with too many details, which will be hard for her to manage or to digest.

1.2 Objectives, Scope and Structure of this Deliverable

The objective of this deliverable is the presentation of the research and development work by PrimeLife work package 4.2 on a usable Data Track, which we have conducted within the first 28 months of the PrimeLife project.

The Data Track is a user-side transparency tool with a history function, which keeps a record for each transaction, in which personal data are disclosed to a communication partner. This record shows which personal are disclosed to whom, which credentials and /or pseudonyms have been used in this context and what has been the negotiated privacy policy. The first versions of a Data Track have already been developed by us in the PRIME FP6 EU project as part of the PRIME integrated prototype, on which our work in PrimeLife is building. Within the scope of the PrimeLife project, we have further conducted work for enhancing the functionality and usability of the Data Track. For this, we have especially developed and tested user-friendly search functionalities plus online functions, which now allow end users to access, correct or delete their data at the remote services side (as far as permitted). The Data Track is thus a transparency-enhancing tool, which addresses the characteristics 2 and 3 of the definition given above. The Data Track functionality is presented in more detail in chapter 2 ("Basic Functionality of the Data Track"). More background information on technical implementation is briefly provided in chapter 3 ("Technical Background").

The emphasis of our work in WP 4.2, which will be reported here, has been on the HCI (Human Computer Interaction) related aspects. As people engage in many transactions, which may involve multiple providers simultaneously, the implementation of a usable Data Track is difficult from an HCI perspective. Providing users with easy-to-use search tools for finding relevant records about past data disclosure is one example. Besides, so far users have little experiences with online access functions, which allow them to access their data on remote servers. This may also have impacts on how easy the online access functions will be to learn by the end users.

For the development of a usable Data Track, we have followed an iterative design based on a cyclic process of UI (User interface) prototyping, usability testing, and refinements of the Data Track user interfaces. The results of our usability tests as part of the iterative design process are reported in chapters 4 ("Usability Tests at Karlstad University") and chapter 5 ("Usability Tests at CURE").

Furthermore, we have started with research on a Data Track for social communities, which allow users to keep track and better control what information about them is published by others on social networking sites. Our first results on photo management system are presented in chapter 6. ("Data Track for Social Communities: the Tagging Management System")

Finally, also conceptual aspects and ideas on a Lifelong Data Track have been discussed in cooperation with PrimeLife Activity 1, which are summarized in chapter 7 ("Lifelong Data Track").

1.3 Related Work

There is some previous related work on transparency tools for keeping track of previous transactions, even though there is not as much on the usability of these tools.

As mentioned above, a first Data Track version, with a more limited functionality, was developed and tested within the PRIME EU project [Pettersson et al. 06]. The PrimeLife Data Track, which is presented in this deliverable, is enhancing the PRIME Data Track in terms of usability and functionality.

User side tracking functions including online access functions were also already suggested in the PISA EU project [van Blarkom et al. 03].

"iJournal"[Brückner et al. 05], a part of Mozilla Privacy Enhancement Technologies (MozPETs), lets users define what data they want to keep track of and then analyzes the released data for that information, thus keeping track on what information was released and when.

"iManager"[Jendricke 02] for use with PDAs and mobile phones makes it possible for users to attach contexts (application, location and receiver) with identities, thus knowing what data are handed out. However, to our understanding, there is no way of knowing what data have been released if the user dynamically changesheridentity during a session or changes the settings of an identity. Thus, it keeps track of data that were released, but does not really have any history functionality.

Microsoft CardSpace [Chapell 06] also has some transaction tracking capabilities, which however do not include detailed information about negotiated policies. During the final phase of the PRIME project we ran a small test comparing the (still prototypical) PRIME Data Track with Microsoft's CardSpace. The focus in CardSpace on visual although virtual "identity cards" is also reflected in its history functions; users had to search data "per card", while our prototype Data Track allowed for searches across the templates used for data releases. The latter is more of a traditional database design which, admittedly, can be more demanding but this solution was definitively more liked by the test participants although they managed to solve tasks more easily with CardSpace [Pettersson 08].

Besides, there are some commercial systems and applications, such as Google Dashboard, Amazon's Recommendation Service, or the Norwegian E-Government Service Min Side, which grant users online access to their data and allow them to rectify and/or delete their data. In contrast to the Data Track, these are services side functions and not user side tools. Besides, they usually grant users access only to parts of their data and not to all the data that the respective services side processes (e.g., Google Dashboard only provides access to the user's search query history, Amazon only provides access to the user's profile information). Besides, they can only provide

access to authenticated (non-anonymous) users. To the best of our knowledge, no usability studies of these approaches have been published yet.

Chapter 2

Basic Functionality of the Data Track

The Data Track is a tool that is meant to give the user an overview of what data have been sent to different data controllers under which conditions and also to make it possible for a data subject to, in an easy and online way, exercise her rights to access data according to the EU Data Protection Directive. It is thus both a history tool and an interactive transparency tool providing online access to data at remote services side. The Data Track working prototype is currently integrated in the PRIME core for testing purposes but could with a little effort be moved to other environments provided that certain requirements holds (See Chapter 3). This chapter will give a basic overview of the functionality of the Data Track and discuss UI concepts used.

As mentioned above the Data Track both presents sent data as well as gives the user online access to stored data on the service side. When presenting the functionality of the Data Track it is therefore beneficial to divide it into these two parts. For simplicity reasons we will call the functionality for locally keeping track of data disclosures the "history functions", and the functionality taking care of online access to the user's data at a remote services side "online access functions". The following sections will describe these two function groups.

2.1 History functions

Every time the user sends personal data to a data controller that information is stored in the Data Track. The storage itself is not performed by the Data Track but by the application sending the personal data (in the prototype case it is the PRIME core). These data are then accessed and presented by the Data Track. The first thing a user sees when opening the Data Track is a listing of all data controllers that received data from the user (see Figure 1). The listing contains the name of the receiver, over what time period the receiver has received data and the number of sessions in which data have been given away to the receiver (i.e. the total number of sessions recorded in the data track for this receiver. The list also has filtering and sorting functionality. Users can also add columns to the listing in order to see the different categories of personal data sent. By expanding the summary row of a receiver the individual sessions made to the receiver is shown (see Figure 2).

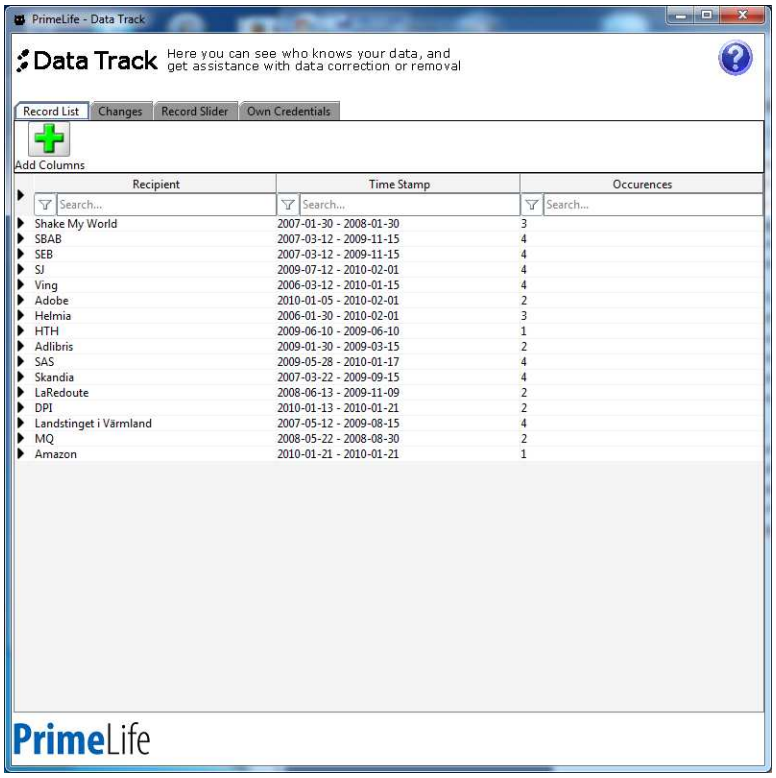

Figure 1: Receiver listing.

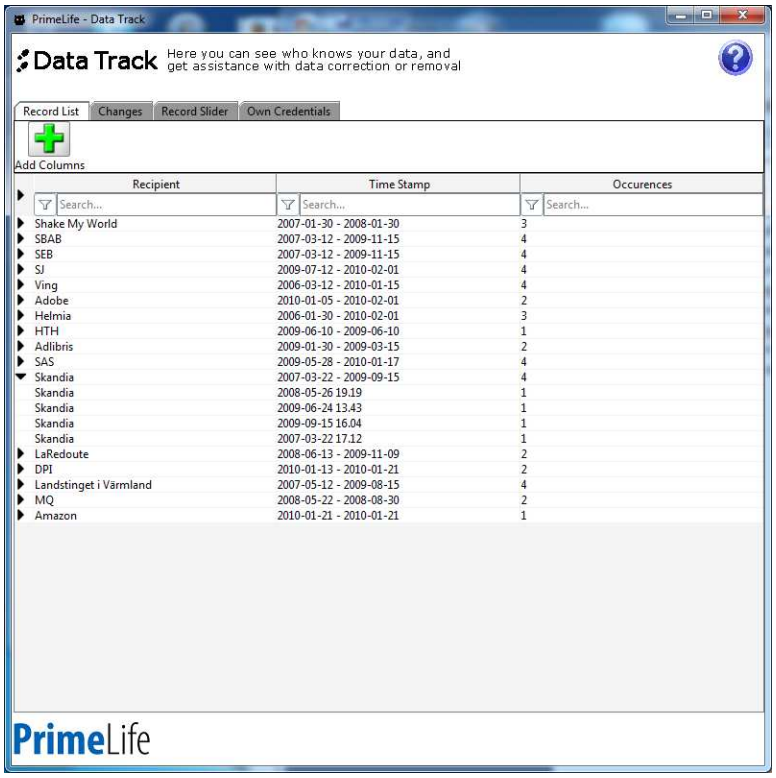

Figure 2: Receiver listing with one receiver expanded

By double clicking on a session (or through a popup choice) the user can open a session window (see Figure 3). This window gives the user detailed information on what data were sent in the session, the exact values of the data and for what purpose the data were sent. The window also contains a button that makes it possible for the user to view a snapshot of the actual negotiated or displayed privacy policy for the receiver.

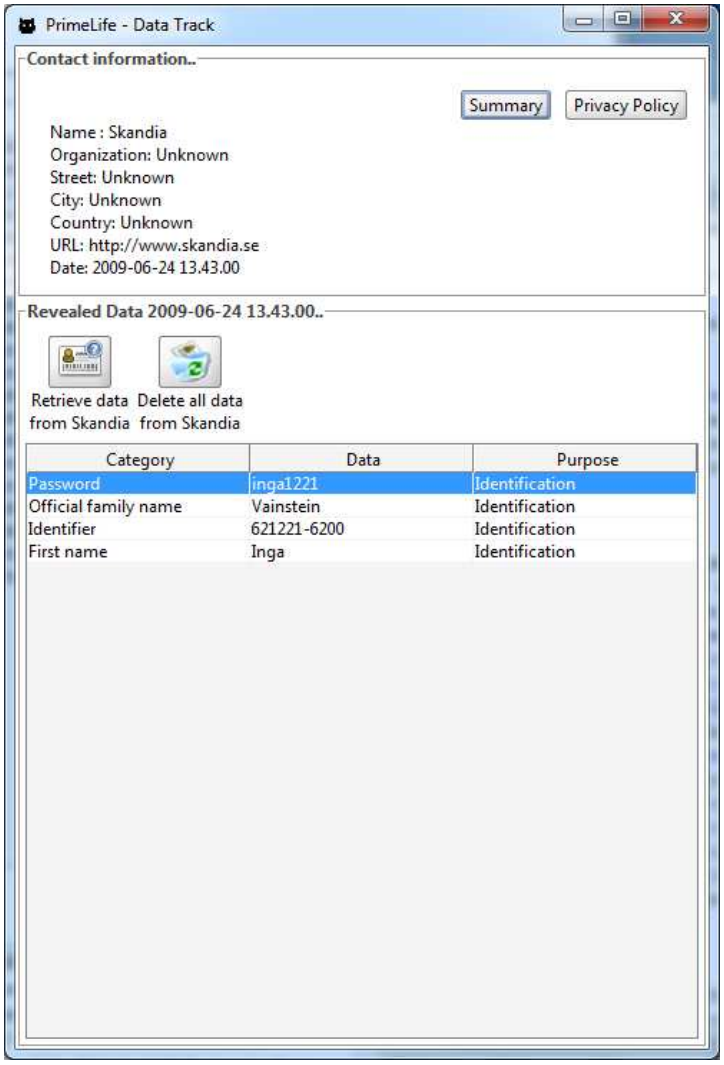

Figure 3: The session window

If the user presses the summary button or double clicks on a receiver summary in the receiver list a summary window is opened (see Figure 4). This window gives a detailed view on all data sent to this receiver in all sessions together with the time they were sent and what entity (if any) verified the authenticity of the data. The history functionality will be further discussed and analyzed in Chapter 4 (UI Tests).

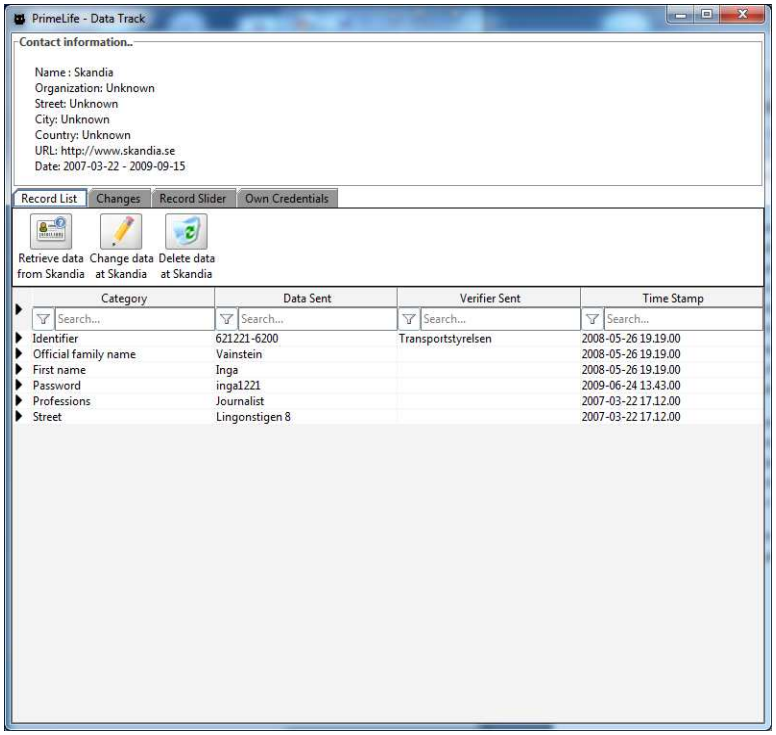

Figure 4: The summary window

2.2 Online access functions

Online access is of course dependent on the rights to access and the privileges that the data subject has on the remote system. Generally these rights are given and managed by the owner of the remote system and could for example be part of the privacy policy that is agreed upon or formulated in some form of service contract. In some cases the system owner is, by law, required to store and process data for a specified time period. In these cases there likely would be limitations to access or manipulation of these data specified by the applicable law.

The online access functions are mostly integrated into the session window and the summary window (see Figure 4). Both windows contain a number of buttons for accessing, changing and deleting data. Starting with the session window, it contains the online access buttons: retrieve data from “receiver” and delete data at “receiver”. If the user presses the retrieve-data button the Data Track will contact the receiver and (if allowed) retrieve the data stored under the identifier used for that session at the receiver side. These data will be presented alongside the data stored in the user Data Track (see Figure 5).

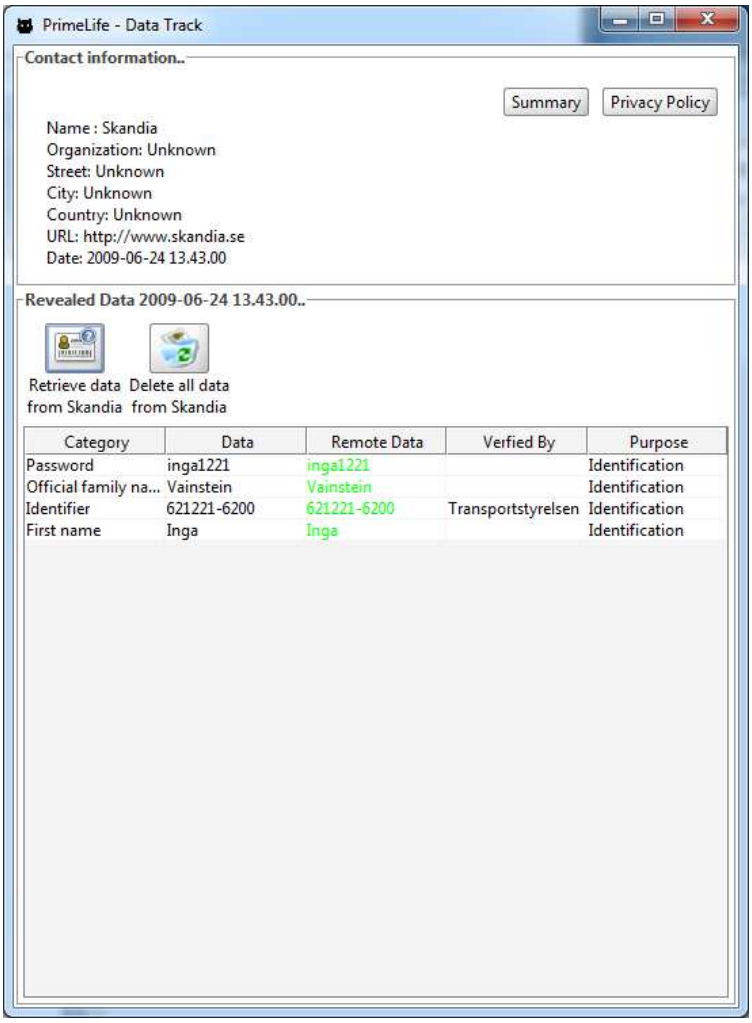

Figure 5: Session window with remotely stored data.

Any deviation between what is stored locally and remotely will be marked in this view so that it is easy for the user to spot any deviations.

If the user pressed the delete all data at “receiver” button, all data stored under the identifier used for this session will be deleted (if the user has the right to do so) from the data controller. A number of warning windows are shown before deletion takes place in order to minimize errors.

Going back to the summary window it contains three buttons for online access functionality, i.e., retrieve data from “receiver”, change data at “receiver”, and delete data at “receiver”. The retrieve data from receiver has the same functionality as the button in the session window with the exception that all data stored under any identifier used to communicate with the receiver is retrieved (if the user is allowed to do this). Further, the verifier of the data (if any) stored at the data controller is returned. The retrieved data are presented in a similar manner as for the session window (see Figure 6)

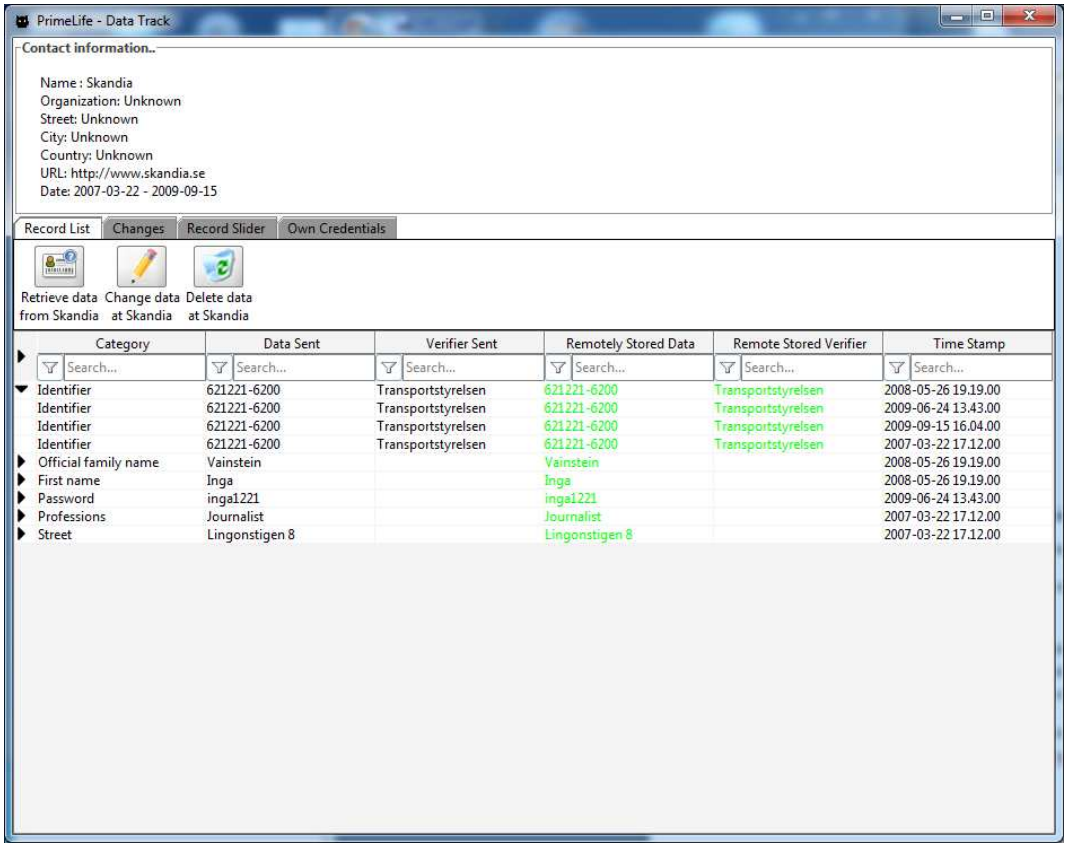

Figure 6: Summary window with retrieved remote data.

By marking an entry in the list and pressing the “change data at “receiver”” button the user can change the value of the remotely stored data (if the user is allowed to do this) and if the user marks an entry and presses the delete data at “receiver” the marked data are deleted on the receiver side.

All changes made will be stored locally and presented in the changes view so that the user has an overview what changes have been made (or requested) and when (see Figure 7). The online access functionality is further discussed and analyzed in chapter 4 (Usability Tests at Karlstad University).

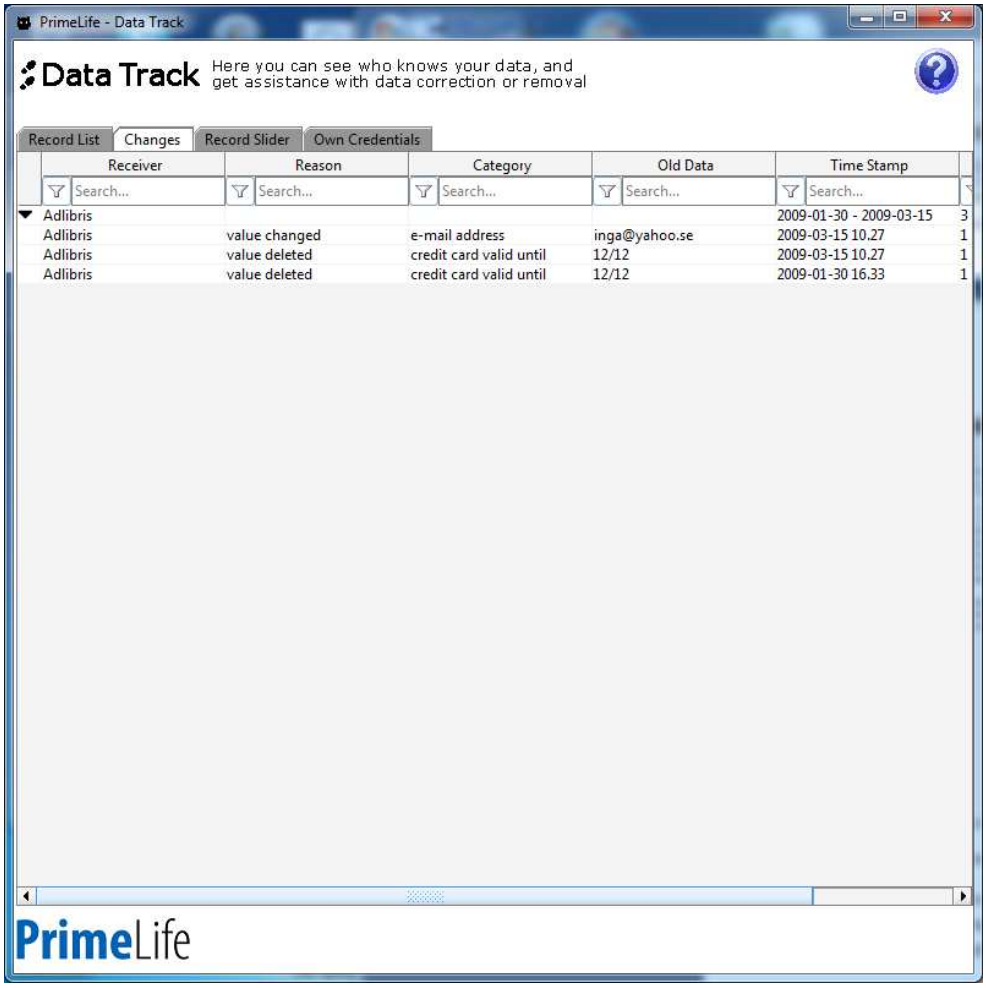

Figure 7: The Changes View

Chapter 3

Technical Background

Data Track - behind the scenes

In this section, we will discuss the internal workings of the Data Track. This will in essence be an overview, not an in depth description, of the technical details of the Data Track. The reason for this is twofold. First, the nature of the deliverable is mainly focused on the HCI problems and the technical part is a support for the HCI parts and second, we want to keep the deliverable in a feasible size.

3.1 Local Function of the Data Track

The Data Track itself is in essence a window on three databases. These databases are the session database, the Personally Identifiable Information (PII) database and the changes database.

The session database contains information related to a specific web server session and contains information such as the contact information of the data controller, the time of the session and links to personal data released during that session. Each session is uniquely identified with a random Universally Unique Identifier (UUID). In the implemented case all UUID are 128-bit random values

The PII database stores all personal data that have been released in the different sessions. The entries there present the category and value of the data. Each category-value entry is stored with a local UUID. The identifier used when the data were released is stored together with each category-value pair. The identifier itself is also a UUID that is shared by the client side and the service side.

Finally, the changes database contains a history of requested changes by the client on sent personal data and changed sessions.

The Data Track itself does not care how the information is entered into the different databases, this could be done by any entity controlling and monitoring the release of personal data. The important thing is that the database structure is preserved. In our current implementation it is the PRIME core and specifically the “send-data–dialog” that stores the data. The Data Track will read the information stored in the databases and presents it in a number of different views, making it easier to understand, and also adds functionality such as the possibility to filter and search the data.

3.2 Remote Function of the Data Track

In order to access remotely stored data the Data Track currently makes use of web services calls to the service side. The web services are divided into three types of services, those that return the data stored on the service side to the local Data Track, those that change or update data stored on the service side and those that delete data stored on the service side.

The services that return data will either return all data associated with an identifier or the value of a specific category of data associated with an identifier. The data returned by the services is compared by the Data Track with the locally stored data and presented in a comparison view. Any deviations between the two sets of data are marked so that the user easily can see if the service side's information is the same as the one sent by the user. Since all data stored on the service under a specific identifier is returned it is possible to derive if the service stores more data than were sent and the value of these data. The data sent back also contains the verifier (if present) of the individual data records. This verifier is presented to the user and thus gives the user an idea from where any "non-sent" data are collected or at least the basic origin of the data.

The services that changes data will change the value of a personal data associated with an identifier based on the category and its previously stored value. The service will not in fact change the value of a PII database entry. Rather, a new PII database entry is created with the new values associated with the identifier and that entry is linked with the session in the Session database. The old entry is unlinked and instead linked to a changed session entry in the changes database. This has been done in order for both sides to keep track of what changes have been made and when and also makes it possible to do a rollback of the changes in case of errors or malfunctions in the system.

Finally, the services deleting personal data associated with an identifier will do this based on the category and the current value of the stored data. For audit reasons and for error handling the data entry itself is not deleted as such, rather its value on the remote service is set to null on the service side. On the client side the entry is handled much like a change and is thus unlinked from the session and linked to a changed session in the changes database. This is done in order to make it possible for a user to keep track of which data that has been deleted.

The functions are all called as responses to different user actions in the interface. Usually these actions are initiated by the user pressing a button or choosing a menu entry in a popup menu. The reasons for not calling functions automatically e.g. when session windows are opened or other actions occur is that this behavior would likely cause a lot of unmotivated error messages when the client tries to open the Data Track and either the client or the service is not on line. We also like the Data Track to have a smooth operation without having access to the net. Of course the remote functionality will not work in this case but the local functionality of keeping track of sent data and searching and filtering in these data would work as expected. This would not be the case if we called the remote service automatically on when opening new views.

3.3 Security Considerations

There are a number of security issues that are not taken care of in the current implementation of the Data Track. These are all related to some form of access control. First, none of the databases used are currently encrypted. This is of course essential in a productive setting since otherwise a compromised client would turn into a great privacy risk for the user. The reason for this in the current implementation is that we are using the databases native to the PRIME core as the data feed and they are not encrypted in the latest version of the PRIME core.

Second, the access control on the web services is at present stage rudimentary. In order to access the data, all that needs to be known is the random identifier shared by the client and the service. In essence this is similar to a 16-byte password access scheme. Clearly this would not be enough in a production system since the data accessed is (or might be) highly privacy-sensitive. This state of affairs can however be easily overcome by exploiting the fact that the services, due to the privacy logging functionality in the core, is also in possession of an identifier unique public key. By encrypting the response of the services with this public key, an attacker needs not only to know (or to guess) the identifier but also be in the possession of the private key tied to the identifier in order to compromise the system. Similarly the private key could be used to sign requests for change and deletion in essence accomplishing a two factor authentication scheme. This is however not yet implemented in the current prototype.

Finally, there is a need for a more fine-grained way of specifying access, e.g., by stating that the user is not allowed to change or delete certain entries or specify under what conditions an entry can be modified. In order to do this in a general manner a policy language is needed. The current version of the PRIME core not fully suited for this purpose. However, there is a new policy language under development in PrimeLife and we are following this development to see if and how this could be used to accomplish a more fine-grained access control in the prototype.

One can remark that strictly speaking the access control is outside of the Data Track since the Data Track is agnostic to how the service accesses and stores the data as long as it is delivered through the specified web services interface. One must also keep in mind that all communication between the client and the web services is conducted over TLS/SSL thus minimizing the possibility of eaves dropping by an external attacker.

Chapter 4

Usability Tests at Karlstad University

In order to evaluate the usability of the Data Track UI, four rounds of usability tests were performed between March and May 2010.

4.1 Test scenarios & test setups

As all four rounds of tests were more or less identical they are described together and differences are pointed out where they occur.

4.1.1 Purpose

The general purpose of all the tests was to evaluate the users' comprehension of the Data Track UI. The first test was a pilot test to validate the test set up and procedure which was followed by two rounds of tests which differed only in regards to the amount of instructions given. The last test round was a combined test were the participants first where asked to use the Credential Selector UI to perform a transaction followed by the Data Track test. This was done in order to see whether users would get a better grasp of the applications if they got to experience both sending data and reviewing stored data firsthand.

4.1.2 Participants

The 48 test participants were aged between 19 and 32, 25 male and 23 female. All participants, except one, use internet on a daily basis. All participants shop online at least once a year. Most users state they shop online once or several times a month and a few users state they shop online once or several times a week. All participants were students at Uppsala University of which none studied computer related topics.

4.1.3 Procedure

All tests followed the same procedure except in regards to the pre-test instructions. The test session was around 30 to 60 minutes long and contained the following parts:

- Oral and written information about the test in general (Appendix A.1)
- Pre-test questionnaire (Appendix A.2)
- Pre-test introduction
- Pilot and first round of tests: instruction movie
- Second round of test: very short oral presentation after which users were given a few minutes to click around as a familiarising task
- Third round (Data Track and Credential Selection combination) as above but with additional information regarding the Credential Selection mock-ups.
- Test person reads task information (see below) and interacts with prototype
- In the third round (Data Track and Credential Selection combination) the participants were asked to use the Credential Selection UI to purchase a book from Amazon.com both before and after using the Data Track.
- Post-test questions (Appendix A.3)
- Online Post-test PET-USES questionnaire (Appendix A.4)
- Discussion about the given answers

4.1.4 Tasks

More specifically understanding the Data Track_UI was operationalized as a number of smaller questions.

- Do users uunderstand how to search within the tables? (Tasks 2,4,5 & 9)
- Do users uunderstand how to open the “summary card”? (Tasks 1,3 & 6)
- Do users understand how to update information via the “summary card”? (Tasks 7,10 & 12)
- Do users understand how to add columns to the main table? (Tasks 2 & 12)
- Do users se the sort function of the main tables? (Task 5)
- Do users se the expand function of the tables? (Tasks 2 & 12)

The questions presented above were investigated through the following specific tasks:

Task 1 - What information have you sent to Amazon?

To complete task 1 in Data Track version 0.61 the user had to first double click the Amazon row in the main window, Figure 8, so that the Summary card for Amazon is opened, Figure 9. Here the users are expected to see that the information sent is the “Card number”, “Credit card valid until”, “Official family name” and “First name”, but also that the credit card information verifier “VISA” and the person verifier “Transportstyrelsen” also is sent.

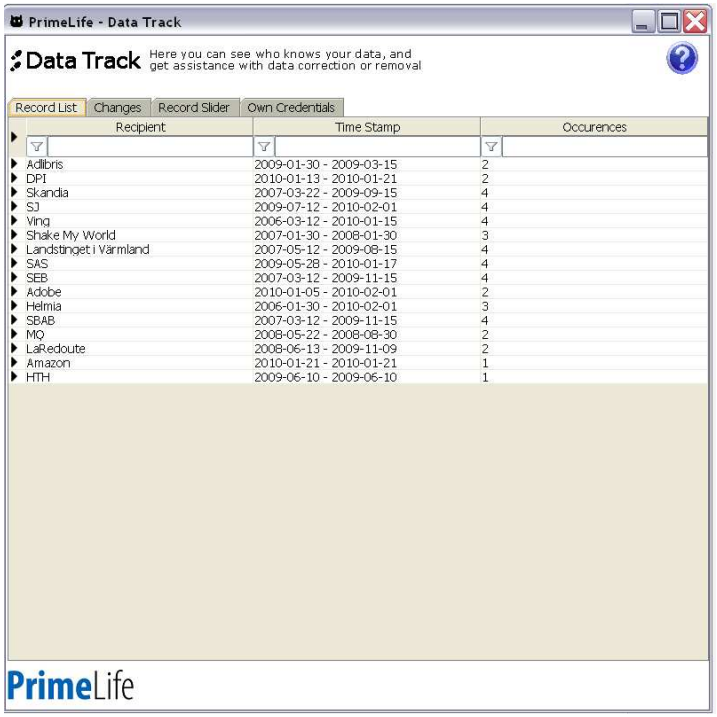

Figure 8: Main window for Data Track v.0.61

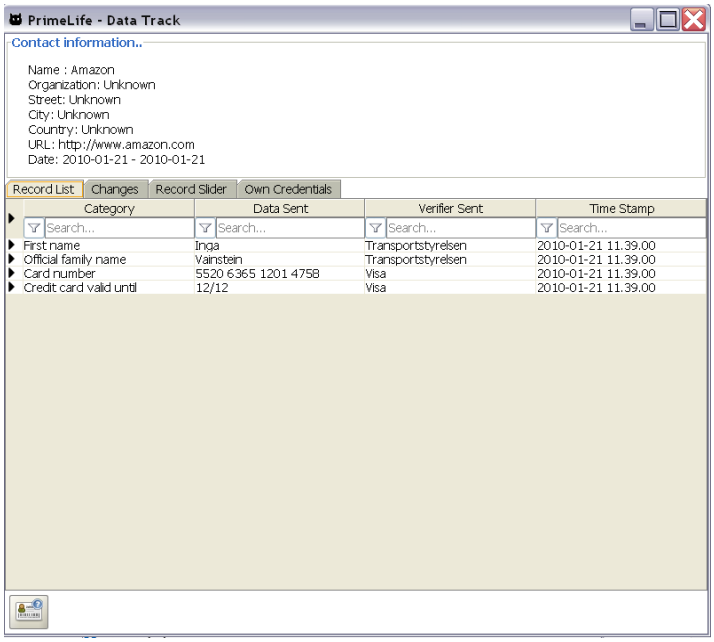

Figure 9: Summary Card for Amazon in Data Track v0.61 and v0.71.

For version 0.71 of Data Track the main window's record list was updated to also include right clicking, both for the summary rows, Figure 10, and the transaction rows, Figure 11. This version also implements an "add column" button, Figure 10, which will be discussed later in this chapter.

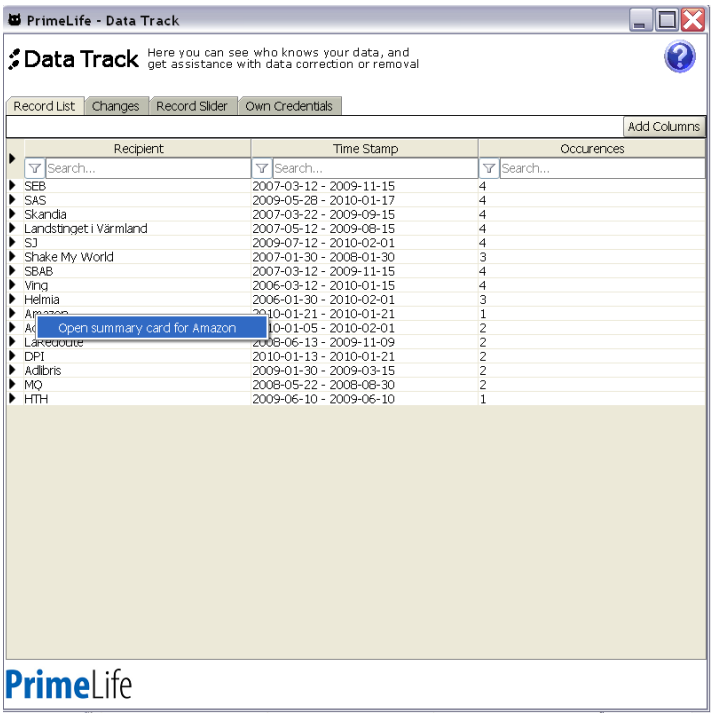

Figure 10: Main window of DT v.071, view of the Record List.

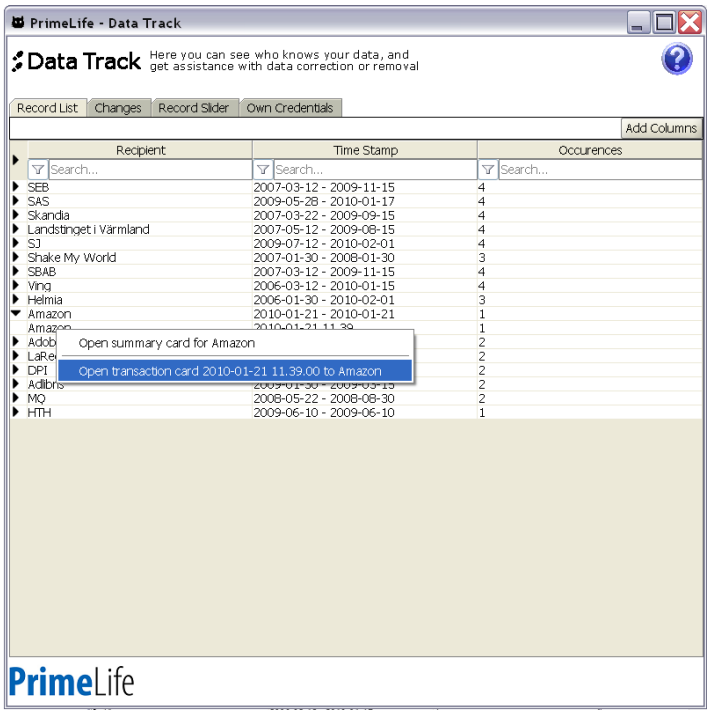

Figure 11: Main window of DT v0.71 showing new interaction of right clicking.

In version 0.8, an “icon bar” is included in the main window and the summary card. In the main window the “icon bar” contains the “add column” button, Figure 12. In the summary card the “icon bar” contains all summary card actions, Figure 13. These features will be discussed later.

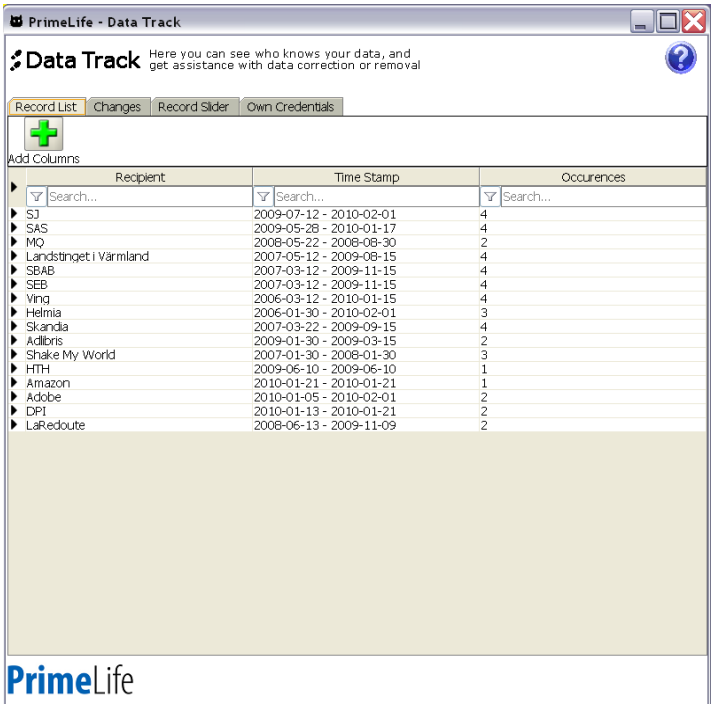

Figure 12: Main window of DT v.0.8, view of the Record List.

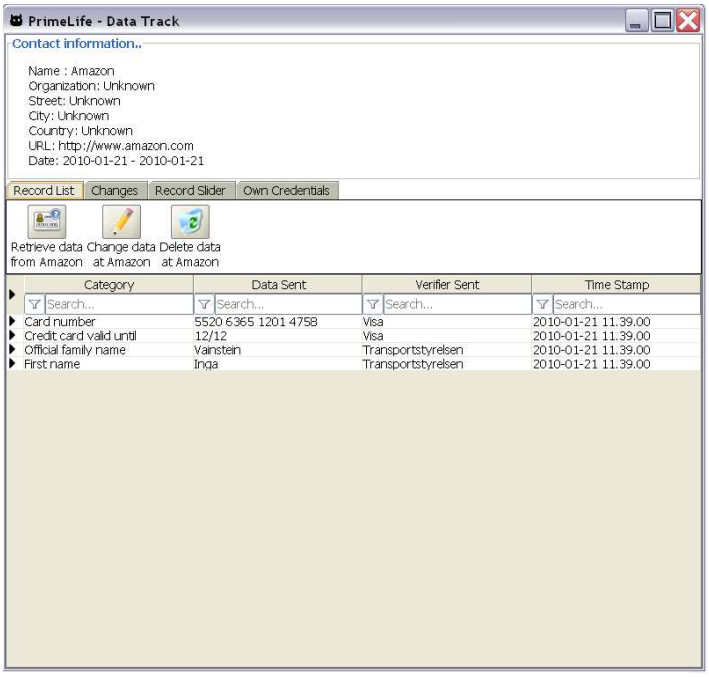

Figure 13: The Summary Card for Amazon in DT v.0.8.

Task 2 - How many times have Helmia received information about your e-mail address ”inga@private.eu”?

To solve this task in the most efficient way the users have to add a new column to the record list. To do this in version 0.61, the users had to right click the headings of the columns, Figure 14.

Figure 14: Adding a column in DT v 0.61

To add a column in Data Track version 0.71, the users could either right click as in v.0.61 or they could click the “add column” button as seen in Figure 10. In version 0.8 the “add column” button in the icon bar is used in the same manner as the button in v. 0.71, Figure 12. When the add column button was clicked in either DT v. 0.71 or v. 0.8, the list in Figure 15 pops up and the user can select which columns to add. When the column has been added the result would in all versions look similar to Figure 16 with differences in the GUI according to their version differences.

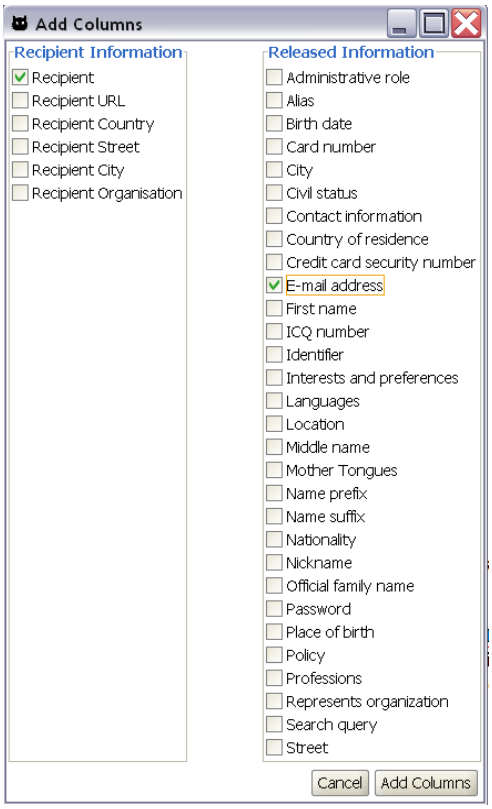

Figure 15: The Add Columns pop-up in DT v.0.8

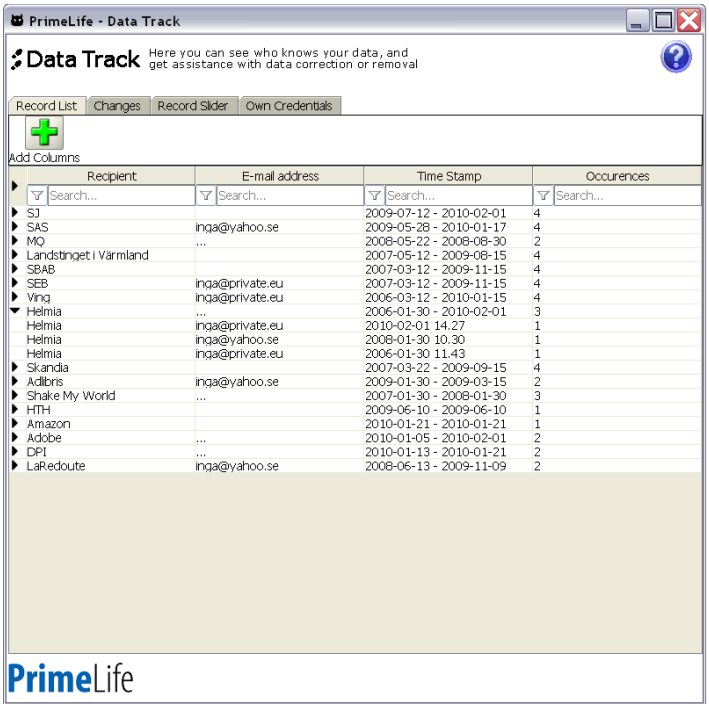

Figure 16: Record List with “E-mail address” column added and “Hemlia” summary row expanded in v.0.8.

When the “E-mail address” column has been added the users then expand the “Helmia” summary row to see all transactions to “Helmia”, Figure 16. Here the users see that information has been sent to “Helmia” three times but only two of these contain the e-mail address inga@private.eu.

Task 3 - You remember having sent some information to Adlibris in the afternoon January 30th last year, but you can't recall what delivery address you specified. Try to find it and write down the information you’ve sent.

To solve this task the users open the summary card for “Adlibris”, Figure 17, and look at the rows with a Time Stamp at 2009-01-30 to see what data that was transferred at that date.

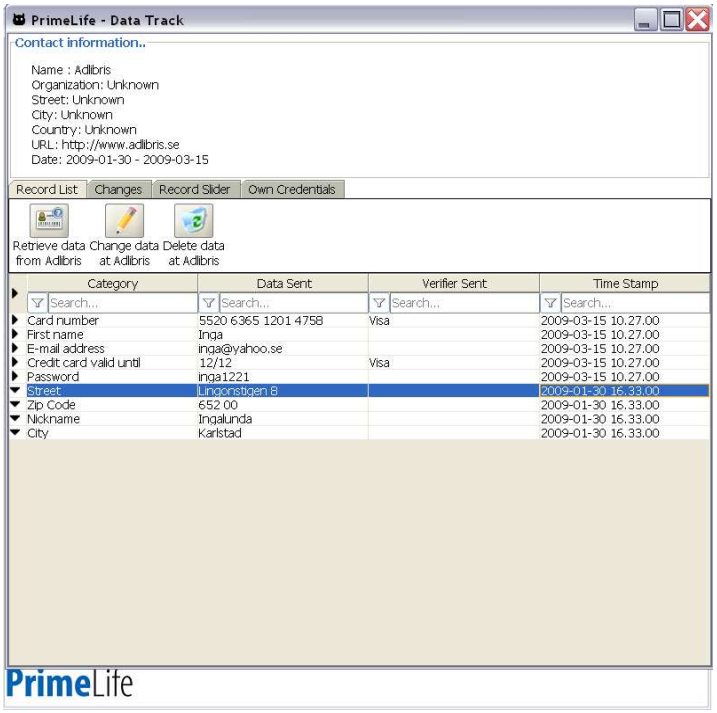

Figure 17: Summary Card for “Adlibris” with the first transaction at 2009-01-30 selected v.0.8.

Task 4 - How many times have you sent information to Adlibris?

This task is solved by looking at the Record List, Figure 12, where the users see that the column “Occurrences” for the row “Adlibris” says “2”.

Task 5 - Who was the first recipient you sent information to using your new software?

To solve this task the user clicks the name field in the column for “Time Stamp” so that the columns are ordered by date, Figure 18. The top row then says “Helmia”, which is the first recipient that the user sent information to.

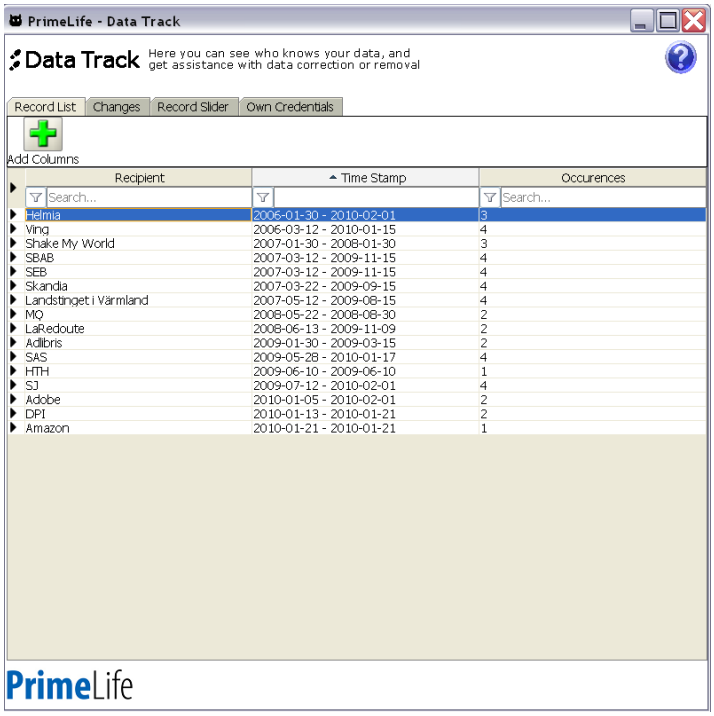

Figure 18: Record List sorted after dates v.0.8.

Task 6 - What information does the recipient have about you?

When the user opens the Summary Card for “Helmia”, Figure 19 is shown and the user can see which information that has been sent to “Helmia”.

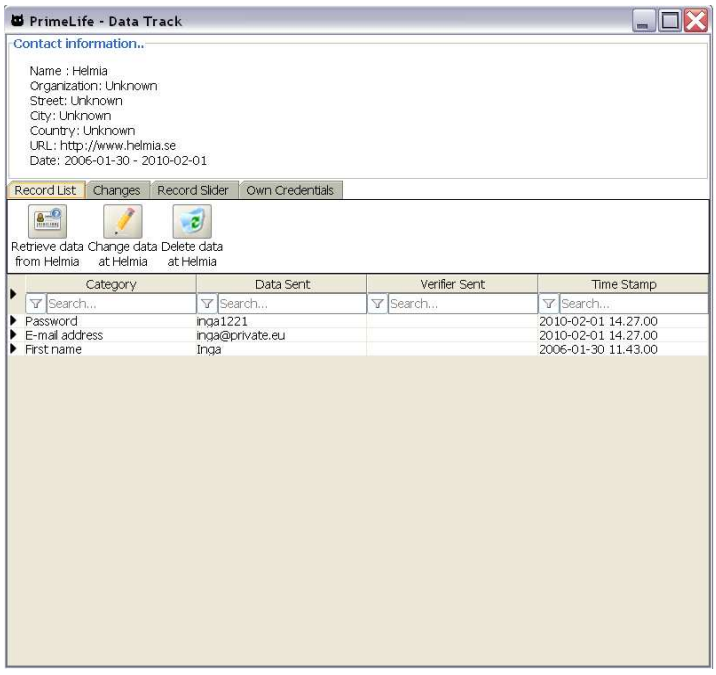

Figure 19: Summary Card for “Helmia” v.0.8.

Task 7 - Before you started using PrimeLife you registered at DPI with the alias ”Trulls”. After you started using PrimeLife you changed your alias to ”Snapshot”, but DPI still welcomes you as Trulls on their website. (The fact is that you've tried to change it twice already on their website). Change the information at DPI using your PrimeLife-system.

How did you complete the task?

To complete this task, the user needs to retrieve the remotely stored data from “DPI”. To do so in versions 0.61 and 0.71, the user had to locate the “Retrieve all remotely stored data” button at the bottom of the GUI, Figure 20. In Data Track version 0.8 the users can use the “icon bar” at the top where the button and text “Retrieve data from DPI” is shown, Figure 21.

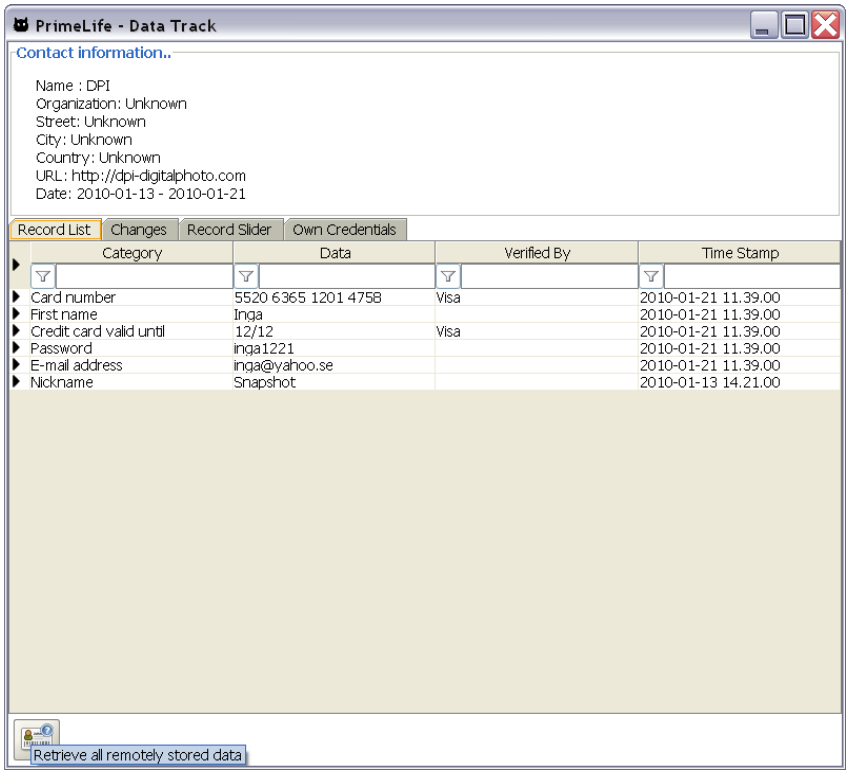

Figure 20: Summary Card for “DPI” DT v.0.61 and v.0.71.

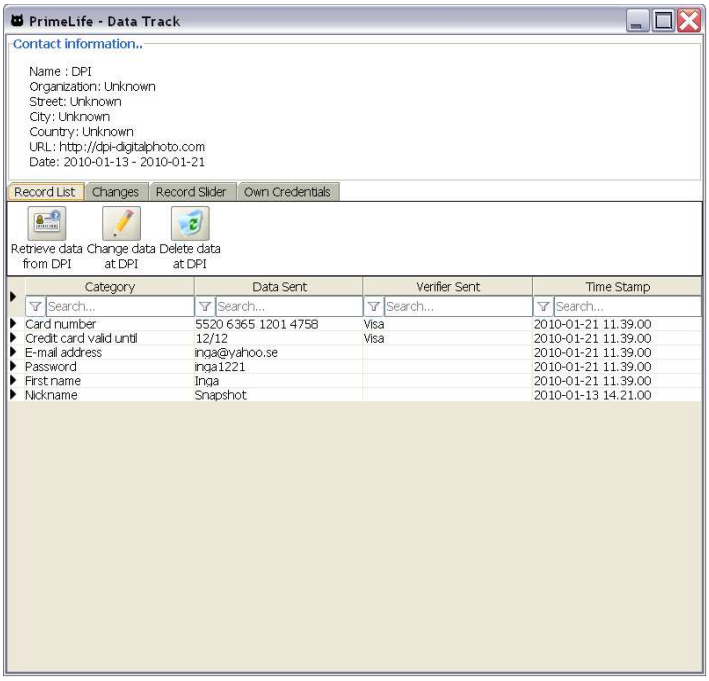

Figure 21: Summary Card for “DPI” v.0.8.

The data are then retrieved, Figure 22, and shown, Figure 23. In Figure 23 the users see the data remotely stored and more especially that the nickname stored by “DPI” is “Trulls” while the nickname sent is “Snapshot”.

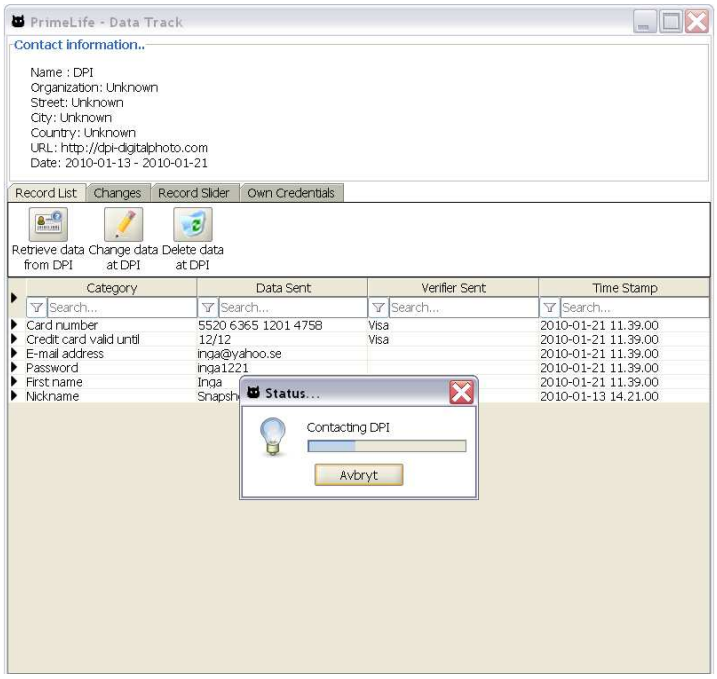

Figure 22: Retrieving data from “DPI” v.0.8.

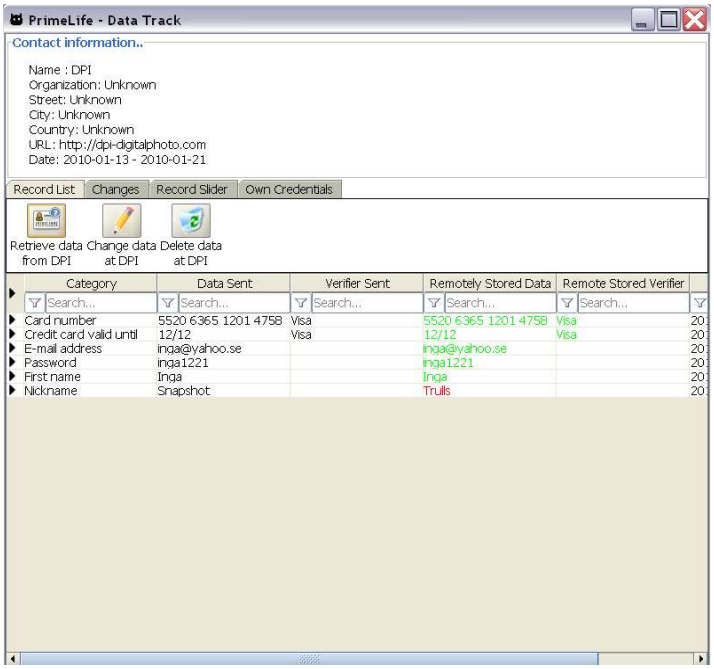

Figure 23: Remotely Stored Data at “DPI”

In version 0.61 and 0.71 the users had to right click the “Nickname” row to get a menu, Figure 24, where they can choose to change remotely stored data. In 0.71 double clicking was also implemented to open the “Change Remotely Stored Value…” pop-up. In Data Track v.0.8 the users can still right click to get the menu for actions to perform, but they can also select the “Nickname” row and then click the “Change data at DPI” button in the “icon bar”.

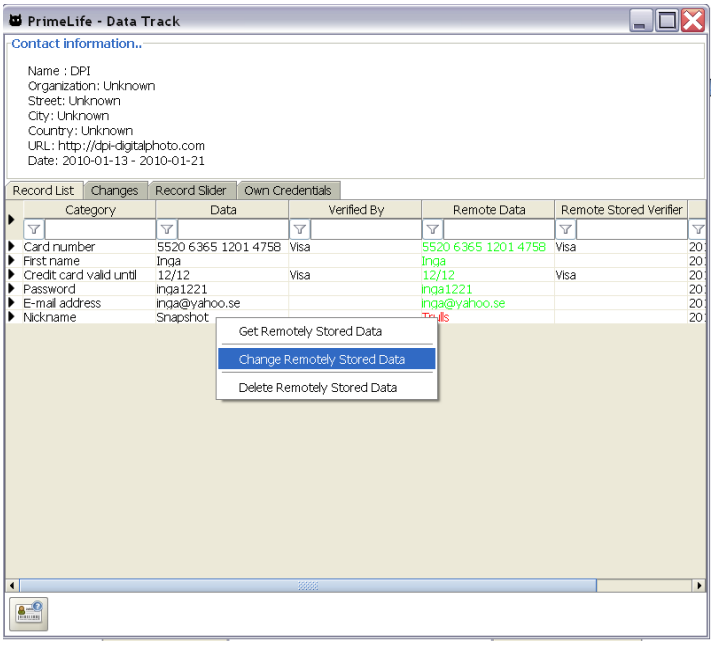

Figure 24: Right clicking to change Remotely Stored Data in DT v. 0.61 and 0.71.

If one of these actions is performed, the interaction in Figure 25 is shown where the nickname “Snapshot” is written. To change the nickname the user clicks “OK” and the information is sent to “DPI” in the same manner as if the data were retrieved from “DPI”, Figure 22. The new data are then updated and displayed, Figure 26.

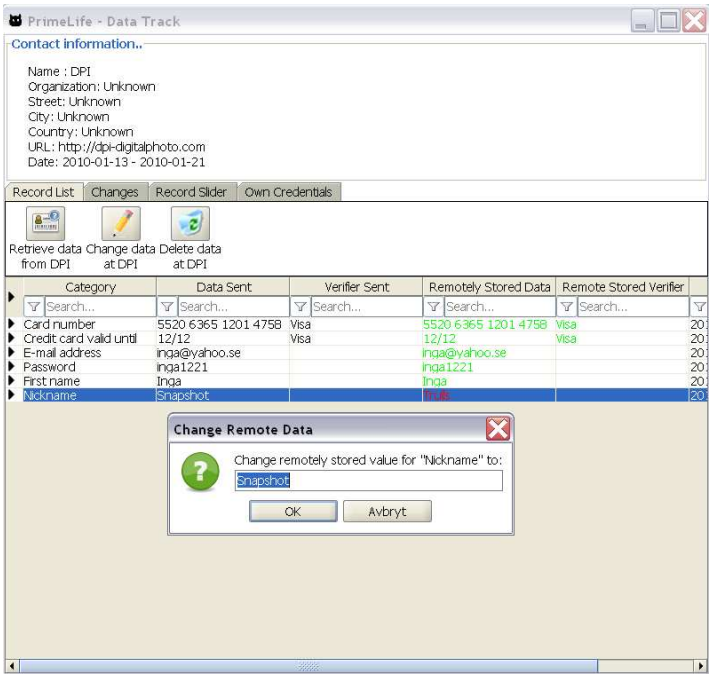

Figure 25: Change remotely stored value for “Nickname” at “DPI”

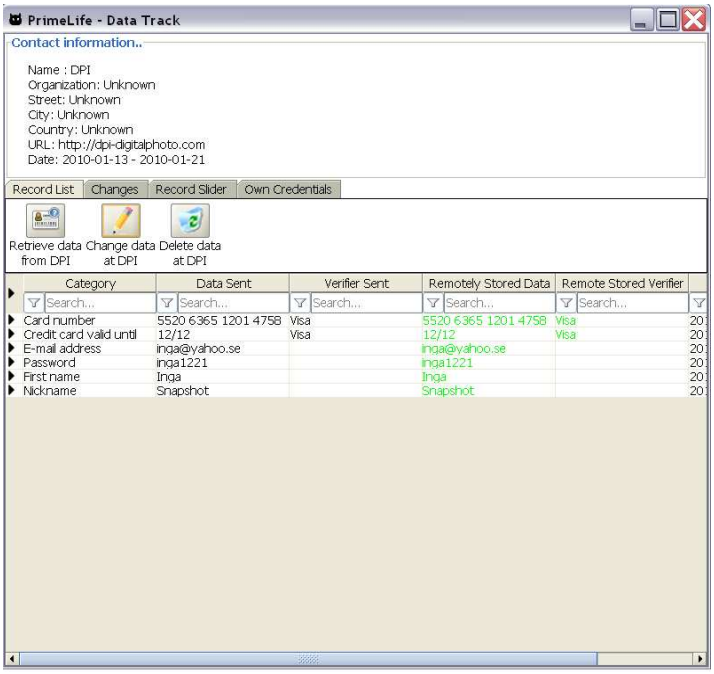

Figure 26: Remotely stored data changed at “DPI”

Task 8 - What happened after you made the change in task 7?

The correct answer here is simply to describe what happened in task 7.

Task 9 - Have you ever disclosed any information to a company named BEIFA?

In the Record List the users have to search for the recipient “BEIFA” to complete this task, Figure 27. This makes it obvious that there is no information disclosed to this particular company.

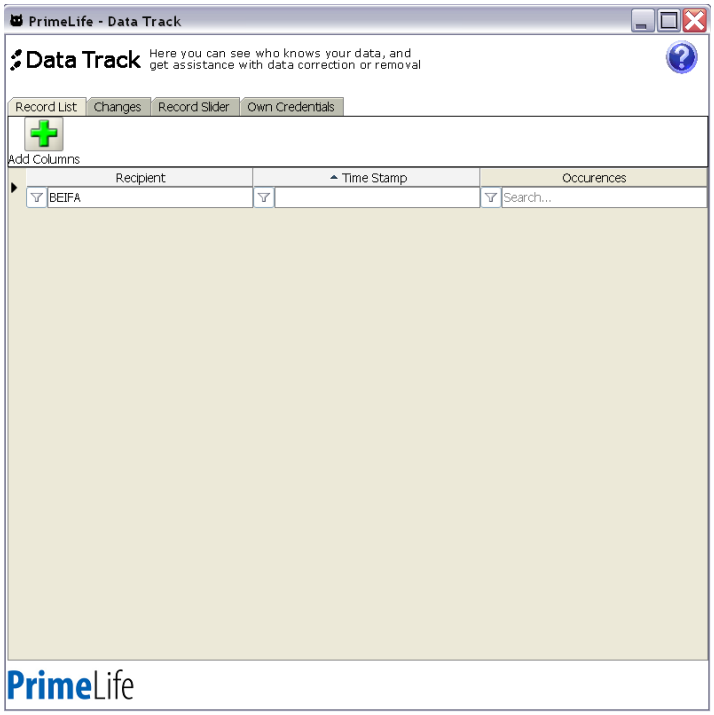

Figure 27: Record List search for “BEIFA”

Task 10 - It is summer and you've ordered a new kitchen from HTH to your summer place in Ångermanland. You realize in retrospect that you've sent the wrong postal code for the address to your summer place in the PrimeLife-system. Because it takes several weeks for the kitchen to be delivered you assume you still have time to make changes before the actual delivery takes place. Correct postal code is 873 91. Change it!

How did you complete the task?

To complete this task the user has to open the summary card for “HTH” and then find the “Delivery Zip Code”, not the “Zip Code”, Figure 28. The user can, as discussed in task 7, change the zip code by right clicking, double clicking or using the icon bar option “Change data at HTH”. The data will be sent, updated and shown as was already shown and discussed for task 7.

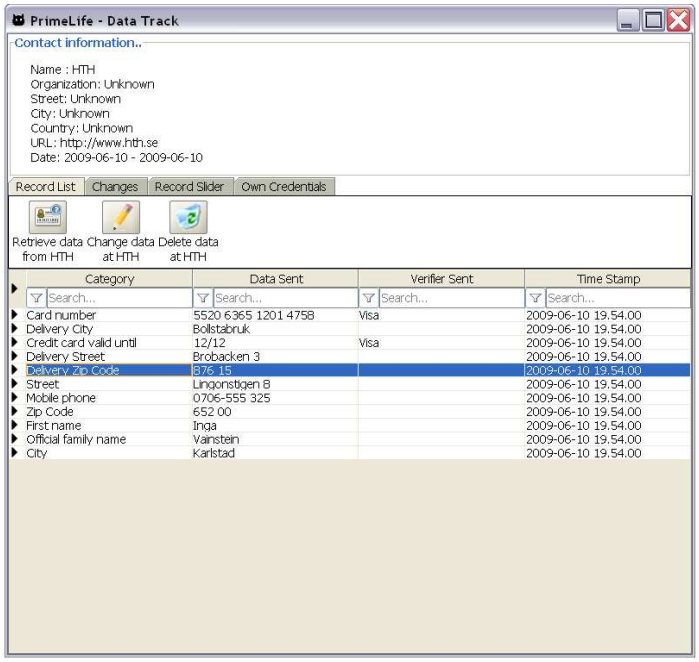

Figure 28: Summary Card for "HTH" showing the "Delivery Zip Code", v.0.8.

Task 11 - What happened when you made the change in task 10?

The correct answer here is simply to describe what happened in task 10.

Task 12 - You have shared your e-mail address "inga@yahoo.se" on several occasions, now you want to find out who has received it from you.

As shown and discussed in Task 2, the users first have to add the column "E-mail address". After this the users searched for the e-mail address "inga@yahoo.se" in the new column. If they have not expanded all rows only three recipients will be shown, Figure 29. The users will see only those companies who have received only the e-mail address "inga@yahoo.se", companies who have received more than one e-mail address will not be shown here. To show all transactions to all companies the user first has to expand all rows and then search for "inga@yahoo.se", Figure 30. The expansion is done by clicking the black arrow to the left of the table headings. The companies that have received the e-mail address can then be seen in the list.

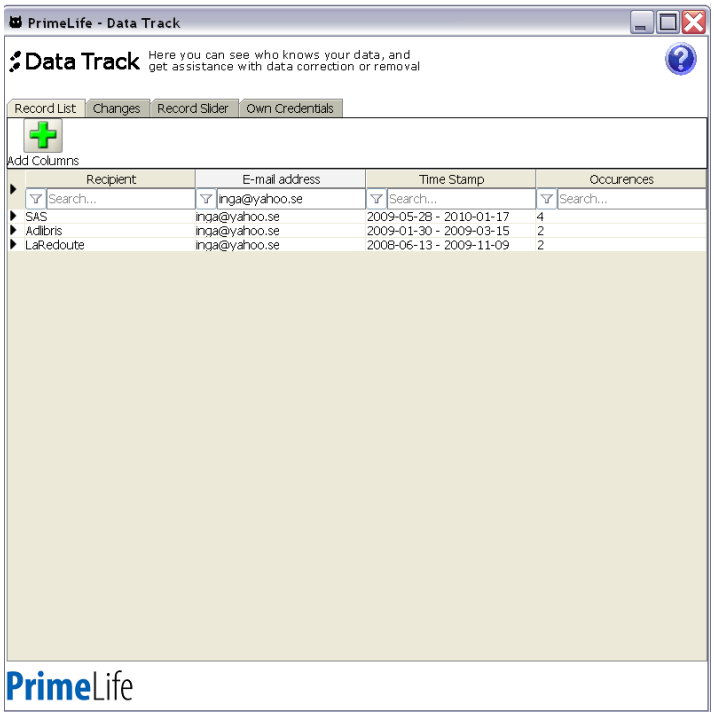

Figure 29: Record List search for e-mail address without rows expanded, v.0.8.

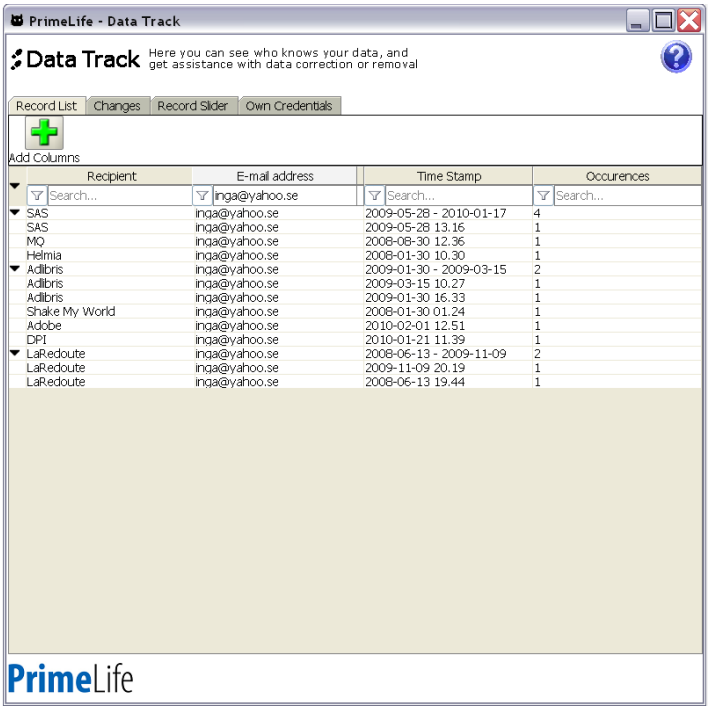

Figure 30: Record List search for e-mail address with all rows expanded, v.0.8.

Task 13 - Deny ”Shake My World” to use your e-mail address (you discovered that you used the same e-mail address on another online chat and don't want to risk getting recognized).

First the user must open the summary card for “Shake My World” and then select the row for E-mail address. To deny “Shake My World” to use the e-mail address the user has to delete it and to do so the user can either right-click the row, in versions 0.61 and 0.71, or select it and then click the “Delete data at Shake My World”, in version 0.8, Figure 31. The data will be updated at “Shake My World” and shown as in Figure 32.

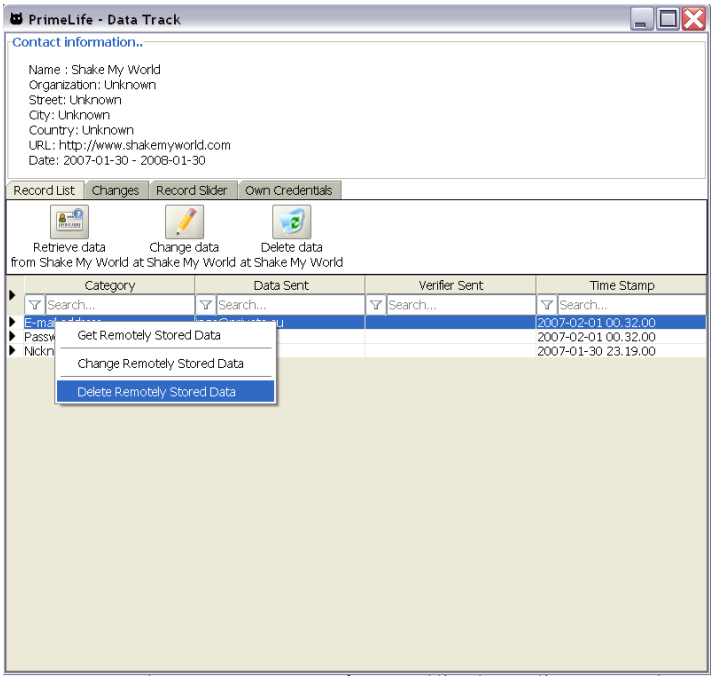

Figure 31: Summary Card for “Shake My World”

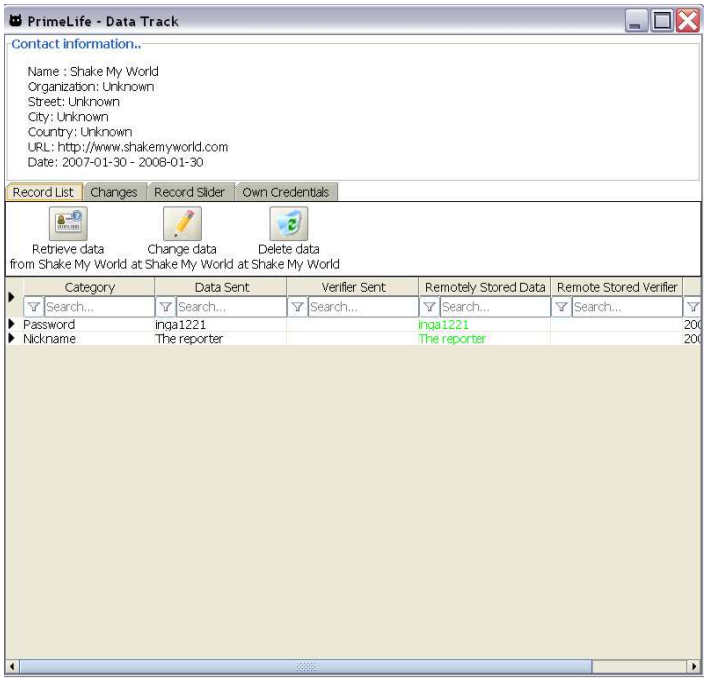

Figure 32: Summary Card for “Shake My World” after e-mail addresses has been deleted.

Task 14 - You recently received an e-mail from MQ where they greet you as Inga Vainstein but you cannot remember giving this information to them. Is it true that MQ have stored more information about you than you have sent?

This question was added in the second and third round of tests.

To fully complete this task the user has to first retrieve all data from “MQ”. When this is done, Figure 33, the user can see that “MQ” has stored the “Official family name” while this never has been sent to them.

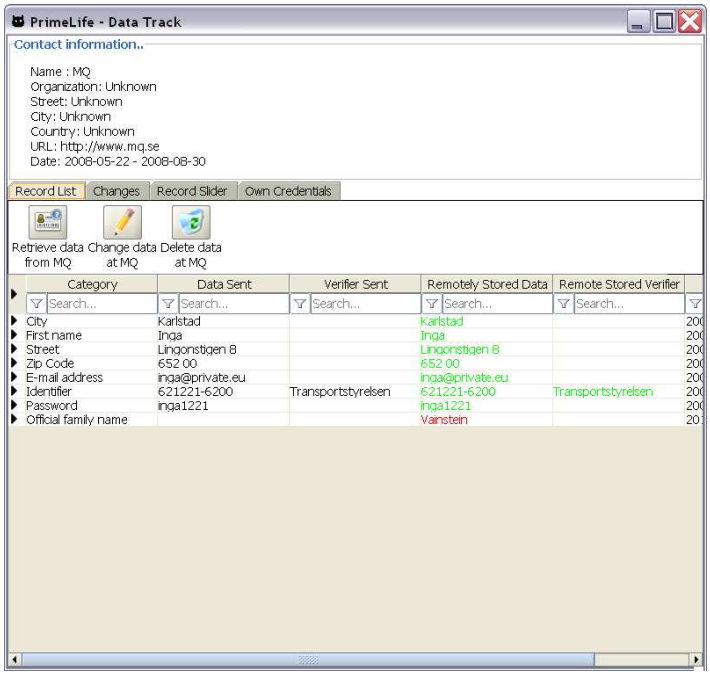

Figure 33: Summary Card with Remotely Stored Data Retrieved, v.0.8.

Task 15 - Did you send information to any recipient on 2009-06-27 and/or 2009-06-28?

This task is solved by searching for the dates 2009-06-27 and 2009-06-28 in the Record List column “Time Stamp”. It is then easy to see that there has not been sent any information at these particular dates.

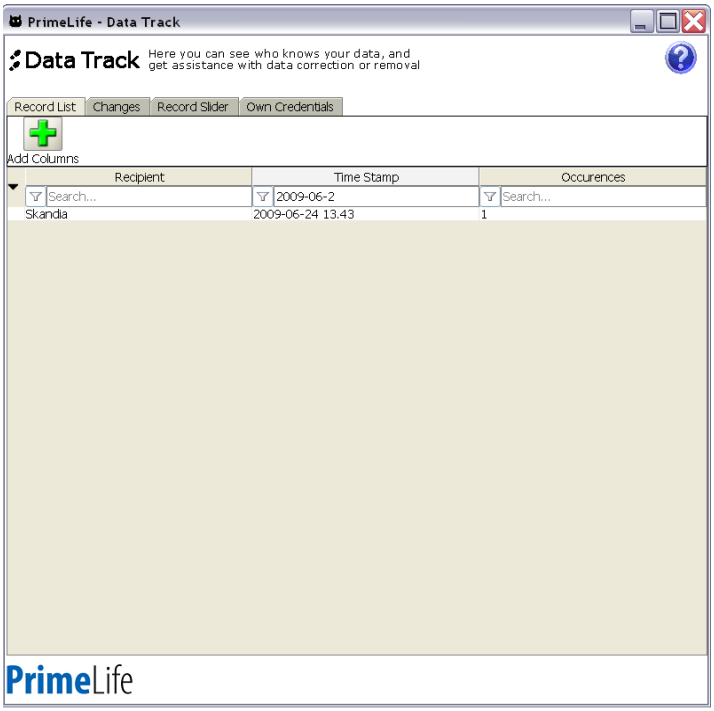

Figure 34: Record List search for dates with all rows expanded, v.0.8.

4.2 Test results

4.2.1 Task 1 - Information sent to Amazon

During the three rounds of tests, only 5 of the 48 participants understood that their name was verified by 'Transportstyrelsen' and 2 of the participants thought that information regarding their name was being sent to 'Transportstyrelsen' instead of Amazon.

During post-test discussions all participants understood the concept of verifiers indicating that the idea is to novel too be solved by an intuitive UI and that one might expect a need for education.

4.2.2 Task 2 - Number of times "Helmia" got the e-mail "inga@private.eu"

In total, 26 of 48 participants completed the task correctly, 8 of the participants were lacking information and 14 adding information. The main reason for lacking information was the fact that participants did not understand that they were viewing the summary line and hence did not expand the table.The main reason for adding information was that participants included the summary line as an entry. Thus, the majority of errors stemmed from participants not comprehending the design of the table.

4.2.3 Task 3 - Retrieving the delivery address from "Adlibris"

All in all 41 out of 48 participants completed this task correctly. The participants who did not do so basically misunderstood the question and either did not state the full address of Adlibris or responded with extraneous information.

4.2.4 Task 4 – Number of times “Adlibris” was given information

In total 42 of 47 (1 missed the question) participants completed the task correctly. The five participants that erred counted the summary row as an occurrence.

4.2.5 Task 5 – First recipient of information

In total 42 of 48 participants completed the task correctly while the rest read the table incorrectly. The main reason for errors seems to be that the participants did not sort the table but rather looked through it for the earliest date.

4.2.6 Task 6 - Information given to the recipient in previous task

In total 41 of 48 participants answered correct (although five of these looked at the wrong company due to being erroneous in task 5). The seven that erred all based their answer on the first transaction card (which they found in task 5) and did not look at the summary of all transactions to the recipient. This error might stem both from participants’ not understanding the difference between a summary and transaction card but they might also have misinterpreted the question and deliberately looked for the information sent during the first transaction.

4.2.7 Task 7 – How to update information via the summary card 1 (nickname)

This task was changed somewhat between test one and tests two and three. The reason for the change was that although the participants answered correctly the test leader suspected that the participants got it right by mistake. In total 11 of 32 completed the task correctly, i.e. they retrieved remotely stored data and changed it at the service side. The majority of the errors come from not retrieving remotely stored data but rather just changing or deleting the data on the client side.

4.2.8 Task 8 - What happened after you made the change in task 7

The objective of this task was to further investigate the participant’s perception of task 7. The results show that out of the 20 participants who understood that they had changed the nickname at the service side, eight had done so by mistake, i.e. by just clicking change without actually knowing what data were stored remotely.

4.2.9 Task 9 – Information sent to “BEIFA”

All 48 participants completed this test correctly.

4.2.10 Task 10 – How to update information via the summary card 2 (postal code)

All 32 participants of test rounds two and three completed this task correctly (it was not included in test one).

4.2.11 Task 11 – What happened in task 10

47 participants completed this task correctly (one read on the wrong line).

4.2.12 Task 12 – Who has received the e-mail address “inga@yahoo.se”

None of the participants answered this question in the easiest way which was to add a column and searching that column while all rows are expanded. However, 7 participants completed the task correctly by opening all summary cards and manually counting the occurrences. In the first round of tests all but one added the e-mail column (this feature had been shown in the introductory film) but none expanded all rows. Thus this task shows that both the add column feature and the table expansion features are difficult to comprehend.

4.2.13 Task 13 – Deny “Shake My World” to use the e-mail “inga@private.eu”

In total, 43 out of 48 participants completed the task correctly. The five that did not solve the task either did not find the e-mail address or did not dare to delete data from the server side.

4.2.14 Task 14 – Family name not sent to MQ

This test was included in rounds two and three. Of the 32 participants 13 completed the task correctly. The errors basically stemmed from the fact that the participants only compared the information in the task description with the sent data deduced that MQ must have retrieved data from an additional source.

4.2.15 Task 15 – Information sent on 2009-06-27 and/or 2009-06-28

All participants completed this question correctly.

4.2.16 Pre- and Post Data Track Credential selection

In the third test round the users were instructed to use a credential selector to purchase a book from Amazon.com and describe what data they had sent to Amazon before they used the Data Track. After they had tested the Data Track they were asked to re-evaluate their initial response to what data they had sent. The results show that 7 of 15 users understood what data they sent before they used the Data Track and an additional three got it when they were allowed to re-evaluate their answer. The majority of errors where based on the users’ current understanding on what is needed to perform a transaction and how data-minimization technologies work.

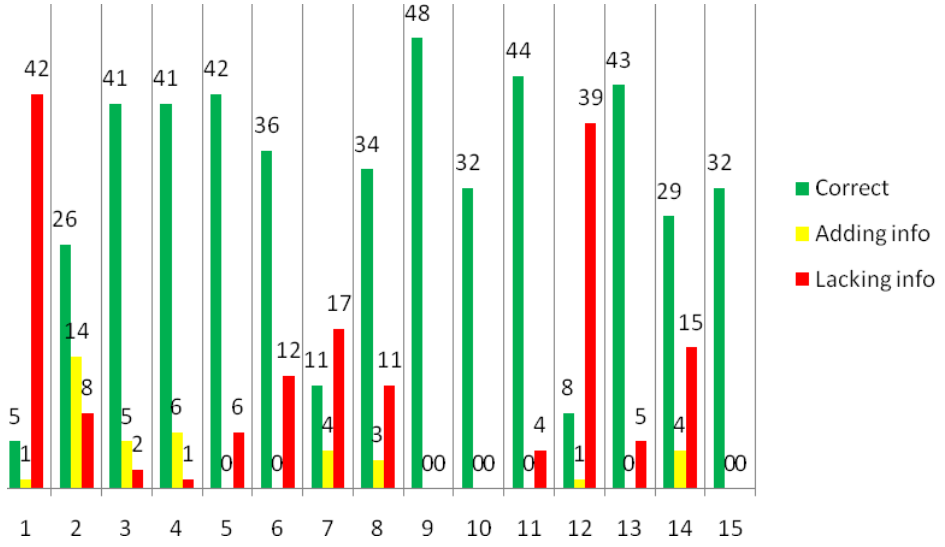

Figure 35: The diagram shown above illustrates the answers given by the participants related to whether or not they completed the task correctly, added information or gave less information than the correct answer required.

4.3 Conclusions

On a general level, the results of the usability tests show that with some exceptions users have little trouble navigating the Data Track and finding information that is stored locally. Especially noteworthy is the use of the summary card which all users understood correctly and the table search function which were also widely understood. The users' problems with the Data Track can be divided into two areas, namely UI problems and mental model problems.

In regards to UI problems, the main issue is the summary rows in the tables. The idea of the summary row is to show that the user has sent information to a given recipient. However, the problem is that users often do not understand that this is a summarizing heading of possibly multiple attributes and that only the last value is being shown. This results in users not expanding the row and thus missing a lot of information that has been sent to the recipient. Quite the opposite has also occurred, namely that users have interpreted the summary row as a separate transaction making them overestimate the amount of data they have sent to the recipient.

In regards to issues based on users' mental models, the key problem is that users often do not distinguish between service and client side. This results in users not retrieving data from the service side in order to verify what information they have stored. Thus, tasks where the users can see the incorrect data locally have been satisfactory solved, while tasks that depend on users retrieving remotely stored data have been more difficult.

Lastly, the combined tests did not show any reliable effect on users' understanding of the Data Track. However, three out of eight participants who overestimated the amount of data they had sent to Amazon with the Credential Selector, actually understood what they had sent after they had used the Data Track. Thus, using applications such as the Data Track and Credential Selector in combination helps users get into the right mental model.

In sum, the results show that users have little trouble using most parts of the Data Track that concern locally stored data. In regards to locally stored data, it is mainly parts of the table UI that needs to be improved. A more challenging issue is conveying to the users what is happening on the client side vs. what is happening on the service side.

Chapter 5

Usability Tests at CURE

In order to further investigate the issues reported in Chapter 4, a follow-up usability study was performed by CURE in CURE's Experience Labs in Vienna. This chapter describes the qualitative results of the Data Track usability laboratory evaluations such as general usability findings, provides suggestions for improvement, and concludes with a summary of the experiences made during the evaluations.

5.1 Test setup

The test took place with 10 participants, 7 male, 3 female. The oldest participant was 56, the youngest 21; the average age was 33.8 years. All participants have been registered to a web shop or an online community privately, so they have already disclosed private data in the web. Hence they are the target group for Data Track.

The Data Track version 0.8 was used throughout the entire test. The tasks were the same as described in Chapter 4. It should be noted that in seven of the ten tests it was not possible to change data online since there was an exception error that the server wasn't found. So there was no possibility to conduct Task 8 and Task 11. In Task 7 and Task 11 we looked if end-users interact correctly with the system. When this happened, the tasks were stopped as no feedback from the system was provided.

5.2 Usability findings of the test

In general, users had no problems solving the majority of the tasks, but some of them were solved by using inefficient strategies like counting items manually (e.g. e-mail occurrences) rather than according to the strategies provided by the GUI (e.g. filtering for e-mail occurrences).

Only one out of ten participants used the help function in the Data Track, even so, offering help is a very important part of software.

Another important feature, which should be implemented in future versions for user support is tooltips. Tooltips give users hints what will happen if they, for instance, click a button. This is especially important when the interactive elements of the application are ambiguous or if the user is new to the task at hand.

5.2.1 Time Sorting

One technical finding was that the date format in the Data Track test at Karlstad University and at CURE was different even though v0.8 of the Data Track was used at both locations. This discrepancy is visible in Figure 16 and Figure 36. We attribute this to the JAVA localization mechanism, which should be used consistently to solve the inconsistent date appearance. Within the application the notation should be used as common with the respective cultural sphere.

Since the date format was dd-mm-yy and the sorting was alphanumerical the column was sorted by day (c.f. Figure 36). Because of this sorting problem all tasks, where users had to deal with data sorting, where difficult to solve. For example, in Task 5 the users had to look through the whole list to find the correct solution. From a usability point of view this is no user-friendly solution. The solution is the use of debugging software to find out why the date format was displayed different. Especially when thinking of a real-life Data Track the numbers of entries will be enormous so the "manual" solutions performed by users are not applicable in practice.

An expert notice is that the date format in the record list and the record slider is inconsistent (due to the mentioned localization mechanism). From a usability point of view it is necessary to provide consistency within a User Interface [Nielsen 05].

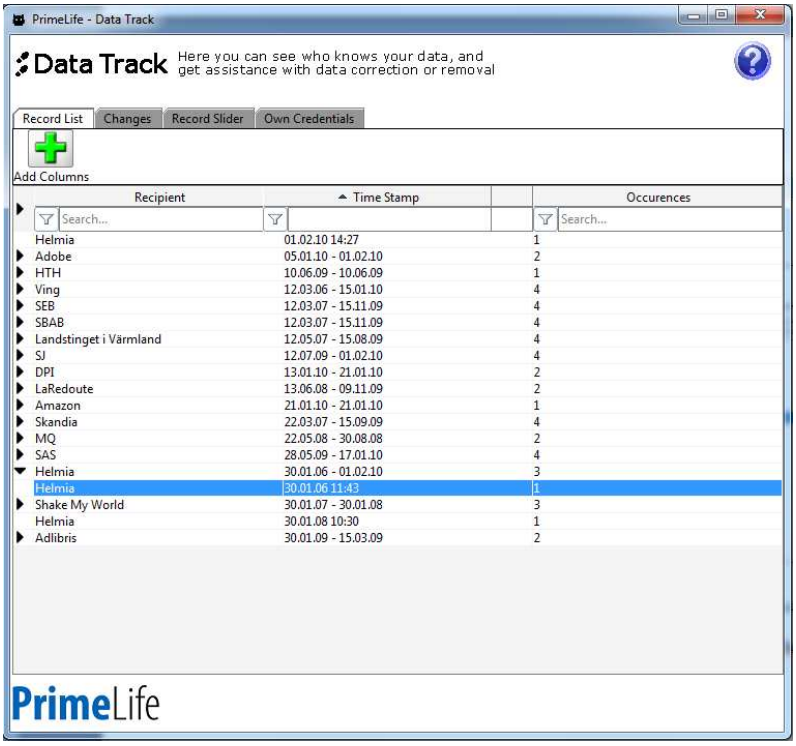

Figure 36: Record List with TimeStamp

5.2.2 Add Columns

The main problem was that users did not recognize the icon functionality as the labeling is too un-concrete and tooltips are missing. The results of the eye tracking analysis show that during the test users looked at the "Add Columns" Icon but did not press it. This might be due to the toolbar approach, which does not seem to be recognized as such. It seems to be a gestalt problem that the

users do not think the big button belongs to the table headers. A suggestion from a participant was that the adding of new columns should look similar to the functionality for adding columns in Microsoft Outlook. This means an icon on the right of the columns for personalizing the table.

Another observation was that just one out of ten participants used the right click on the table header for adding new columns. It took the users quite some time to find “E-mail address” in the alphabetically sorted list of the “Add Columns” button and it took them even longer in the unsorted right-click list. A recommendation is therefore to sort the right-click list alphabetically. Even better would be a more fine-grained classification inside “Released Information”.

These two described problems were also highlighted in Task 12. Most of the participants solved the task by looking through each card in the record list. Since the Data Track shall store a lifelong history of data this way will not be efficient when more data are in the track.

The results show that it is necessary to use a more meaningful icon and labeling. Also the position of the icon should be re-thought.

One possible solution is to use a ‘+’ button next to the last visible column on the right side.

5.2.3 Calendar

A very severe finding is that the calendar in the record slider view is currently displayed in an unusable position when working in maximized mode (c.f. Figure 37). Users have to drag and drop the window to a usable position. This is a very important problem concerning the efficient use of the program. This can be solved by letting the calendar pop-up.

Another problem that was observed was that the “Apply” and “OK” button of the calendar confused the participants. Since both buttons provide the same functionality, from a usability point of view, the “Apply” Button is unnecessary and just confusing for users.

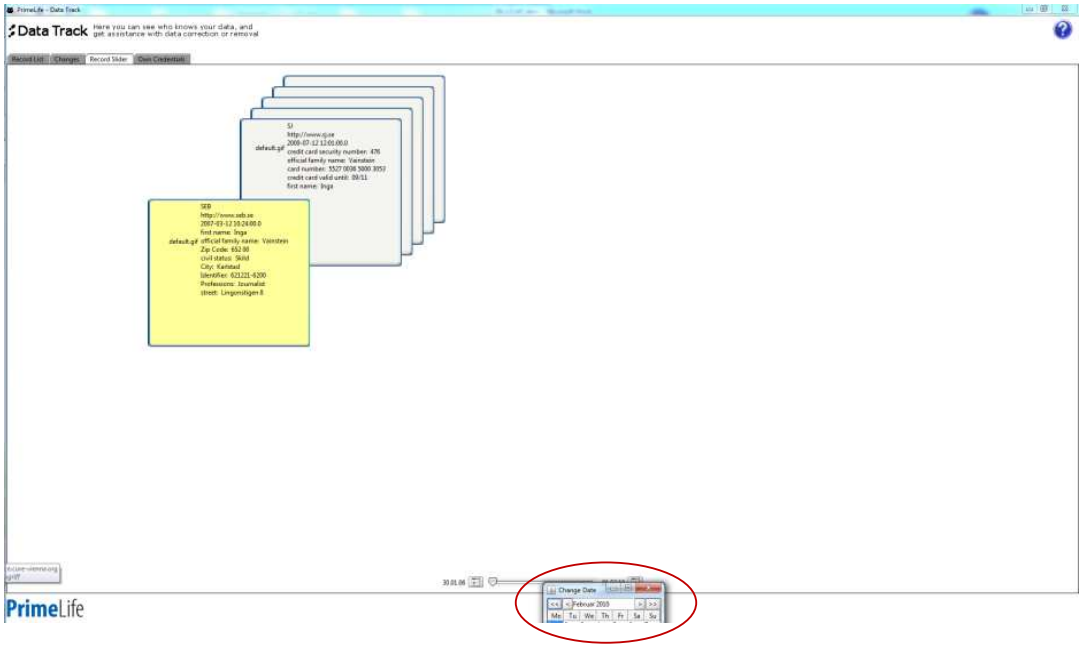

Figure 37: Maximized Window with cut off calendar (red ellipse)

5.2.4 Interactive Table

A very positive feature of the interactive tables is that users can modify the columns by making a right-click on the table header. This was only recognized by one participant but in general it works great (besides the sorting of the elements in the menu as described above).

Problems occurred with the fold-out mechanism (the arrows) because participants often did not recognize the "expand" functionality. A comment from a participant concerning this problem was that MS Excel uses an arrow to indicate the actual line. This comment suggests an external consistency problem with already existing software. Maybe using '+' and '-', which are known from trees, would work better here. Furthermore the general fold-out arrow is only present in the record list but not in the changes window; an inconsistency which should be solved.

Most of the participants also had problems recognizing the filter symbol (Figure 38). One participant suggests using glasses instead.

Figure 38: Filter Symbol

An expert notice is that the filter symbol sorts the column alphabetically. It provides the same function as a click on the table header. We think it is not necessary to provide the same feature in two different ways. Experience from other CURE projects has shown that the empty text field provides enough affordance for the users.

Furthermore two users want a "general search" or "extended search" for the interactive tables. One person noted that she would prefer to add queries like "display all entries before 01-01-2009".

5.2.5 Retrieve Data

Most of the participants clicked on the "retrieve data" button in the summary-card view before starting another interaction with the summary card. Our assumption is that they thought they had to fetch it before working with it. We suggest re-labeling the button more concrete ("Retrieve data" seems to be too abstract).

5.2.6 Pop-Up Info-Window

In general, users had a hard time understanding two similar looking screens – they had problems distinguishing between the summary card view and the single entry view. Some of them tried to edit data in the single entry view, which is not possible. From a usability point of view, users should be able to manipulate every data set directly. If necessary, give feedback that this will change all entries for this receiver.

During preparation of the evaluation we noticed that right click in table headers works on MacOS X 10.6.3 and on Windows, but in the pop-ups like "change data" the right-click on MacOS X 10.6.3 does not work.

5.2.7 Labeling

Users tended to change the 'address' instead 'shipping address'. 'Address' is before "shipping address' with some elements between. To be more robust against this error we suggest grouping them together.

Another problem was that users tend to change the wrong zip-code when asked to change the 'delivery zip-code'. This traces back to the gestalt-theory. Grouping similar items like 'zip-code' and 'delivery zip code' might help.

Furthermore there are some labels that were unclear to the participants:

- "Time Stamp" is also used for "Time Frames". This was very confusing for the participants.
- The "Summary" button in the single entry view is not self-explanatory. Users are not sure what will happen if they press this button.
- Same for the "Privacy Policy" button. One participant asked where to get the privacy policy from the given domain after he saw the button. We assume that the participants thought that the button shows the privacy policy of the Data Track. So a more meaningful label will guard against misunderstandings – like "To Privacy Policy from Amazon.com".
- "Occurrences" should be renamed. Most of our participants did not understand / know the word. Some of them asked for a translation of the word, three tried to find the e-mail address in the occurrences. Please note that the participants were Austrian and no English native speaker, but all of them were able to speak English. We think that "Number of Visits" will be more understandable by users with a non-English mother tongue.

5.2.8 Record Slider

Even though there was an exploratory task at the beginning where most users have seen the record slider it was not much used. Most of the problems occurred because users tried direct manipulation at the record cards and did not use the slider at the bottom or they have not been aware of it.

Half of our users tried direct manipulation at the record cards to navigate through the cards. Another user tried to double click the cards to change data. Both problems show that the record cards lead the user into an inefficient interaction. We assume direct manipulation must be implemented 100% if this view ought to work.

Another problem is that two users thought that a movement with the record slider displays the next three cards and were not aware that a card from the background comes to the foreground. Here it is necessary to provide some feedback for the users. This feedback should help to present the interaction in an understandable way.

Apple's "cover flow" mechanism lets users drag the cards, then the cards gently move to the place in the center; in the record slider the cards do not really move but it looks like content is exchanged. We assume that the missing user experience from the movement and the missing direct manipulation (click-and-drag on the cards) are the reason why the record slider was not successful during the evaluations.

Two participants also tended to use the record slider view to count the appearances of the mail address. Here the problem was that users were not aware of the possibility to add new columns in the table view as described "Add Columns" in the section.

5.3 Conclusions

The evaluations of the Data Track showed only 3 main areas of improvements:

1. Efficiency improvements in the workflow (calendar pop-up & summary vs. single information screens)
2. Sorting by time
3. Direct manipulation in record view

We recommend solving these main problems because they are so severe they could stop users interacting with the software (which means not using it anymore), which should be avoided.

The other findings should be implemented also to raise usability and user experience but priorities should be set to the three main issues above.

As the objective of an HCI evaluation is to criticize the user interface this chapter consists of a lot of UI bugs. We therefore clearly want to state that the overall usability of the Data Track is already very mature. When the three main improvements will have been implemented we see no reason for not publishing the Data Track to the real end-users then.

Chapter 6

Data Track for Social Communities: the Tagging Management System

When users publish information online, they are subject to laws and regulations making them liable for their actions. For example, a user assumes the role of a data controller under the Data Protection Directive 95/46/EC when she publishes personal data, e.g. in form of photos, about others and makes it publicly available to a broad audience (unless she does this for journalistic purposes). If the personal information is posted only to a closed group of friends, the "household exemption" according to Art.3 II EU Directive 95/46/EC applies with the consequence that the Data Protection Directive does not apply for this type of data processing in course of a "purely privacy activity" (see [Art.29 WP 09]). In either case, if the user obtains informed consent from the individuals concerned (the so-called data subjects) before publishing information about them, the user will not risk to have responsibilities from the Data Protection Directive but also from being liable under several other laws and regulations.

Tagging (or labeling) is the process of adding "meta-information" to an object usually by adding some form of identification or type information. The technique is used in a number of applications, e.g., in the security area it is used to control and restrict the flow of information and in the network area to create some versions of virtual private networks. Within the social network area tagging usually refers to the activity of annotating pictures (or rather individuals in pictures) with extra information. The information added is usually the name of the individual. It is clear that these activities if not done in a responsible and privacy respecting manner will lead (and are causing) privacy problems in social networks and not only for the participants of the network but also for individuals outside of the network. For the later it might also be hard or nearly impossible to act on the privacy breach without joining the social network (see [den Berg et al 10] for a detailed discussion on the privacy problems of social networks). However, if done in a responsible and privacy friendly way, e.g., by using pseudonyms and user control or trusted third parties it could be used to enable user consent and also to enable data subjects to keep track on information published about them.

A tagging management system could, for instance, help the user Frank Falk to tag persons (including Inga Vainstain) on photos (or any other resources with other personal data about Inga) that he wants to publish, to obtain Inga's consents, and to accept resources for publication for which consents by Inga (and possibly other data subjects) have been obtained. A request for consent, which is sent by the tagging management system to Inga, can in turn trigger an entry in

Inga's Data Track. Such an entry in Inga's Data Track documents that data about Inga are stored at a site under Frank's control with her consent (or that consent was requested, which she did not grant). This means that a future version of the Data Track would not only store records about the disclosure of data, which was directly obtained from the data subject, but also records of personal data that others published about the data subject with her consent (or even, as said above, records for publication requests to which the data subject did not agree, which can still be useful to store as proofs).

As mentioned above, such a tagging management system has to be implemented in a privacy-friendly manner. This means that its tags should include a minimal amount of personal data (e.g., there could be pseudonymous tags) and should not be visible to other social network users. Preferably the tagging system should also be under the control of the user and not controlled by the social network provider.

A first outline of such a tagging management system is given in this chapter. It is worth noting that the system currently does not force the user to tag pictures and thus pictures could still be published without consent. However, it gives the user the possibility to act responsibly and a way to do this in a user friendly and semi automatic fashion. Thus making it easier to behave in a privacy friendly manner and also reminding the user that the data that she uploads might be privacy invasive.

6.1 Overview of the proposed solution

For illustrating the proposed solution, assume that a resource, such as a picture or a document, is hosted by a data controller. The resource includes (personal) information about a number of data subjects, for example the resource is a picture showing a group of people. Information about which data subjects are included in a resource, is identified through the continuous process of tagging, where the user who wishes to publish the resource and *potentially* data subjects with access to the resource perform the tagging. The data controller runs a tagging management system, which facilitates the tagging and ultimately decides if a resource is published or not (see Figure 39 for an overview of the tagging system).

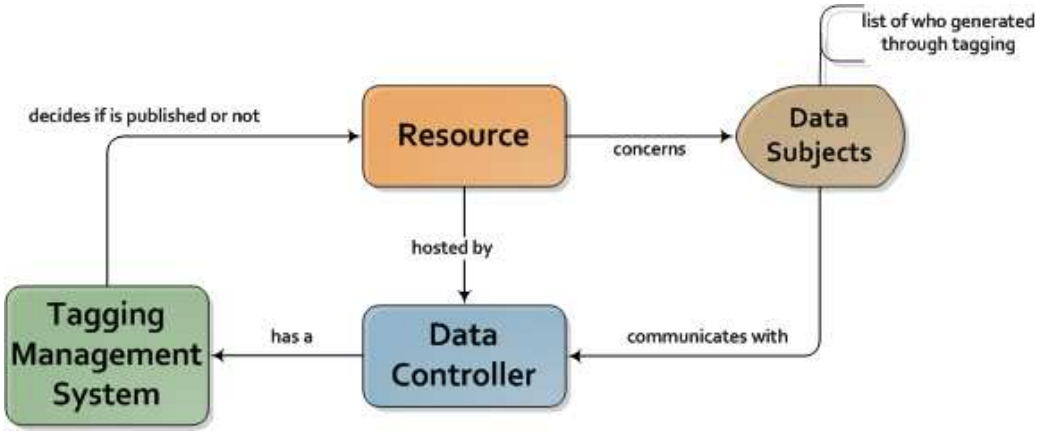

Figure 39: Conceptual overview of the Tagging Management System

The tagging management system should ensure that the data controller has obtained consent if needed before the resource is published.

Examples of tagging management functionality are:

- Answer a query asking if a resource can be published.

- Add a subject to resource.
- Remove a subject from a resource.
- Supply proof of consent.

6.2 An Example

Bellow follows a simple example to illustrate the functionality of the tagging management system:

1) A user uploads a picture, checking a box indicating that she wishes to obtain consent from all individuals on the picture before it is made public.

2) The system scans the picture trying to identify possible faces on the picture to tag. The purpose of the scan is not to identify individuals but rather to find areas in a picture that are possible faces. The idea here is to make it easier for the user to perform the tagging.

3) The user tags two out of three people in the picture.

4) The two identified data subjects are contacted and asked for consent. At this point, any request for the picture will be denied.

5) The two identified data subjects consent. At this point, since all identified data subjects have given consent, any request for the picture is allowed. If not all of the identified individuals give consent several actions are possible. The strictest one would be to deny the publication of the picture. Another variant would be to blur or "black out" the face of the individual who did not give his consent. We have chosen the latter and "black out" faces of non consenting individuals.

6) Bob, another user, tags the third person in the picture. If the strict version in point 5 is chosen this will cause any request for the picture to be denied until the newly identified person has also given consent. Otherwise the newly identified individual will be blured or "blacked out" until she has consented to the publication.

6.3 Status of the work

A prototype tag management system behaving in such a manner has been developed. However it is very much in its infancy and no user tests have been performed. The prototype is currently developed in php as a proof of concept and the plan is to develop a plug-in to the Clique social network or to develop a standalone module that can be interfaced by Clique through a plug-in. The idea is to also integrate functionality for storing and manage given consent for a user in the Data Track of the data subject thus making it possible for the user to get an overview of the pictures she consented to or which ones she received. We also believe that it is quite easy to extend the tagging system to any taggable data once the management system is in place thus making it possible to request and manage consent for a much wider range of personal data.

Chapter 7

Lifelong Data Track

While European societal values such as data protection and self-determination have been proven quite stable over the last decades, this is not true for information and communication technologies (ICT). ICT undergo changes all the time; today hardware or software systems are outdated after a few years. This also influences all kinds of identity management systems and their technological surrounding. In addition, the personal needs of the individual handling her identity management with supporting tools such as the Data Track will change over lifetime. PrimeLife Deliverable H1.3.5 gives an overview of requirements and concepts for identity management throughout one's lifetime [Storf et al. 09].

This chapter will sketch challenges for the Data Track in a lifelong setting and will describe what has to be considered if instruments such as the Data Track are used to support individuals in their privacy and identity management throughout life.

According to [Hansen et al. 08], three main categories play an important role and pose specific challenges to privacy and identity management throughout one's life:

1. privacy and identity management covering all areas of life
2. privacy and identity management covering the full lifespan
3. privacy and identity management covering all stages of life

The following sections elaborate on requirements for the Data Track to cope with the challenges of each of those categories.

Note that current approaches to privacy and identity management as well as the legislative view on personal data under the data protection regime base on data from a single individual and the individual's rights concerning these personal data. However, there could be necessity also to handle data with multiple persons concerned – for privacy reasons of each individual concerned or also for the sake of the group's privacy (this extended view on privacy was already introduced by Alan Westin in 1967 [Westin 67]). This will generate further questions to be tackled by the Data Track concept, as explained later.

7.1 Data Track covering all areas of life

Comprehensive privacy-enhancing identity management systems have the task to act as the communicational gateway to the outside world. The Data Track provides a key functionality for identity management. The communicational gateway to the outside world would require the Data Track – directly or by integrating other modules – to handle all digital partial identities in all digital communication in all areas of life: logging the relevant data, communicating the services' privacy policies, possibly giving advice to users on typical or allowed processes for the covered areas of life etc. The Data Track would have to integrate the data and the related communication from governmental eIDs, healthcards or SIMs of mobile phones. For instance, the Data Track should provide storage space for school reports or diploma certificates, and it also should inform users on who is allowed to request or demand access to those documents and how sensitive those data are [Hansen et al. 08]. In addition the users should be notified via the Data Track of irrevocable consequences even if they withdraw their consent later on.

Further the Data Track should be enabled to keep track of the data others reveal that may be part of the own partial identity. Examples are the declaration of friendship or knowing each other like in social networks [Hansen et al. 08]. It could also manage the user's consent for the various areas of life (see also chapter 6).

A major challenge for the Data Track is to give the user a comprehensive overview on her data disclosed in all areas of life, at best with showing linkages that other parties may establish even for pseudonymous data disclosed. It should support users in viewing specific areas of life only or getting the full picture (see also the next section). This is especially hard if the environment of the identity management system do not support the Data Track: How can data from the offline world be captured by the Data Track? What about sensor data in a ubiquitous computing setting? And if it was possible to capture all the data: What about scenarios of personal life in families or other relations where people don't want to have a communication log in the Data Tracks of the persons involved?

Probably not all users wish to have all the sketched functionality all the time, so there may be Data Tracks that offer more functionality than others. However, also Data Tracks with minimal functionality should be extensible by other modules. So if the Data Track does not directly support a certain function as described here, it should provide interfaces to other modules that may be integrated by the user.

7.2 Data Track covering the full lifespan

The instrument Data Track tackles the challenge of putting the user in a position to track which data she submitted to which data controller at what time. The Data Track has to handle huge amounts of data entries which cover the disclosure of personal data throughout one's life. This requires suitable data handling strategies so that important data entries are accessible when needed, that data which are not relevant in everyday life (e.g., relating to school attendance) are archived, that data which are not needed anymore can be deleted etc. [Clauß et al. 09]. Of course different people may have different ideas on which data entries are important for a certain context or which entries are not needed anymore. This should be configurable in a convenient way (e.g., by downloading standard settings that work for many people and applying individual changes to those settings). The Data Track should contain some functionality that prevents users from accidentally deleting data entries. In addition it could be combined with trustworthy backup systems. Still the Data Track should not overrule the autonomy of an authorized user to delete own data entries. If data formats change, old data entries would have to be migrated. Note that it

may not be possible to migrate one's data to new hardware and software systems, e.g., when data are bound to specific hardware for security reasons [Hansen et al. 08].

The Data Track with its database containing personal data and the transaction logs for a longer time period is a key component of the identity management system and therefore it is an attractive target for any kind of attacks. It is not a trivial task to maintain the necessary level of security (in particular confidentiality, integrity and availability) over a long time period. For achieving an appropriate level of security, there is the need of an ongoing security management process.

The aspect of maintaining long-term security also plays a role in the Data Track's component that informs its users about privacy and security breaches or in assessing one's privacy rights to access or rectify data.

7.3 Data Track covering all stages of life

A *stage of life* of an individual with respect to managing her privacy is a period of life in which her ability to do so remains between defined boundaries characterizing this stage of life [Storf et al. 2009]. Characterizing factors comprise the age, a familiar situation or specific activities. We focus on everything that has influence on the capabilities of the individual regarding privacy management. Every individual during her lifetime passes through one or more stages during which she is incapable of managing her privacy on her own. Such an incapability of managing one's privacy means not having the ability to sufficiently understand the consequences of data processing relevant to one's private sphere or to (re)act upon them appropriately. This is regularly the case in the phase of early childhood, and it can happen during lifetime, e.g., if the data subject lapses into a coma or if her capabilities have degrade significantly because of dementia.

Individuals may want to issue guidelines for others who deal with their personal data in periods in which they cannot be asked. This encompasses preparations for the case of emergency, e.g., lapsing into a coma, for the case of scheduled or unscheduled absence, or even for the case of death.

The design of Data Tracks should take into account that there may be defined situations in which other people should get access rights to all or some of the data. For examples, the Data Track could store instructions in case the person concerned is absent or cannot be consulted – including the case of death. This information shall only become accessible to others in the case of explicit clearance by the person concerned or in the case of death of the person concerned [Hansen et al. 10].

Usually, other persons or institutions support individuals who are incapable of managing their privacy on their own. For instance, parents are in charge of managing the privacy of their children until they can make the relevant decisions on their own. This could be solved by an individual Data Track for each child that is managed from the time of birth – or even earlier, as soon as there exists information such as entries to the maternity log – by the parents. These Data Tracks would be involved in all kinds of digital communication concerning the child. At a specific age the grown-up child could take over parts of the Data Track, and finally the young adult gets full access and full responsibility for the Data Track. The Data Track contains the documentation of all privacy-relevant transactions the parents have done on behalf of their children. From a technical point of view, the individual Data Tracks should be implemented as separated databases so that they can be switched from the parents' identity management system to the child's system.

Generalizing from the parents-kid scenario, the Data Track should support delegation. *Delegation* is a process whereby a *delegate* is authorized to act on behalf of a *person concerned* via a *mandate of authority*. The mandate of authority usually defines in particular (1) the scope of authority for the actions of a delegate on behalf of a person concerned and (2) when and under which conditions the delegate gets the *power of authority* to act on behalf of the person concerned. The

delegate shall only act on behalf of the person concerned if the delegate has the actual power of authority and if her action lies within the scope of authority [Hansen et al. 10].

The Data Track should handle "mandate certificates" that are issued to the delegate. At least the following procedures have to be specified: issuance of the mandate of authority to the delegate, activation of the actual power of authority, conducting actions under the name of the person concerned within the scope of the authority, verification of the authority, revocation of the authority from the delegate, and expression of acceptance of the mandate by the delegate.

As far as the delegate has to get access to data from the Data Track of the person concerned (e.g., to continue an ongoing communication), it must be possible for the person concerned to control which delegate can access and see specific partial identities. The person concerned may prefer to explicitly export the data entries that the delegate should access instead of granting access to parts of the own Data Track. In addition, the person concerned should be enabled to provide guidelines for the delegate, e.g., to partially or absolutely restrict certain disclosures [Hansen et al. 10].

Actions performed by a delegate on the behalf of the person concerned must produce entries in that person's Data Track, too. This may be done by exporting all relevant data from the delegate's Data Track as soon as the person concerned can take over again, or by writing into a Data Track accessible for both the person concerned and the delegate. All Data Tracks involved have to show the fact that specific actions were conducted by a particular delegate on behalf of another person.

7.4 Data Track for joint data

There is little work done by now on the possibilities of joint privacy and identity management and the relation to the Data Track instrument. Surely "Group Data Tracks" (or "Shared Data Tracks") could be set up that work for joint data, e.g., if research groups jointly publish papers and want to jointly manage their individual rights concerning privacy or also intellectual property. The group would have to define who handles the co-authors' communication with the editors, the publishers or other parties, which group-defined policies the acting persons have to adhere to, in which boundaries a negotiation with other parties should be possible and how policy changes over a long time period can happen.

For the specific situation of the relation between a delegate and the person concerned first proposals have been made in [Hansen et al. 10]: This comprises logging of actions performed by the delegate on behalf of the person concerned in both the Data Tracks of the delegate and the person concerned. For the purpose of delegation, specific (parts of the) Data Tracks could be defined where specific retention periods are defined: In particular, Data Track entries which comprise privacy-relevant information for both the delegate and the person concerned may be cut apart, the person concerned may check the delegate's actions on the basis of the logged data, and then only the parts belonging to the person concerned may be kept.

An interesting task is the avoidance of conflicts of interests or resulting misuse, e.g., when the person concerned and her delegates have competing interests, or if delegates are biased in their decisions on behalf of the person concerned, e.g., when getting percentages from transaction partners. This is especially challenging if the parties involved act under different pseudonyms each. Here supervision of the process by external parties should be made possible, e.g., by assigning certain access rights to parts of the various Data Tracks involved, by requesting integer data entries from the Data Tracks, or by creating specific Data Tracks for supervision purposes only.

More work has to be done on handling of joint data with all privacy implications.

7.5 Conclusion

There is still a long way to go to for privacy-enhancing identity management systems that cope with all challenges of lifelong privacy. This is true for both individual and group aspects of privacy and identity management. How to use Data Tracks for joint data is a new research issue that has to be dealt with in the next years. Here it is not sufficient to build technical solutions because the related issues have to be reflected in the legal and societal discussion on privacy and identity management in today's and emerging settings.

In addition, practical problems have to be solved, e.g., how to cope with the integration of offline data or other information from applications that do not support the user's Data Track. Further Data Tracks that function as non-manipulable logging devices have societal implications: Here it has to be discussed when people involved in a communication may or may not store what information, who else may get access to the data and how and when data can and will be deleted. This yields the question under which conditions there may even be the necessity to add some fuzziness to the data – for privacy reasons.

Chapter 8

Conclusions & Outlook

The Data Track is a transparency tool which has the purpose to give users the possibility to see what data they have sent to what recipients under which conditions (history function) and if such a recipient has modified or deleted these data or collected and stored further data about them (online access functions).

This deliverable presented PrimeLife WP 4.2's research and development work on a usable Data Track. The implementation of a usable Data Track poses several challenges from an HCI perspective. First of all, users typically engage in many transactions, which may involve multiple providers simultaneously. Hence, easy to use search tools will be needed. Besides, as we have already reported in [Pettersson et al. 05], users have difficulties to differentiate between the user and the services sides, which will make it difficult for users to learn the difference between the history function and the online access functions.

The technical implementation of the Data Track is by now in the state of a working application. In principle, this is also true from an HCI point of view.

Although there are still some minor HCI issues to be addressed, our usability tests showed that most users understand and appreciate the history tool part of the Data Track. The online access function part of the Data Track is somewhat more difficult for users to work with. It is not possible to conclude from the usability test data, if this is mainly a user interface issue or if the main problem is that users are not readily accepting the idea that they can actually retrieve data from the remote server side and also, if they wish, edit the data stored by the remote service provider. Independent of reason, this part of the Data Track would benefit from further elaboration and will still be addressed by WP 4.2 in the last project year.

In future, we plan to implement an interface of the Data Track to the privacy-enhancing logging system that PrimeLife partner KAU has developed in task 2.2.1. By this, we will not only provide a data subject with access to the data stored at a remote services side, but also with access to the transaction logs at the services side that document how the data subject's personal data have been used and processed by the services side.

Additionally, from a technical perspective, our future work includes adding a mechanism to the Data Track which will give users the possibility to track data posted by themselves or by others in web 2.0 type of on-line environments. The current working solution is based around a tagging mechanism that will not only give users the possibility to see if data pertaining to themselves are posted online, but also gives them the power to let those data be published or not.

Finally, we would like to mention that work package 4.2 is currently also cooperating with work package 3.2 (Open Source) on implementing a Data Track functionality into the browser-integrated PrimeLife Dashboard, which is planned to become open source.

References

[Art.29 WP 09] Article 29 Data Protection Working Party, 01189/09/EN, WP 163, Opinion 5/2009 on online social networking, adopted on 12 June 2009

[van Blarkom 03] van Blarkom, G.W., Borking, J., Olk, J., Handbook of Privacy and Privacy-enhancing Technologies – The case of Intelligent Software Agents, PISA project, 2003.

[Brükner et al. 05] Brückner L., Voss M., MozPETs – a Privacy Enhanced Web Browser. In Proceedings of the Third Annual Conference on Privacy and Trust (PST05), 2005, Canada.

[Chappell 06] Chappell, D., Introducing Windows CardSpace, Windows Vista Technical Articles, 2006.

[Clauß et al. 09] Clauß, S., Hansen, M., Pfitzmann, A., Raguse, M., Steinbrecher, S., Tackling the challenge of lifelong privacy. In: Paul Cunningham, Miriam Cunningham (Eds.): Proceedings of eChallenges 2009, 2009.

[den Berg et al 10] van den Berg, B, Leenes, R, .ed, PrimeLife deliverable D1.2.1 Privacy Enabled Comunities. PrimeLife, April, 2010.

[Hansen et al. 10] Hansen, M., Raguse, M., Storf, K., Zwingelberg, H., Delegation for Privacy Management from Womb to Tomb – A European Perspective. In: Proceedings of IFIP/PrimeLife Summer School 2009, to appear in 2010.

[Hansen et al. 08] Hansen, M., Pfitzmann, A., Steinbrecher, S., Identity Management throughout one's whole life. Information Security Technical Report (ISTR) Vol. 13, No. 2 (2008), Elsevier Advanced Technology, Oxford (UK), pp. 83-94, doi:10.1016/j.istr.2008.06.003.

[Hedbom 09] Hedbom, H., A Survey on Transparency Tools for Enhancing Privacy 2009. In: The Future of Identity in the Information Society. 4th IFIP WG9.2, 9.6/11.6 11.7/FIDIS International Summer School Brno, Czech Republic, September 2008, Revised Selected Papers, Springer, 2009.

[Jendricke et al. 02] Jendricke, U., Kreutzer, M., Zugenmaier, A., Mobile Identity Management. Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Göteborg, Sweden.

[Nielsen 05] Nielsen, J., 10 Heuristics for User Interface Design, 2005, http://www.useit.com/papers/heuristic/heuristic_list.html.

[Leenes et al. 05] Leenes, R., Lips, M., Poels, R., Hoogwout, M., User aspects of Privacy and Identity Management in Online Environments: Towards a theoretical model of social factors. in PRIME Framework V1 (chapter 9), Editors: Fischer-Hübner, S., Andersson, Ch., Holleboom, T., PRIME project Deliverable D14.1.a, June 2005.

[Pettersson et al. 05] Pettersson, J.S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauß, S., Kriegelstein, Th., Krasemann, H., Making PRIME usable. SOUPS 2005 Symposium on Usable Privacy and Security, Carnegie Mellon University, July 6-8, 2005, Pittsburgh. Available in ACM Digital Library.

[Pettersson et al. 06] Pettersson, J.S., Fischer-Hübner, S., Mike Bergmann, B., Outlining Data Track: Privacy-Friendly Data Maintenance for End-Users, Proceedings of the 15th

International Conference on Information Systems Development (ISD 2006), Budapest, 31 August - 2 September 2006, Springer Scientific Publishers.

[Pettersson 08] Petterson, J.S., HCI Guidelines, PRIME Deliverable D6.1.f, February 2008.

[Storf et al. 09] Storf, K., Hansen, M., Raguse, M. (Eds.), Requirements and concepts for identity management throughout life. PrimeLife Deliverable H1.3.5, Kiel/Zürich, November 2009, http://www.primelife.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_life-public.pdf.

[Trustguide 06] Lacohée, H., Crane,S., Pippen, A., Trustguide: Final Report, October 2006.

[Westin 67] Westin, A.F., Privacy and Freedom. Atheneum, New York 1967.

Appendix A

Usability test plan

A.1 Introduction to today's test

The test is anonymous, you will be given a randomly assigned number and it is only through this number your answers can be identified.

If you would like to abort the test you are free to do so at any time.

If there are any questions you feel that you cannot solve not solving it is an equally good or better indication that something is designed in a bad way. The software is supposed to be usable for everyone in the society and not just computer experts. It is the software that is tested and not you, so if there is something you do not understand this only means that we have designed it wrong.

In the first part of the test you will use "Prime Life" to buy a digital book at Amazon.com.

In the second part you will use "Data Track". It is used to show which information one has given via the internet, to which companies and when. By using "Data Track" it is possible to see which information the companies have stored about you and also if it correlates to the information you have sent. If the company allows it is also possible to change or delete the data they have stored.

Example:

If you buy a CD on CDON.com you have to send information about your address, e-mail, credit card information and so on. "Data Track" helps you to see which information you have sent to CDON, which information they have stored and if they allow you can also change their remotely stored data.

The test takes between half an hour and an hour.

After the test you will be compensated as agreed upon.

A.2 Pre-test Questionnaire (translated from Swedish)

1. Gender:

☐ Man

☐ Woman

2. Age: _____

3. How often do you use internet?

☐ Once or several times a day?

☐ Once or several times a week?

☐ Once or several times a month?

☐ Once or several times a year?

☐ Never?

4. How often do you shop on the internet?

☐ Once or several times a day?

☐ Once or several times a week?

☐ Once or several times a month?

☐ Once or several times a year?

☐ Never?

5. What type of services do you usually use online?

A.3 Post-test questionnaire

What's your opinion on the search function? Please, motivate your answer.

What's your opinion on the summary function? Please, motivate your answer.

How would you like to be able to find out what kind of information you've sent to a specific website?

Is there anything you feel is missing from the software you've just tested?

Was there anything you didn't understand in the program? Please, give a brief answer.

Would you consider using a program like this yourself? Why or why not?

Other thoughts, suggestions or comments?

A.4 PET-USES Questionnaire

Instructions

This test is designed to measure your experience with the system you've tested today. Your answers will be used to evaluate the system so please answer the questions as truthfully as you can. As the questions are designed to measure various aspects of the systems usability there are no right or wrong answers. Please use the scale below to indicate to what extent you disagree or agree to the statements that follow.

1 Strongly disagree

2 Disagree

3 Neither agree nor disagree

4 Agree

5 Strongly agree

General Usability

1. I found it easy to learn how to use the *system*	1 2 3 4 5
2. I had to learn a lot in order to use the *system*	1 2 3 4 5
3. I keep forgetting how to do things with this *system*	1 2 3 4 5
4. I need a lot of assistance to use this *system*	1 2 3 4 5
5. I find the *system* interface easy to use	1 2 3 4 5
6. I find the organisation of the *system* interface understandable	1 2 3 4 5
7. I get confused by the *system* interface	1 2 3 4 5
8. I find it very difficult to work with the *system*	1 2 3 4 5
9. I find that the benefits of using the *system* are bigger then the effort of using it	1 2 3 4 5
10. I would like to use this *system* regularly	1 2 3 4 5

Data Management

11. I get a clear view of my personal *data* from the system	1 2 3 4 5
12. I find organising my personal *data* easy with this system	1 2 3 4 5
13. I find keeping track of various user names and passwords is easy with this *system*	1 2 3 4 5

Data Release

14. I know what personal information I'm releasing when I’m using this *system*	1 2 3 4 5
15. The system makes it easy to decide how much or how little *data* to release in a given transaction	1 2 3 4 5
16. I get help from the system to understand who will receive my *data*	1 2 3 4 5
History	
17. I can easily find out who has received my personal *data* with this *system*	1 2 3 4 5
18. I get a good view of who knows what about me from this *system*	1 2 3 4 5
19. I can easily see how much I’ve used a particular user name with this *system*	1 2 3 4 5