From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions

Patrick, Andrew; Kenny, S.

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC-CNRC

*From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions **

Patrick, A.S., and Kenny, S.
March 2003

* published in Proceedings of the Privacy Enhancing Technologies Workshop (PET 2003) Dresden, Germany, March 26-28, 2003. NRC 45787.

Canada

From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions

Andrew S. Patrick
Institute for Information Technology
National Research Council of Canada
Building M-50, 1200 Montreal Rd.
Ottawa, ON Canada K1A 0R6
Andrew.Patrick@nrc-cnrc.gc.ca

Steve Kenny
Independent Consultant
stephen_mh_kenny@yahoo.com

Abstract. Internet users are becoming more concerned about their privacy. In addition, various governments (most notably in Europe) are adopting strong privacy protection legislation. The result is that system developers and service operators must determine how to comply with legal requirements and satisfy users. The human factors requirements for effective interface design can be grouped into four categories: (1) comprehension, (2) consciousness, (3) control, and (4) consent. A technique called "Privacy Interface Analysis" is introduced to show how interface design solutions can be used when developing a privacy-enhanced application or service. To illustrate the technique, an application adopted by the Privacy Incorporated Software Agents consortium (PISA) is analyzed in which users will launch autonomous software agents on the Internet to search for jobs.

1. Introduction

1.1. Project Motivations and Goals

There is increased awareness by the general public of their right to, and the value of, their privacy. Recent surveys indicate that Internet users are very concerned about divulging personal information online, and worried that they are being tracked as they use the Internet [8]. Research has indicated that users are failing to register for WWW sites because they feel that they cannot trust the Internet with personal or financial information [14]. In addition, information privacy is increasingly being associated with business issues such as reputation and brand value [6]. Moreover, governments within the European Union, Canada, Australia, and Switzerland have adopted privacy protection legislation that is enforced through independent governmental bodies with significant oversight powers. There has been little guidance, however, provided to system developers and operators on how to implement and comply with these privacy guidelines and rules, and how to soothe users' privacy concerns. This paper is an attempt to fill that gap.

This work was conducted as part of the Privacy Incorporated Software Agents (PISA; www.pet-pisa.nl) project, a European Fifth Framework Programme project whose goal is to develop and demonstrate Privacy-Enhancing Technologies (PET) that will protect the privacy of individuals when they use services that are implemented through intelligent software agents. An integral part of the project is an

analysis of the European privacy legislation and the development of methods to translate legislative clauses into human-computer interaction (HCI) implications and interface specifications. HCI is the study of mental processes and behavior as they pertain to users interacting with computers (and other technical devices). The goal of this paper is to document a process that begins with privacy legislation, works through derived privacy principles, examines the HCI requirements, and ends with specific interface design solutions. The approach taken is one of "engineering psychology" in which knowledge of the processes of the brain is used when doing system design [18].

In the sections that follow we explain how the European Privacy Directive 95/46/EC [3] has been analyzed to produce a set of detailed privacy principles (Section 2). The principles are then examined from a human factors point of view and a set of HCI requirements are developed (Section 3). We then demonstrate how the HCI requirements can be used when planning or analyzing a software application or service (a process we call a "Privacy Interface Analysis"; Section 4). Overall, our intent is to introduce the core concepts of privacy protection and HCI requirements, and then illustrate a Privacy Interface Analysis that other developers can follow.

To illustrate the technique, we use an example application adopted by the PISA consortium. This example is a computer service in which users will launch autonomous software agents on the Internet to search for jobs. The agents will have personal information about the users that the agents will use when seeking appropriate placements with various employers, so protection of the users' privacy is required and important. In the PISA demonstrator, each user has a personal agent to which he can delegate tasks such as searching for a job or making an appointment with another person or company. The personal agent in turn creates a dedicated agent for each task it is given. For example, a Job Search Agent (JSA) might communicate with Market Advisor Agents to locate good places to look for jobs. A Job Search Agent may also interact with a Company Agent to get more information about a position. Maintaining privacy protection as the agents share information and make autonomous decisions is the challenge of the PISA project.

1.2. Related Work

Alfred Kobsa [7][8] has recently conducted analyses with goals similar to the current project. Kobsa is interested in personalization services, such as WWW sites that remember your name and preferences. Such personalized services are made possible because the sites collect personal information about the users, either explicitly by asking for the information, or implicitly by tracking usage patterns. Although the personalized services can be useful and valuable, the storage and use of personal information both worries some users, and falls under the auspices of privacy guidelines and legislation. Kobsa has examined the implications of the privacy laws and user concerns and developed design guidelines to help WWW site operators build privacy-sensitive systems. These guidelines include suggestions like: (1) inform users that personalization is taking place, and describe the data that is being stored and the purpose of the storage, (2) get users' consent to the personalization, and (3) protect users' data with strong security measures. The current analysis goes deeper to focus on the requirements necessary when complying with the European Privacy Directive, and includes a discussion of specific interface techniques that can be used to meet those requirements.

2. Privacy Principles

2.1. EU Legislation

The right to privacy in the EU is defined as a human right under Article 8 of the 1950 European Convention of European Human Rights. The key privacy document is Directive 95/46/EC of the European Parliament on the protection of individuals with regard to the processing of personal data, and the free movement of such data (hereafter referred to as The Directive) [3]. Also, Directive 97/66/EC [4], concerning the processing of personal data and the protection of privacy in the telecommunications sector, applies and strengthens the original directive in the context of data traffic flow over public networks. These two directives represent the implementation of the human right to privacy within the EU.

The Directive places an obligation on member states to ratify national laws that implement the requirements of The Directive. This has resulted in, for instance, Wet Bescherming Persoonsgegevens 1999 in The Netherlands and The Data Protection Act 1998 in the UK. The national legislatures of EU member states must implement The Directive to substantially similar degrees. Such implementation includes sanctioning national enforcement bodies such as the Dutch Data Protection Authority with prosecution powers.

The Directive defines a set of rights accruing to individuals concerning personal data (also known as Personally Identifiable Information, or PII), with some special exceptions, and lays out rules of lawful processing on the part of users of that information that are applicable irrespective of the sector of application. Specifically, The Directive specifies the data protection rights afforded to citizens or "data subjects", plus the requirements and responsibilities of “data controllers” and by association “data processors”. The Directive attempts to balance the fundamental right to privacy against the legitimate interests of data controllers and processors -- a distinctive and central characteristic of the EU approach to data protection.

2.2. Overview of the Resulting Principles

As The Directive concerns itself with data processing, it must be implemented through a combination of information technology and governance initiatives. Privacy principles abstracted from the complexities of legal code have been developed to simplify this process. Table 1 shows a high-level summary of the privacy principles. Our research has focused on the privacy principles of (1) transparency, (2) finality and purpose limitation, (3) lawful basis, and (4) rights because these principles have the most important implications for user interface design. The remainder of this paper will be restricted to these four privacy principles.

3. HCI Requirements

3.1. Deriving the Requirements

The principles shown in Table 1 have HCI implications because they describe mental processes and behaviors that the Data Subject must experience in order for a service to adhere to the principles. For example, the principles require that users *understand* the transparency options, are *aware* of when they can be used, and are able to *control* how their PII is handled. These requirements are related to mental processes

and human behavior, and HCI techniques are available to satisfy these requirements. For example, an HCI specialist might examine methods for ensuring that users understand a concept, such as providing documentation, tutorials, and interface design characteristics.

Table 2 (in the Appendix) presents a more detailed summary of the four privacy principles under consideration in this paper. Included in Table 2 are the HCI requirements that have been derived from the principles. These requirements specify the mental processes and behavior of the end user that must be supported in order to adhere to the principle. For example, the principle related to the processing of transparency leads to a requirement that users know who is processing their data, and for what purpose.

The HCI requirements outlined in Table 2 are not unrelated. The core concepts in the requirements can be grouped into four categories: (1) *comprehension*: to understand, or know; (2) *consciousness*: be aware, or informed; (3) *control*: to manipulate, or be empowered; (4) *consent*: to agree.

Table 1: High-Level Summary of Privacy Principles
(italic items are analyzed in detail)

Principle	Description
Reporting the processing	All non-exempt processing must be reported in advance to the National Data Protection Authority.
Transparent processing	*The Data Subject must be able to see who is processing his personal data and for what purpose. The Controller must keep track of all processing performed by it and the data Processors and make it available to the user.*
Finality & Purpose Limitation	*Personal data may only be collected for specific, explicit, legitimate purposes and not further processed in a way that is incompatible with those purposes.*
Lawful basis for data processing	*Personal data processing must be based on what is legally specified for the type of data involved, which varies depending on the type of personal data.*
Data quality	Personal data must be as correct and as accurate as possible. The Controller must allow the citizen to examine and modify all data attributable to that person.
Rights	*The Data Subject has the right to acknowledge and to improve their data as well as the right to raise certain objections.*
Data traffic outside EU	Exchange of personal data to a country outside the EU is permitted only if that country offers adequate protection. If personal data is distributed outside the EU then the Controller ensures appropriate measures in that locality.
Processor processing	If data processing is outsourced from Controller to Processor, controllability must be arranged.
Security	Protection must be provided against loss and unlawful processing.

In the category of *comprehension*, the requirements can be summarized as building a system or service that will enable users to:

- comprehend how PII is handled
- know who is processing PII and for what purposes
- understand the limits of processing transparency
- understand the limitations on objecting to processing
- be truly informed when giving consent to processing
- comprehend when a contract is being formed and its implications
- understand data protection rights and limitations

In the category of *consciousness*, the requirements are to allow users to:

- be aware of transparency options
- be informed when PII is processed
- be aware of what happens to PII when retention periods expire
- be conscious of rights to examine and modify PII
- be aware when information may be collected automatically

In the category of *control*, the requirements are to allow users to:

- control how PII is handled
- be able to object to processing
- control how long PII is stored
- be able to exercise the rights to examine and correct PII

Finally, the requirements in the area of *consent* are to build systems that allow users to:

- give informed consent to the processing of PII
- give explicit consent for a Controller to perform the services being contracted for
- give specific, unambiguous consent to the processing of sensitive data
- give special consent when information will not be editable
- consent to the automatic collection and processing of information

This list represents the essential HCI requirements that must be met in order to build systems that provide usable compliance with the European Privacy Directive. System designers will be well served if they consider the dimensions of comprehension, consciousness, control and consent when building privacy-enhanced systems.

3.2. Interface Methods to Meet Requirements

The field of interface design has developed a set of techniques, concepts, and heuristics that address each of the requirement areas. It is beyond the scope of this paper to provide an exhaustive review of the field of interface design, and interested readers are encouraged to examine one of the many HCI books for more information [e.g., 15, 11, 10, 18, 12].

Comprehension. The obvious method to support comprehension or understanding is training. Users can be taught concepts and ideas through classroom training, manuals, demonstrations, etc. Such methods can be very successful, but they can also be expensive, time-consuming, and inappropriate when learning computer systems that will be infrequently used. Today, much effort is devoted to supporting comprehension without resorting to formal training methods.

User documentation, especially online or embedded documentation, is often used as a replacement for training. Most computers and software come with manuals of some sort, and much is known about how to develop material that people can learn from effectively [10]. Studies have shown, however, that most users do not read the documentation, and often they cannot even find the printed manuals [1]. As a result, designers often resort to tutorials and help systems to support comprehension. Help systems can be designed to provide short, targeted information depending on the context, and such systems can be very powerful. It is often difficult, however, to learn an overview of all the features of a system using built-in help. Tutorials are another method of supporting learning, and they can work well if they are designed with a good understanding of the needs of the user.

There are other methods for supporting understanding that do not rely on documentation. For example, research in cognitive psychology has shown that users often develop personal "mental models" of complex systems. These models are attempts to understand something to a level where it can be used effectively, and such models can be quite effective when faced with complex systems. HCI specialists can exploit the human tendency to create models by either guiding users to develop appropriate models, or by examining the models that already exist and accounting for them. For example, people often have a mental model of a furnace thermostat that is analogous to a water faucet. That is, the more that it is "turned on", the faster the water (or heat) will flow. This model is incorrect because most furnaces can only operate at one flow rate and the thermostat only determines the temperature where the heat flow will be shut off. It is interesting to note that this erroneous mental model has persisted for a long time, and thermostat interface designers would likely want to take it into account. Thus, a thermostat designer might add a feature to automatically return the setting to a normal room temperature some time after the thermostat was suddenly turned to an abnormally high setting.

A related interface technique is the use of metaphors. Most modern graphical computer systems are based on a desktop or office metaphor, where documents can be moved around a surface, filed in folders, or thrown in a trashcan. The graphical elements of the interface, such as document icons that look like pieces of paper and subdirectory icons that look like file folders, reinforce this metaphor. The metaphor is valuable because it provides an environment that users are familiar with, and thus they can use familiar concepts and operations when interacting with the system. The familiar metaphor decreases the need to develop new knowledge and understanding.

There are other, more subtle techniques that can facilitate comprehension. For example, the layout of items on the screen can convey some meaning or information. Items that are grouped together visually will likely be considered to be group together conceptually [10], and interface designers can take advantage of that. Also, items that are ordered horizontally in a display will likely be examined from left to right, at least in North American and European cultures. Interface designers can use this sequencing tendency to ensure that users follow the recommended order of operations.

Feedback is also very important for supporting understanding [15]. Most complex systems require some experience and learning before they can be used effectively. Without feedback, users may not learn the consequences of their actions and understanding will be slow to develop.

Consciousness. The requirement of consciousness refers to the user being aware of, or paying attention to, some concept or feature at the desired time. It is related to comprehension because the awareness may require some background knowledge before conscious attention is useful. Consciousness in this context can be thought of as bringing knowledge or understanding to the attention of the user so it can be used when required.

There are many interface techniques for making users aware of something. System messages or pop-up windows are an obvious technique for making the user aware of an event. For important information, these windows can be constructed so the users have to acknowledge the message before they can continue using the system. A more subtle technique is to remind the user of something without interrupting their work. This is sometimes seen in "help assistants" (such as the Microsoft Office Assistant) that make suggestions while users interact with the interface. Another way to remind users is through the arrangement of the interface. For example, if a particular option is available to a user at a certain time, placing icons or messages nearby in the interface layout can ensure that users are aware of the options.

Even more subtle methods use display characteristics to draw attention. Printing text in a certain color, such as red, can draw attention. Changing the color dynamically can be more effective. Sounds are also frequently used to make users aware of some event. The human factors discipline has a long history of designing systems that make users aware of certain things at certain times [18].

Control. Control refers to the ability of the user to perform some behavior. Control is related to comprehension because the user must understand the task and context to behave effectively. Control is also related to consciousness because users must be aware of the need to act before they can execute the behavior. The issue of control, however, is that once the user knows that they are supposed to do something (awareness), and they understand what to do (comprehension), can they actually carry out the action.

Figure 1: A door with poor affordances. The door is solid glass with a vertical handle in the middle. (from http://www.baddesigns.com; reprinted with permission)

An important concept for ensuring control is affordance, which means to provide naturally or inevitably. The classic example is door opener design. With some doors, users may approach the door, understand that it is a door, be conscious that they need to open the door, and still not be able to perform the action (see Figure 1 for an example). In contrast, a simple metal plate placed on the surface of the door tends to be a natural signal to push the door (in fact, these are often called "push plates"), whereas a metal loop placed vertically at the edge of a door tends to be a natural signal to pull the door. By using affordances, interface designers can make the door easy to control.

Another interface technique that supports appropriate actions is mapping. The idea is to map the appearance and function of the interface to the device being controlled. This might mean making a physical analogy of the real world in the interface, such as arranging light switches on a wall in the same order that the lights are arranged in the ceiling [11].

Many of the subtle HCI techniques that can be used to support control are related to "obviousness". To the extent that the interface can be made obvious to the user, control (and understanding) can be smooth and effective. When interfaces are not obvious, users may have serious problems using the device or system. The goal of the interface designer is to build something that is so obvious to the user that comprehension, consciousness, and control will develop with little learning and effort.

Consent. The final HCI requirement category is consent. Users must be able to consent or agree to terms or conditions that may be associated with a system or service. Moreover, the consent should be "informed", meaning that the users fully understand what they are agreeing to, and what implications this may have. Obviously, supporting informed consent is related to the requirements for comprehension and consciousness.

The most common method for supporting consent in computer applications is a "user agreement". When you have installed new software on your computer, or signed-up for an Internet service, you have undoubtedly seen an interface screen that presents a User Agreement or Terms of Service. In order to continue, you have had to click on an "I Agree" button or an equivalent label. These interface screens are commonly called "click-through agreements" because the users must click through the screen to get to the software or service being offered [17]. (An alternative label is "click-wrap agreement", in parallel to more traditional "shrink-wrap" agreements attached to software packaging.) These agreement screens are an attempt to provide the electronic equivalent of a signed user agreement or service contract [16]. By clicking on the "Agree" button, the user is confirming their understanding of the agreement and indicating consent to any terms or conditions specified in the accompanying text.

The legality of these click-through screens in forming the basis of a legal agreement or contract has been established, but with some qualifications. The Cyberspace Law Committee of the American Bar Association has recently reviewed the case law and developed a set of guidelines for creating click-through agreements [9]. These guidelines have been summarized into six principles to be considered by system developers [5][17]:

1. Opportunity to review terms: users must view the terms of the agreement before consenting to the agreement. A recent case involving Netscape [17] established that it is important that there be no other method to obtain the product or service other than by clicking-through the agreement.
2. Display of terms: the terms have to be displayed in a "reasonably conspicuous" [17] manner. A recent case involving Ticketmaster [9] established that simply linking to the terms at the end of a long home page was not enough.
3. Assent to terms: the language used to accept the agreement must clearly indicate that a contract is being formed.
4. Opportunity to correct errors: there should be a method for users to correct errors, such as seeking a final confirmation before proceeding, or allowing the user to back-out of an agreement.

5. Ability to reject terms: the option to reject the terms of the agreement should be clear and unambiguous, and the consequences of the rejection should be stated (e.g., "if you do not agree, you will not be able to install this software").
6. Ability to print the terms: the interface should allow the user to print the terms for later reading.

Other factors that should be considered when creating click-through agreements [16] are to redisplay the terms and conditions at product startup (reminding), and to support the ability to review the terms at any time (e.g., in the "help" or "about" menus). In addition, developers should adapt the terms and conditions to local languages and requirements. If these principles and considerations are heeded, case law suggests that click-through agreements will likely be enforced, at least in US courts. (Some jurisdictions, such as Germany and China, are unlikely to enforce any of these agreements [16]).

The text of many click-through agreements tends to be long and complex, often to ensure that all the points raised above are addressed. The result is that many users have difficulty reading and understanding the documents (a comprehension problem), and many users click the "Agree" button without considering the terms at all (a consciousness problem). The problems arise because people have limited cognitive capacity: we have limited attention spans, a restricted ability to process large quantities of detailed information at one time, and limited memories. Thus, using interface techniques that are sensitive to user characteristics may be valuable here. This observation may be particularly relevant if users are being asked to agree to a number of terms that will affect them substantially, such as the processing of their personal data.

Ensuring that users fully understand and unambiguously agree to the processing of their personal information is important for complying with privacy legislation and guidelines. Consider the definition of consent provided in the EU Directive 95/46/EC on privacy protection [3]:

> 'the data subject's [user's] consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. (Article 2-h)

It is clear that a large, cumbersome, complicated User Agreement presented to the user only when they begin to use a product or service fails to live-up to the requirements for "specific" and "informed" consent, and yet these types of user agreements are the majority. These issues are of particular concern in relation to explicit consent. For example, the EU Directive states that when sensitive data (e.g., race, ethnic origin, religious beliefs) are processed, the user must give "explicit consent" (Article 8-2-a) to the processing of the sensitive data. Again, a single, large, click-through User Agreement does not meet the spirit of The Directive.

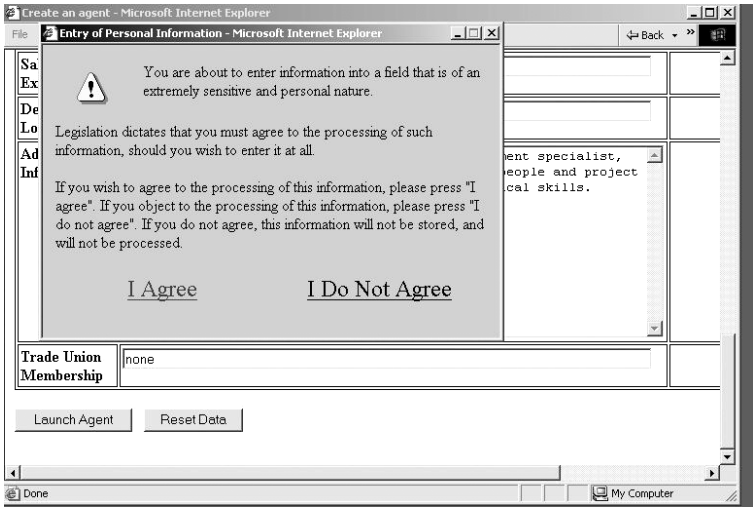

Figure 2: An example of a Just-In-Time Click-Through Agreement (JITCTA)

The solution to this problem proposed here is a new concept of "Just-In-Time Click-Through Agreements" (JITCTAs). The main feature of a JITCTA is not to provide a large, complete list of service terms but instead to confirm the understanding or consent on an as-needed basis. These small agreements are easier for the user to read and process, and facilitate a better understanding of the decision being made in-context. Also, the JITCTAs can be customized for the user depending on the features that they actually use, and the user will be able to specify what terms they agree with, and those they do not. It is hoped that users will actually read these small agreements, instead of ignoring the large agreements that they receive today. The responses made by the user during the JITCTAs can also be recorded so there is a clear, unambiguous record of the specific agreements made with the user. In order to implement JITCTAs, the software will have to recognize when users are about to use a service or feature that requires that they understand and agree to some term or condition.

A sample screen capture of a JITCTA is shown in Figure 2. In this example a user has selected the Trade Union Membership information field in the Create Agent interface screen of the PISA interface. Since this would be considered sensitive information in the EU Privacy Directive, a JITCTA has appeared to obtain explicit, specific, timely, unambiguous consent to the processing of this data.

In summary, well-formulated click-through agreements are legally permissible in many countries, and Just-In-Time Click Through Agreements improve on this device by supporting more appropriate decision-making and control that is sensitive to human factors constraints.

4. The Privacy Interface Analysis

Up until this point, we have described the privacy principles that have been derived from the European Privacy Directive, analyzed these principles for their HCI requirements, categorized and described the nature of the requirements, and reviewed methods to meet these requirements. This section outlines how all of this can be brought together to systematically conduct a Privacy Interface Analysis.

4.1. Develop a Service/Application Description

The first step in the analysis is to prepare a detailed description of the operation of the program or service. A useful technique for conducting this analysis is the Unified Modeling Language (UML) [13], which is a powerful language for specifying, visualizing, and sharing specifications and design decisions. By creating a set of interrelated diagrams or models, the developers can visualize and examine the features of the software long before any programming code is written. Although UML is not required to complete a thorough privacy interface analysis, it does make the process easier and the result more valuable.

A primary UML modeling technique is Use Case modeling. Here a high-level diagram is created to show the functionality of the system from the users' point of view. The purpose of the Use Case analysis is to specify what the software will do, and not to focus on how it will do it (that will come later). Figure 3 shows a simple Use Case diagram for the PISA Demonstrator example. This diagram shows the major functions provided by the software are creating an agent, tracking an agent, viewing agent results, etc. Doing a thorough analysis at this stage is important because each use case represents a function or feature that may involve an interface to privacy protection measures.

The next step is to determine how the application will work internally. UML structure diagrams are useful here to illustrate the software objects or classes that will be necessary to implement the functionality of a use case. Perhaps most useful are interaction diagrams, such as Object Sequence Diagrams. These diagrams model the relations between the software objects, and illustrate any data communication that must take place. Figure 4 shows a sequence diagram for the Register use case in the PISA demonstrator example. This diagram depicts the major software components involved with supporting this function, such as the WWW interface, the WWW server, and the Personal Agent. It also shows the interactions between

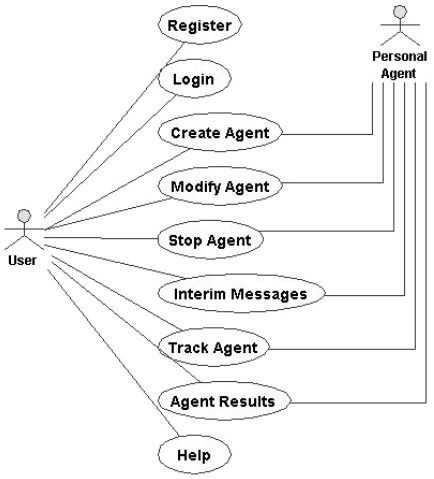

Figure 3: Use Case Diagram for the PISA Demonstrator

the user and the system, as well as the interactions between the software objects. Normally you should create at least one Object Sequence diagram for each use case that was identified earlier.

4.2. Explore and Resolve the HCI Requirements

The third step involves analyzing the HCI requirements of each of the privacy principles in Table 2 and determining their effects on the application models. For each principle, determine if the human requirements related to the principle are already covered in the current models of the application, or if a solution is required. If a solu-

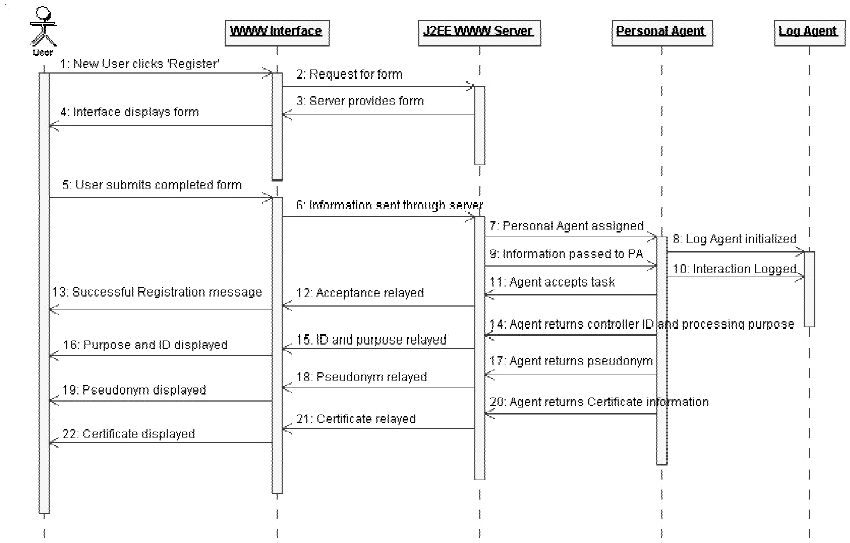

Figure 4: Object Sequence Diagram for the Register Use Case

tion is needed, generic possible solutions to the HCI requirements are presented in the last column of Table 2, but each application may require a unique solution that is suitable for that particular situation. For example, Principle 1.3.1 concerns processing for direct marketing purposes, and states that: "DS receives notification of possible objection". Applied to the PISA example, this means that users need to be made aware that they are able to object to processing of personal data for direct marketing purposes (the comprehension and consciousness requirement categories). One method to satisfy this principle would be to include an "opt-in" feature in the Create Agent use case so users can choose to participate in direct marketing or not, and to display that option in a distinctive color to draw attention to it. In addition, a "review options" function might be added to the Modify Agent use case to remind users that they can view and change their opt-in decision. Also, in the Track Agent use case, a control to change their opt-in decision could be provided.

To further illustrate this step in the analysis, consider what must happen during the Create Agent use case. A naive view might be that the user simply provides the system with personal information, and perhaps reads a user agreement. By applying the

HCI requirements, this Create Agent function can be expanded to ensure usable compliance with the privacy principles. For example, Principle 2.3 states that personal information must have an associated retention period, after which the data is deleted or rendered anonymous. To comply with this requirement, an interface feature to "specify retention period" can be added to the Create Agent use case. Other features that should be included in the Create Agent use case are:

- use a JITCTA to acknowledge rights
- use a JITCTA to acknowledge the formation of a contract and to consent to PII processing
- use a JITCTA if any sensitive information is collected
- provide an interface to "opt-in" to processing for direct marketing purposes

Another example of the results of a privacy interface analysis is shown in Figure 4. Principle 1 states that the use and storage of PII must be transparent to the user. To meet that requirement, the interaction diagrams were examined and extra interactions for the Register use case were added so information about the identity and purpose of the Controller are conveyed to the user.

Another important HCI requirement is that users must understand their ability to track the processing of their PII, and be aware of any limitations. In the PISA exam-

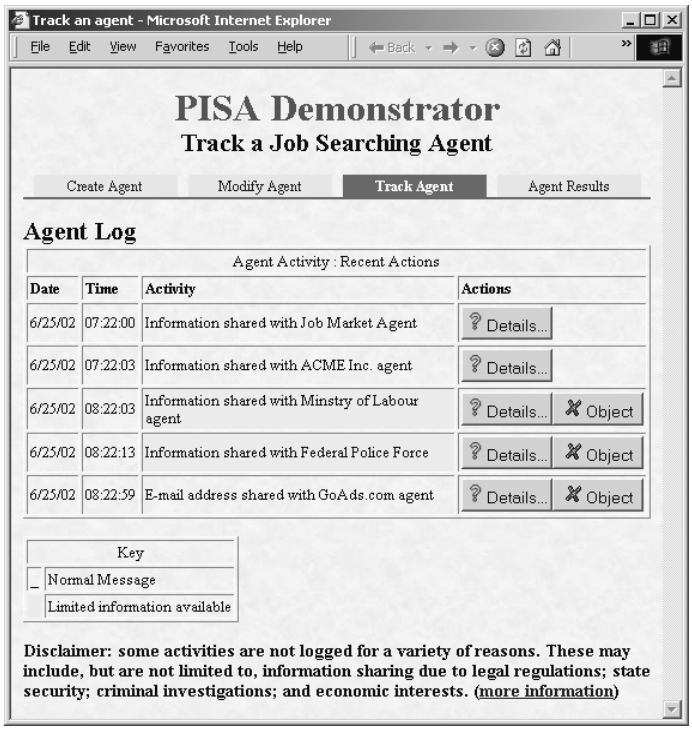

Figure 5: A possible Track Agent interface screen illustrating HCI solutions.

ple, a solution to this requirement is shown in Figure 5, which represents a possible Track Agent interface screen. This screen shows how a log of agent information sharing could be displayed, and some log entries are highlighted to indicate that limited tracking information is available. In addition, users are reminded by the message at the bottom of the screen of the situations where activity may not have been logged at all. Another feature of the interface is to place control buttons for the objection functionality alongside the appropriate log entries. Thus, by using the interface features of highlighting, reminding, and grouping, the privacy principles can be implemented naturally and obviously.

The result of a well-conducted privacy interface analysis is a set of design solutions that will ensure usable compliance with the privacy principles. These can be organized according to the use cases that are affected and incorporated into a produce design specification and passed on to the developers for implementation.

4.3. Conducting A Privacy Interface Analysis for Other Applications

Developers interested in conducting a Privacy Interface Analysis should now be ready to proceed. Again, the key steps are to:

1. develop a detailed description of the application or service from a use case and internal operation point of view.
2. examine each HCI requirement described in Section 3.1 to see if it applies to this application, using Table 2 as a guide.
3. for each requirement that must be met, scrutinize the generic privacy solutions provided in Table 2 (and the interface design methods in Section 3.2) to determine an appropriate specific solution.
4. organizing the solutions according to use cases and capture the solutions in an interface requirements document.
5. implement the interface according to the requirements document.

5. Summary and Conclusions

This paper introduced design guidance for privacy-enhancing technologies from a human factors point of view. For the first time, this work specified what must be included in human-computer interfaces to satisfy the spirit of European privacy legislation and principles, and satisfy the privacy needs of the users ("usable compliance"). A technique called "privacy interface analysis" was introduced to help developers establish the privacy requirements for their projects, and understand the interface design solutions that can be used.

The current work has focused on European privacy legislation and, although the resulting principles, requirements, and solutions are general, one of the challenges that remains is to ensure that the knowledge is equally applicable in other legislative settings, such as Canada, and in areas operating in a self-regulatory fashion (e.g., the USA). For example, it is possible that the market forces operating in the USA will lead to privacy requirements and expectations that have not been anticipated. Even in regulated environments, the privacy legislation and guidelines will change and evolve, and thus the human interface guidelines will also have to be dynamic.

Privacy enhancing technologies are also evolving and changing, and this will have an effect on the types of solutions that are available, and also the privacy needs and expectations of the users. For example, the P3P protocol, if implemented widely, may

have a profound effect on the privacy domain by bringing privacy issues to the attention of millions of Internet users, and hopefully providing an easy-to-use privacy control interface (e.g., [2]).

Our research is continuing in this area. We will use the techniques introduced here during the completion and evaluation of the PISA prototype. Usability studies being conducted now will provide concrete data on the effectiveness of interface design solutions proposed here in meeting users' privacy needs. We are also beginning to examine the process of developing and implementing privacy policies, where we are also interested in the steps required when moving from intentions, to principles, to requirements, and to implementations.

References

1. Comstock, E.M., & Clemens, E.A. (1987). Perceptions of computer manuals: A view from the field. *Proceedings of the Human Factors Society 31st Annual Meeting*, 139-143.
2. Cranor, L.F., Arjula, M., & Guduru, P. (2002). Use of a P3P User Agent by Early Adopters. *Proceedings of Workshop on Privacy in the Electronic Society*. Washington, D.C., November 21.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. *Official Journal of the European Communities* (1995), p. 31.
4. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal L 024* , 30/01/1998 p. 0001 – 0008.
5. Halket, T.D., & Cosgrove, D.B. Is your online agreement in jeopardy? http://www.cio.com/legal/edit/010402_agree.html
6. Kenny, S., & Borking, J. (2002). The value of privacy engineering. *Journal of Information, Law and Technology (JILT)*. http://elj.warwick.ac.uk/jilt/02-1/kenny.html.
7. Kobsa, A. (2001). Tailoring privacy to users' needs (Invited Keynote). In M. Bauer, P. J. Gmytrasiewicz and J. Vassileva, Eds. *User Modeling 2001: 8th International Conference*. Berlin - Heidelberg: Springer Verlag, 303-313. http://www.ics.uci.edu/~kobsa/papers/2001-UM01-kobsa.pdf
8. Kobsa, A. (2002). Personalized hypermedia and international privacy. *Communications of the ACM, 45*(5), 64-67. http://www.ics.uci.edu/~kobsa/papers/2002-CACM-kobsa.pdf
9. Kunz, C.L. (2002). Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent. http://www.efscouncil.org/frames/Forum%20Members/Kunz_Click-thr_%20Agrmt_%20Strategies.ppt. See also C.L. Kunz, J. Debrow, M. Del Duca, and H. Thayer, "Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent," *Business Lawyer, 57,* 401 (2001).
10. Nielsen, J. (1993). *Usability engineering*. San Diego, CA: Morgan Kaufmann.
11. Norman, D.A. (1988). *The psychology of everyday things*. Basic Books.
12. Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S., & Carey, T. (1994). *Human-computer interaction*. Reading, MA: Addison-Wesley.
13. Rumbaugh, J., Jacobson, I., & Booch, G. (1998). *The unified modeling language reference manual*. Addison-Wesley.
14. Saunders, C. (2001). Trust central to E-commerce, online marketing. *Internet Advertising Report*. http://www.internetnews.com/IAR/article.php/12_926191
15. Shneiderman, B. (1987). *Designing the user interface: Strategies for effective human-computer interaction*. Reading, MA: Addison-Wesley.

16. Slade, K.H. (1999). Dealing with customers: Protecting their privacy and enforcing your contracts. http://www.haledorr.com/db30/cgi-bin/pubs/1999_06_CLE_Program.pdf
17. Thornburgh, D. (2001). Click-through contracts: How to make them stick. *Internet Management Strategies*. http://www.loeb.com/FSL5CS/articles/articles45.asp
18. Wickens, C.D., & Hollands, J.G. (2000). *Engineering psychology and human performance* (3rd Ed.). Upper Saddle River, NJ: Prentice Hall.

Appendix: Table 2: Privacy Principles, HCI Requirements, and Design Solutions

	Privacy Principle	**HCI Requirement**	**Possible Solution**
1	Transparency: Transparency is where a Data Subject (DS) is empowered to comprehend the nature of processing applied to her personal data.	users must be *aware* of the transparency options, and feel empowered to *comprehend* and *control* how their Personally Identifiable Information (PII) is handled	during registration, transparency information is *explained* and examples or tutorials are provided
1.1	DS informed: DS is aware of transparency opportunities	users must be *aware* of the transparency options	Opportunity to track controller's actions made *clearly visible* in the interface design
1.1.1	For: PII collected from DS. Prior to PII capture: DS informed of: controller Identity (ID) and Purpose Specification (PS)	users *know* who is controlling their data, and for what purpose(s)	at registration, user is *informed* of identity of controller, processing purpose, etc.
1.1.2	For: PII not collected from DS but from controller. DS informed by controller of: processor ID and PS. If DS is not informed of processing, one of the following must be true: DS received prior processing notification, PS is legal regulation, PS is security of the state, PS is prevention/detection/prosecution of criminal offences, PS is economic interests of the state, PS is protection of DS or rights of other natural persons, PS is scientific/statistical & PII is anonymized, or PII are subject to any other law governing their processing/storage	users are *informed* of each processor who processes their data, and the users *understand* the limits to this informing	- *user agreements* states that PII can be passed on to third parties - user agreement also contains information about usage tracking limitations - when viewing the processing logs, entries with limited information are coded to draw *attention*, and users are reminded about the tracking limitations
1.3	When PII are used for direct marketing purposes, DS receives notification of possible objection. This notification may occur every 30 days	users *understand* that they can object to processing of their PII for direct marketing, and the limitations on those objections	- during registration, users must *opt-in* to processing for direct marketing or charitable purposes - to ensure understanding and awareness, users are given examples and a *Just-In-Time Click-Through Agreement*

	Privacy Principle	HCI Requirement	Possible Solution
			(JITCTA) is used for final acceptance - users are also reminded of their opt-in/out option in a preferences interface screen
2	Finality & Purpose Limitation: the use and retention of PII is bound to the purpose to which it was collected from the DS.	users *control* the use and storage of their PII	interface elements for making privacy decisions are prominent and *obvious*
2.1	The controller has legitimate grounds for processing the PII (see Principle 3.1)	users give implicit or explicit *consent*	click-through agreement should obtain *unambiguous consent* for controller to process the PII
2.2	Obligations: A controller must process according to his PS, controller also ensures other processors present a PS to be considered a recipient of the PII. When assessing a processor, the controller considers PII sensitivity and the similarity of processor PS to agreed-upon PS and location of the processor. The processor can only go beyond the agreed PS if: the processor's PS is state security, or prevention/detection/prosecution of criminal offences, or economic interests of the state, or protection of DS, or rights of other natural persons, or scientific/statistical analysis	users *understand* that their PII could be used for other purposes in special cases	- *user agreement* states that PII can (must) be passed on in special cases - when viewing the processing logs, entries with limited information are coded to draw *attention*, and users are *reminded* about the special cases
2.3	Retention: the DS is to be presented a proposed retention period (RP) prior to giving consent, except where PS is scientific/ statistical. Controller ensures processor complies with RP, except where PS is scientific/statistical. When RP expires, it is preferably deleted or made anonymous. A record should be kept of processor's and controller's past adherence to RPs.	- users are *conscious* of RP prior to giving *consent* - users are *aware* of what happens to their data when the retention time expires	- When data is provided, a retention period entry field will be *highlighted* - Users are *informed* when information is deleted or made anonymous because of retention period expiry.
3	Legitimate Processing: Legitimate Processing (LP) is where the PII is processed within defined boundaries.	users *control* the boundaries in which their PII is processed	interface elements for making privacy decisions are prominent and *obvious*

	Privacy Principle	HCI Requirement	Possible Solution
3.1	Permission: To legitimately process PII, controller ensures that one or more of the following are true: the DS gives his explicit consent, the DS unambiguously requests a service requiring performance of a contract, the PS is legal obligation or public administration, the vital interests of the DS are at stake. When matching the PS agreed to by the DS and the PS of the possible processor, any of the following will prevent processing: The controller/processor's actual PS differs from the PS consented to by the DS, the controller/processor intends passing the PII to a new processor, the controller/processor is not located in the EU, or the processor is violating a fundamental right to be left alone	- users give *informed consent* to all processing of data - users *understand* when they are forming a contract for services, and the implications of that contract - users *understand* the special cases when their data may be processed without a contract	- *JITCTA* to confirm unambiguous consent to data processing - *JITCTA* to confirm the formation of a contract, and the implications/limitations of the contract - in the tracking interface, include a *reminder* of special cases when data can be processed without a contract
3.2	Sensitive Data: The controller may not process any PII that is categorized as religion, philosophical beliefs, race, political opinions, health, sex life, trade union membership, or criminal convictions unless the DS has given their explicit consent or the processor is acting under a legal obligation	when dealing with highly sensitive information (religion, race, etc.), *users provide explicit, informed consent* prior to processing	if sensitive information is provided by the user, use a *double JITCTA* to obtain unambiguous consent for its processing
4	Rights: DS has the right to self-determination within the boundaries and balance of The Directive.	users *understand* and *can exercise* their rights	- at registration, use a *click-through agreement* to ensure that users know their rights - interface layout provides *obvious* tools for controlling the rights functions
4.1	Access: DS is conscious of her rights. The DS has right to retrieve this data on PII processing: (1) who has received it; (2) who gave them it; (3) when; (4) for what PS & (5) if a delete or anonymize operation has been acknowledged & authenticated. Items (1) (3) (4) should be disclosed if the proposed PS is any one of: state security, prevention/detection/prosecution of criminal offences, economic interests of the state, legal regulation, or protection of rights and freedoms (of other persons). If the DS is below the age	- users are *conscious* of their rights, which include right to know who has received their data, from whom, when, and why, and they *understand* the exceptions to these rights - users *understand* and *can exercise* their rights	- the tracking functions are displayed *prominently* - the exceptions to the rights are presented in the *user agreement*, and *reminders* are provided in the tracking interface

	Privacy Principle	HCI Requirement	Possible Solution
	of consent then access requests must be made by his/her legal representative (LR). In all cases, authentication should be proportional to the PII sensitivity		
4.2	Control: DS may issue erase, block, rectify, or supplement commands on their PII. The DS is informed of the result of their command within 30 days. The communication is either: request accepted and executed, or request denied and an explanation. If the PII will not be editable due to the storage strategy applied, then DS is informed & asked to consent prior to providing any PII. Controller is accountable for the correct execution of DS requests for erase, block, rectify, or supplement the PII	- users are *conscious* of their rights, they can *exercise* control over their data, which ability to erase, block, rectify, or supplement the data - users are *informed* when data will not be editable and they provide *consent* to processing	- the tracking functions are displayed *prominently* - the exceptions to the rights are presented in the *user agreement*, and *reminders* are provided in the tracking interface - the *commands* to erase, block, rectify, and supplement are associated with the tracking logs and *obvious* to operate - a *JITCTA* is used when data will not be editable
4.3	Objections: if DS has not given direct consent to processing and the PS is public administrative or Legitimate Processing, the controller determines validity of the objection. If the PII is sensitive data and/or the PS is sensitive then the objection is accepted and the PII is deleted. If the PS is direct marketing then any objection is accepted and the PII is deleted.	users are *empowered* to object to processing for certain purposes	the tracking logs contain a *prominent function* to object to the processing
4.4	Derived Information: Certain PS supplied by processor to controller or controller to DS could be used to gain an insight into a person's personality, e.g., services of interest to the DS. This derived information shall not be processed unless: the DS is informed of the PS related to the derived information, he/she unambiguously requests a service requiring performance of a contract and has issued explicit consent. The DS can object to the processing of the derived information at any time, and the derived information must be deleted.	users *understand* and are *informed* that their behavior may provide some information, and they have provided *consent* for the processing of this information. They are also *empowered* to object to this processing	- the concept of derived information is *explained* at registration, and an example is provided - a *JITCTA* is used to confirm consent to processing - processing logs or other results of derived information are always presented with an *obvious* interface for objection