

**NRC-CNRC**

*From Discovery to Innovation...*

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

**Andrew S. Patrick**

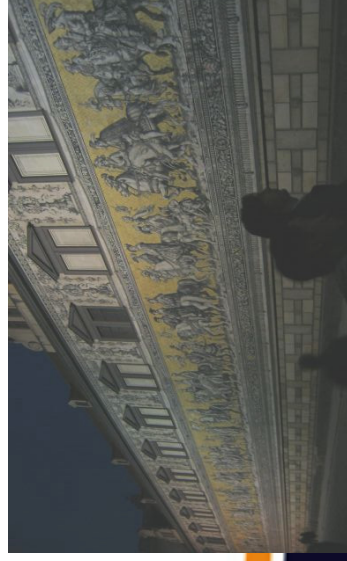
National Research Council of Canada

[www.andrewpatrick.ca](http://www.andrewpatrick.ca)

**Steve Kenny**

Independent Consultant

[stephen\\_mh\\_kenny@yahoo.com](mailto:stephen_mh_kenny@yahoo.com)



National Research  
Council Canada

Conseil national  
de recherches Canada

Canada

PET Workshop, Dresden, March 27, 2003

# PISA: Privacy Incorporated Software Agent

## European Commission 5<sup>th</sup> Framework Project

- international R&D consortium
- [www.pet-pisa.nl](http://www.pet-pisa.nl)



# Privacy Incorporate Software Agent: building a privacy guardian for the electronic age

**PISA** builds a model for **software agents** to perform actions on behalf of a person **without compromising the personal data** of that person

## Aims

- to demonstrate **PET** as **secure technical solution** to protect privacy of citizens when using intelligent agents:
- providing capability for **detailed audit logging and activity tracking** of agent transactions for the user to monitor;
- leveraging **pseudo-identity**;
- using **identification and authentication mechanisms** to prevent spoofing of a user or of the agent as well as **encryption** to prevent sniffing;
- placing **limitations on agent's autonomy** so to ensure the proper empowerment of the user

# HCI Approach Summary

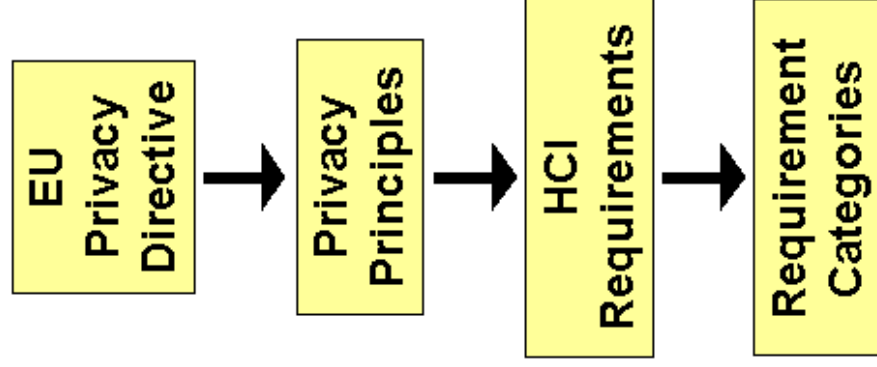
- **problem statement:**
  - Building an agent-based service that people will **trust** with sensitive, personal information and will operate according to privacy-protection **requirements** coming from **legislation** and **best practices**
  - “*Trust in Allah, but tie your camel.*” (Old Muslim Proverb)
- **two approaches:**
  - building **trustworthy** agents through system design
  - “**usable compliance**” with privacy legislation & principles

# Usable Compliance

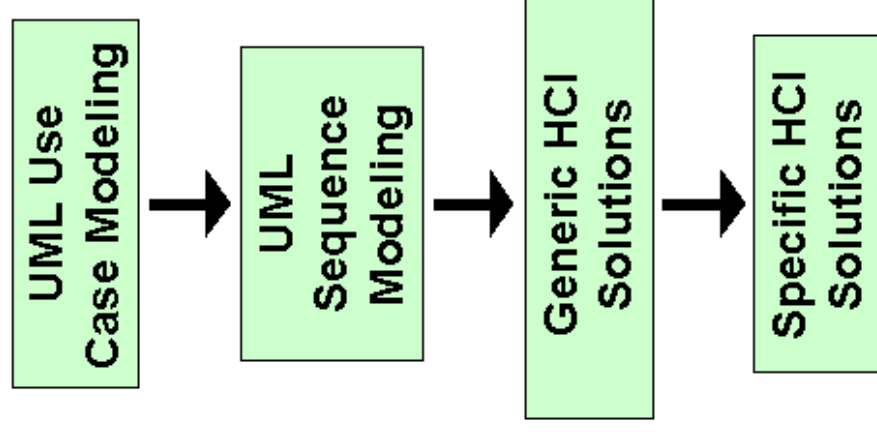
- an “**engineering psychology**” approach: use knowledge of cognitive processes to inform system design
- translate **legislative causes** into **HCI** implications and **design** specifications
- work with EU Privacy Directive and privacy **principles**
- document the process so it is understandable and repeatable

# Privacy Interface Analysis

## Analysis Development Sequence



## Analysis Application Sequence



# Ten Privacy Principles

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 against loss and unlawful processing

# Detailed Analysis Examples

Number	Basic Principle	HCI Requirement	Possible Requirement 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 <b>aware</b> of the transparency options, and feel empowered to <b>comprehend</b> and <b>control</b> how their PII is handled	during registration, transparency information is explained and examples or tutorials are provided
1.1	Data Subject (DS) inform: DS is aware of transparency opportunities	users must be <b>aware</b> of the transparency options	Opportunity to track controller's actions made clearly visible in the interface design
1.1.1	For: Personally Identifiable Information (PII) collected from DS. Prior to DS PII capture: DS informed of: controller Identity (ID) / Purpose Specification (PS)	users <b>know</b> 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 / 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 securi	users are <b>informed</b> of each processor who processes their data, and they users <b>understand</b> the limits to this informing	<ul style="list-style-type: none"> <li>- user agreements states that PII can be passed on to third parties</li> <li>- user agreement also contains information about usage tracking limitations</li> <li>- when viewing the processing logs, entries with limited information are color coded to draw attention, and use</li> </ul>



# HCI Requirement Categories

Consciousness

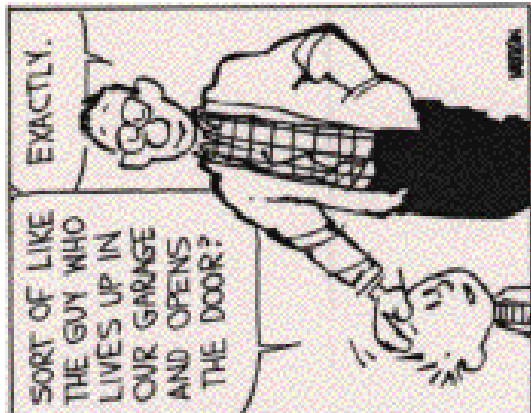
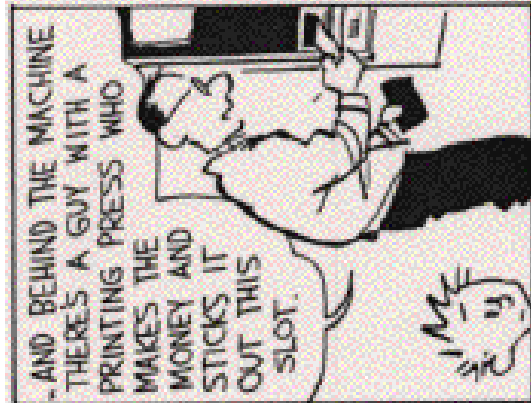
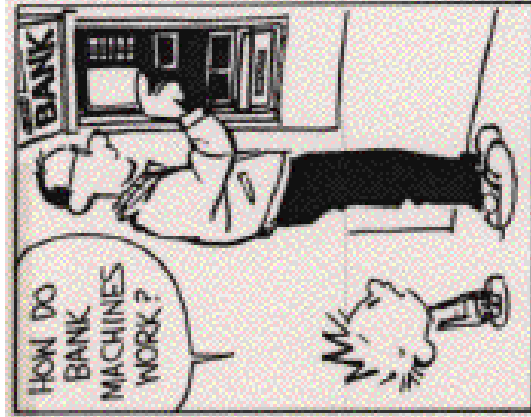
Comprehension



# Comprehension

Requirements	Possible Solutions
<ul style="list-style-type: none"><li>• <b>comprehend</b> how PII is handled</li><li>• <b>know</b> who is processing PII and for what purposes</li><li>• <b>understand</b> the limits of processing transparency</li><li>• <b>understand</b> the limitations on objecting to processing</li><li>• <b>be truly informed</b> when giving consent to processing</li><li>• <b>comprehend</b> when a contract is being formed and its implications</li><li>• <b>understand</b> data protection rights and limitations</li></ul>	<ul style="list-style-type: none"><li>• training</li><li>• documentation</li><li>• user agreements</li><li>• help</li><li>• tutorials</li><li>• <b>mental models</b></li><li>• <b>metaphors</b></li><li>• layout</li><li>• feedback</li></ul>

# Mental Models



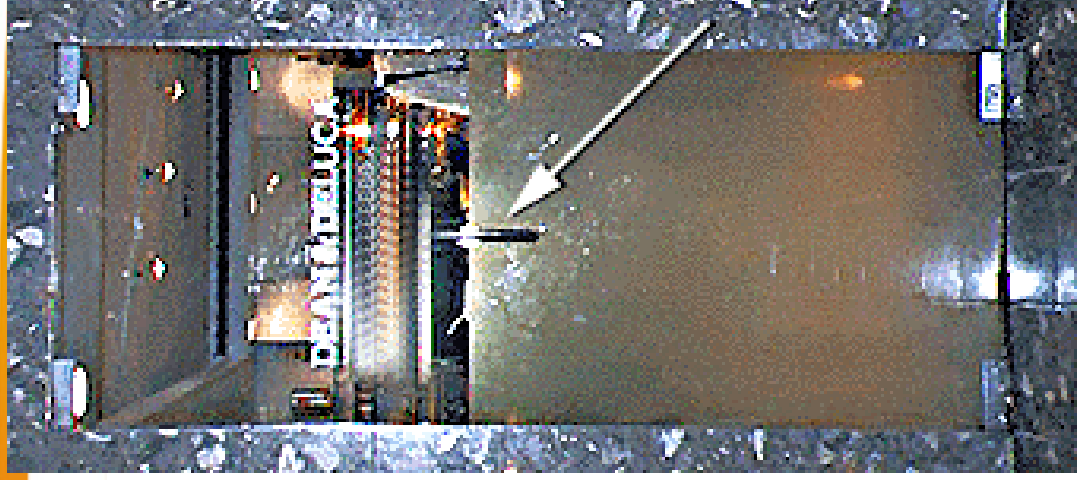
# Consciousness

Requirements	Possible Solutions
<ul style="list-style-type: none"><li>• be aware of transparency options</li><li>• be informed when PII is processed</li><li>• be aware of what happens to PII when retention periods expire</li><li>• be conscious of rights to examine and modify PII</li><li>• be aware when information may be collected automatically</li></ul>	<ul style="list-style-type: none"><li>• messages</li><li>• pop-up windows</li><li>• assistants</li><li>• layout</li><li>• highlight by appearance</li><li>• alarms</li></ul>

# Control

Requirements	Possible Solutions
<ul style="list-style-type: none"><li>• <b>control</b> how PII is handled</li><li>• <b>be able to object</b> to processing</li><li>• <b>control</b> how long PII is stored</li><li>• <b>be able to exercise</b> the rights to <b>examine and correct</b> PII</li></ul>	<ul style="list-style-type: none"><li>• <b>affordances</b></li><li>• <b>obviousness</b></li><li>• <b>mapping</b></li><li>• <b>analogy</b></li></ul>

# When Control is Hard




# Consent

Requirements	Possible Solutions
<ul style="list-style-type: none"><li>• give <b>informed consent</b> to the processing of PII</li><li>• give <b>explicit consent</b> for a Controller to perform the services being contracted for</li><li>• give <b>specific, unambiguous consent</b> to the processing of sensitive data</li><li>• give <b>special consent</b> when information will not be editable</li><li>• <b>consent</b> to the automatic collection and processing of information</li></ul>	<ul style="list-style-type: none"><li>• <b>user agreement</b></li><li>• <b>click-through agreement</b></li><li>• <b>“Just-In-Time Click-Through Agreements”</b></li></ul>

# Just-in-Time Click-Through Agreements

The screenshot shows a Microsoft Internet Explorer browser window titled "Create an agent - Microsoft Internet Explorer". The address bar displays "Entry of Personal Information - Microsoft Internet Explorer". The main content area contains a form titled "Trade Union Membership" with a dropdown menu set to "none" and two buttons: "Launch Agent" and "Reset Data".

A dialog box is overlaid on the browser window, containing the following text:

 You are about to enter information into a field that is of an extremely sensitive and personal nature.

Legislation dictates that you must agree to the processing of such information, should you wish to enter it at all.

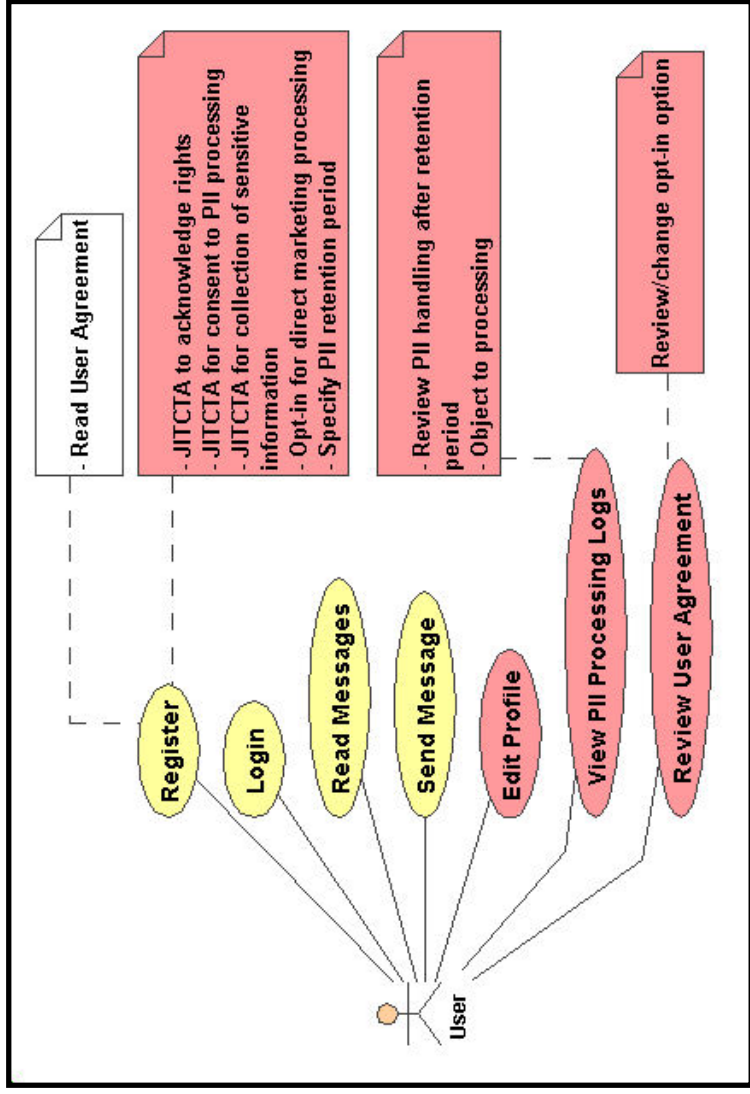
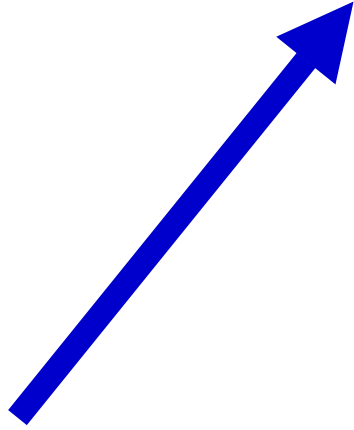
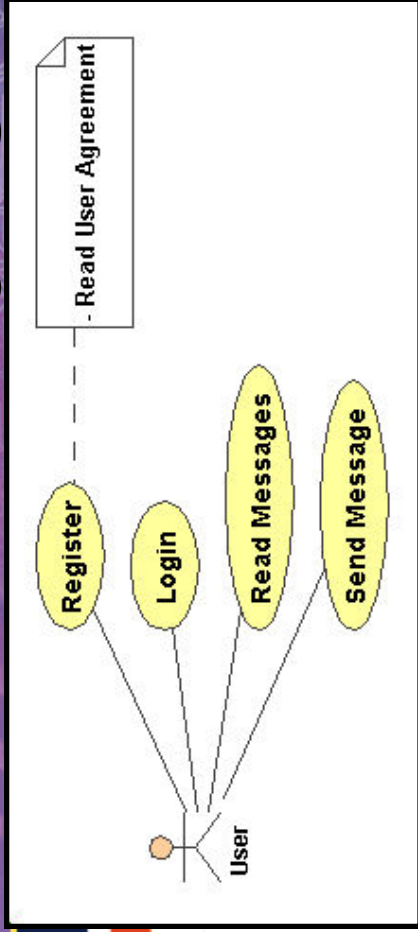
If you wish to agree to the processing of this information, please press "I agree". If you object to the processing of this information, please press "I do not agree". If you do not agree, this information will not be stored, and will not be processed.

[I Agree](#)      [I Do Not Agree](#)

The browser's status bar at the bottom shows "Done" and "My Computer".



# Applying the Solutions



# PISA Interface Prototype

- developed using DHTML, CSS, and CGI
- includes **simulated agent back-end** for realistic behaviors
- page design undergoing **user-testing & iterative refinements**
- **currently being integrated** into reference system

The screenshot shows a web browser window displaying the 'PISA Demonstrator Personal Agent Overview' page. The browser's address bar shows 'PISA Descriptions and Pages - Microsoft Internet Explorer'. The page features a navigation menu with links for Home, Create Agent, Modify Agent, Track Agent, Agent Results, Help, and Logout. A message at the top states: 'You have 111 message(s) waiting. Messages can be read by clicking on "Track Agent"'. The main content area is divided into several sections, each with a title and a description:

- Create Agent**: Create your profile, Set your handling preferences; Launch your new agent. (Icon: person at computer)
- Modify Agent**: Change Agent profile; Stop active agents; Adjust handling preferences. (Icon: person at computer)
- Track Agent**: View agent history; Receive agent messages; Object to agent actions. (Icon: person at computer)
- Agent Results**: View the results of your job search. (Icon: person at computer)
- Help**: Consult the help section for answers to your questions. (Icon: person at computer)
- My Profile**: Update your profile and change your privacy settings. (Icon: person at computer)

Below the main content area, there are five numbered items, likely representing a list of features or instructions:

1. this is the main overview page
2. the interface design theme is based on three types of needs: overview, focus and control, details on demand
3. goal is to provide obvious access to all control functions
  - 1. is a stronger model or metaphor of agent functionality needed?
4. the tabs across the top represent the major control functions
  - 1. the left-to-right ordering shows the most likely use sequence
  - 2. a forcing function is used so that the later agent functions (i.e., modify agent) are not active until an agent is created
5. visual icons for the major functions are introduced, and will be used in all screens associated with that function (e.g., the Show Profiles icon in all tracking screens) the links across the page are prior to an understanding of the functions

At the bottom of the page, there is a link: '5. links across the button provide ability to review important information (not shown)'. The browser's status bar at the bottom indicates the time as 11:40 AM.

# Design Highlights

- security/trust measure **obvious** (logos of assurance)
- consistent visual design, **metaphors**
- conservative appearance
- **functional** layout
- overview, focus & control, details on demand
- **sequencing** by layout
- **embedded help**
- confirmation of actions
- **reminders** of rights, controls
- double **JITCTA** for specially sensitive information
- **obvious** agent controls (start, stop, track, modify)
- controls for setting, customizing, modifying privacy **preferences** and **controls** (e.g., retention period)
- visual design to **emphasize** transparency limits
- objection controls **obvious** by layout

# Usability Analysis

- being conducted with Cassandra Holmes, Human Oriented Technology Lab, Carleton University
  - M.A. thesis comparing local and remote usability test methods
  - only tested creating and launching a job-searching agent
- preliminary findings (college undergraduates)...
- Utility & Appearance
  - The prototype worked fairly well (72%) and was easy to navigate (76%), but it had poor visual appeal (42%)

# Usability Analysis Results: Usable Compliance

- **Comprehension**
  - users had trouble understanding privacy concepts and the need for protection (e.g., ability to track and modify data, retention period)
- **Consciousness**
  - many users appreciated reminding when key steps are taken (e.g., empowering agent to act on their behalf), but some did not
- **Control**
  - users generally able to use forms and widgets
- **Consent**
  - mixed results with JITCTAs: some appreciated pop-up agreement when sensitive information entered, others found it annoying, or ignored it (“all pop-up windows are advertisements”)

# Usability Analysis Results: Trustworthiness

- **Trust with Personal Information**
  - Whereas only 54% willing to send personal information on the Internet at large, 84% would provide their resume to the prototype, 80% would provide their desired salary, and 70% would provide name, address, and phone number.
- **Trustworthiness**
  - Whereas only 34% thought that Internet services at large acted in their best interest, 64% felt that the prototype service would act in their best interest.