NRC · CNRC

From Discovery to Innovation...

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

Andrew S. Patrick

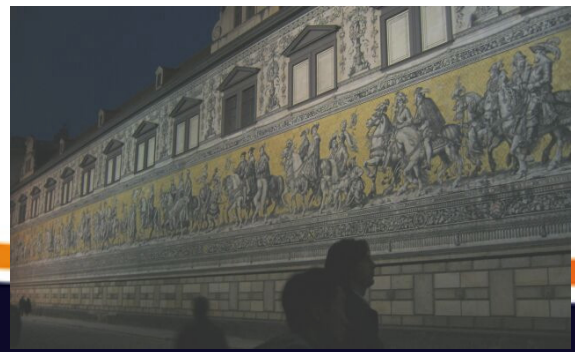
National Research Council of Canada

www.andrewpatrick.ca

Steve Kenny

Independent Consultant

stephen_mh_kenny@yahoo.com



PET Workshop, Dresden, March 27, 2003

PISA: Privacy Incorporated Software Agent

European Commission 5th Framework Project

- international R&D consortium
- 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

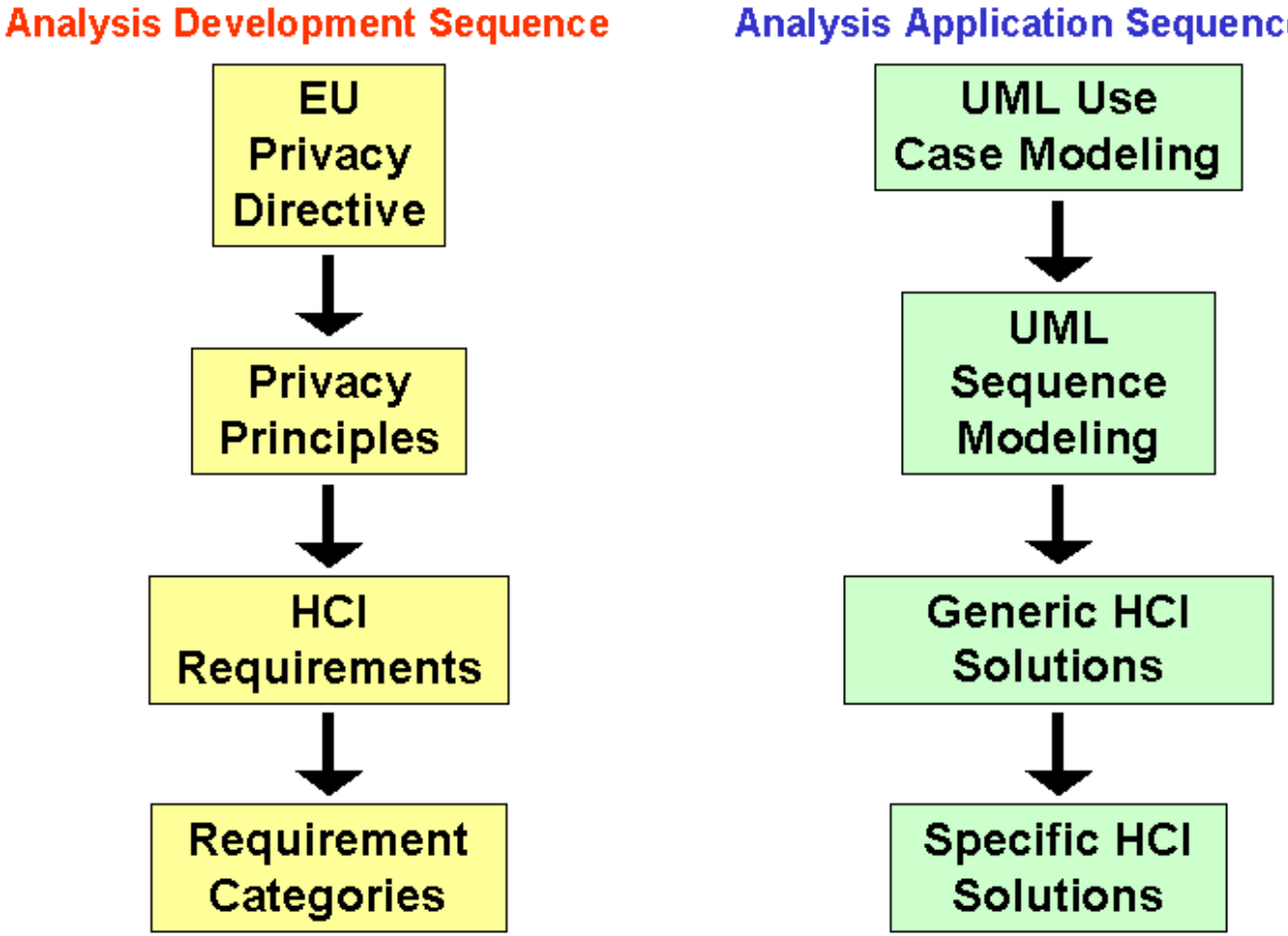
HCI Approach Summary

- **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



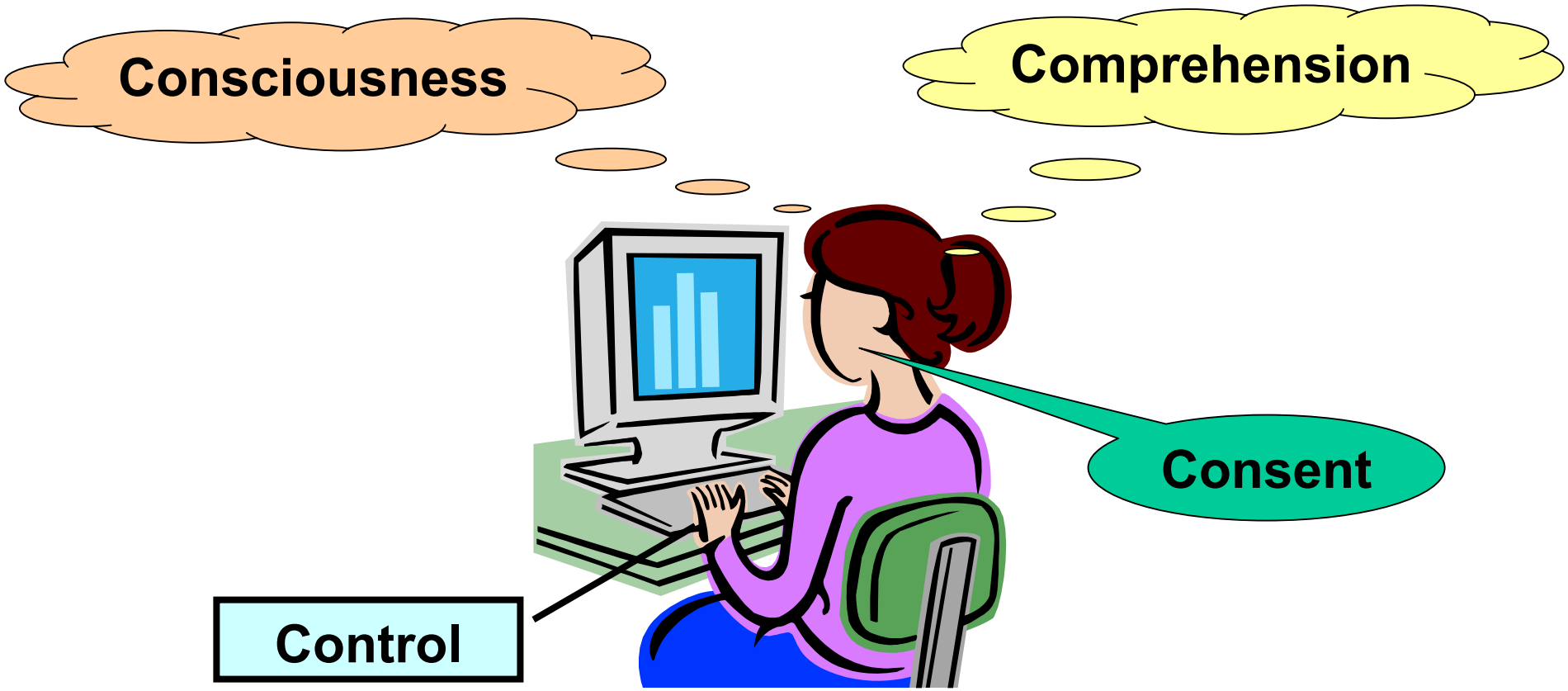
Ten Privacy Principles

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 **aware** of the transparency options, and feel empowered to **comprehend** and **control** 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 **aware** 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 **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 / 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 **informed** of each processor who processes their data, and they 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 color coded to draw attention, and use

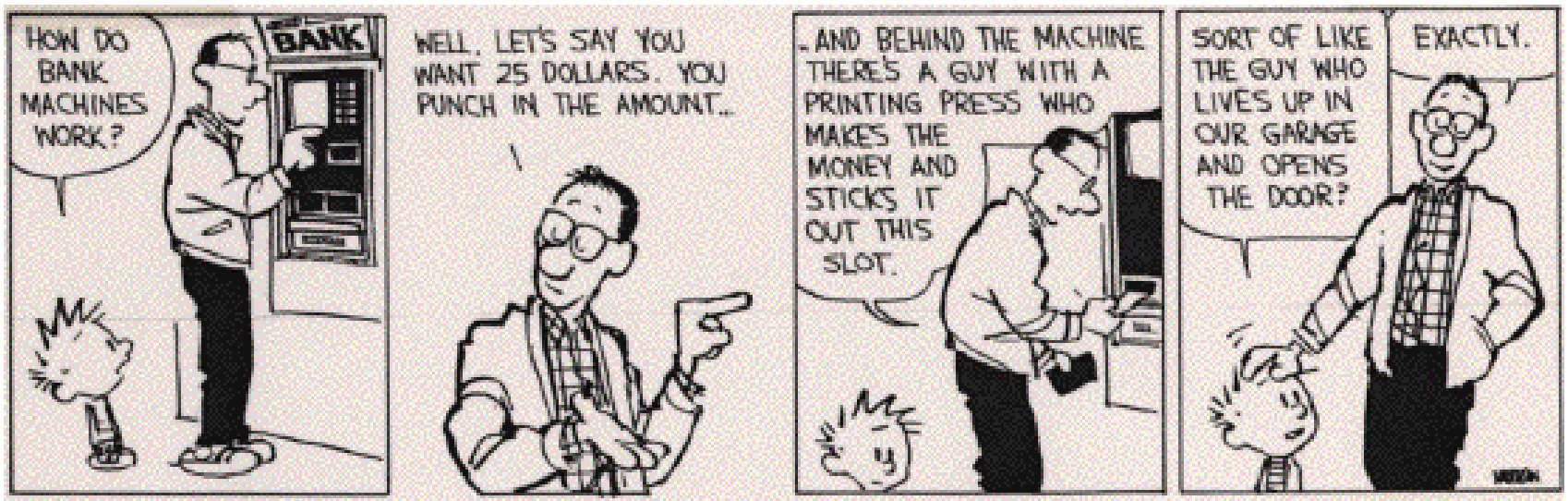
HCI Requirement Categories



Comprehension

Requirements	Possible Solutions
• **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**	• training • documentation • user agreements • help • tutorials • mental models • metaphors • layout • feedback

Mental Models



Consciousness

Requirements	Possible Solutions
• 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	• messages • pop-up windows • assistants • layout • highlight by appearance • alarms

Control

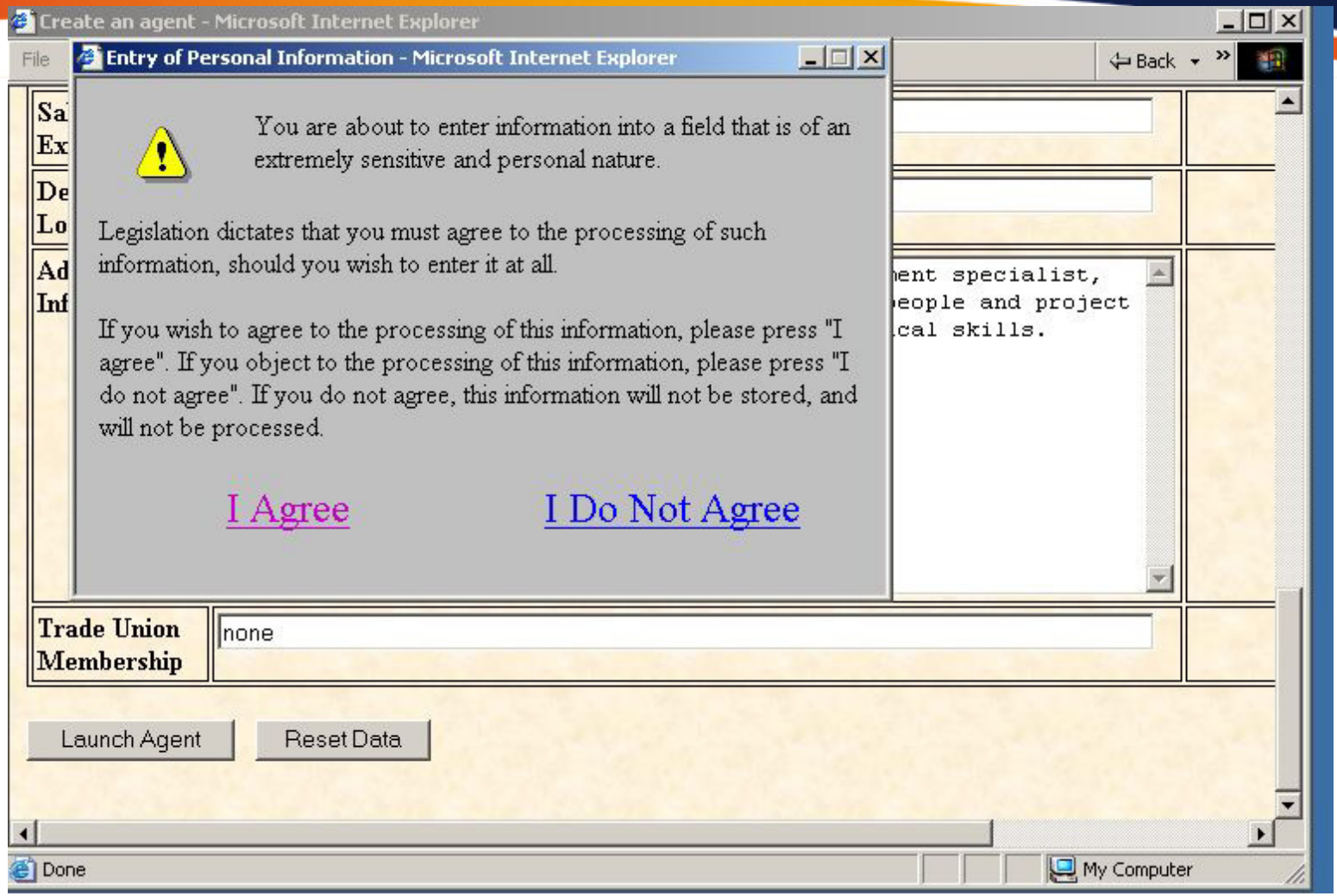
Requirements	Possible Solutions
• control how PII is handled • be able to object to processing • control how long PII is stored • be able to exercise the rights to examine and correct PII	• affordances • obviousness • mapping • analogy

When Control is Hard

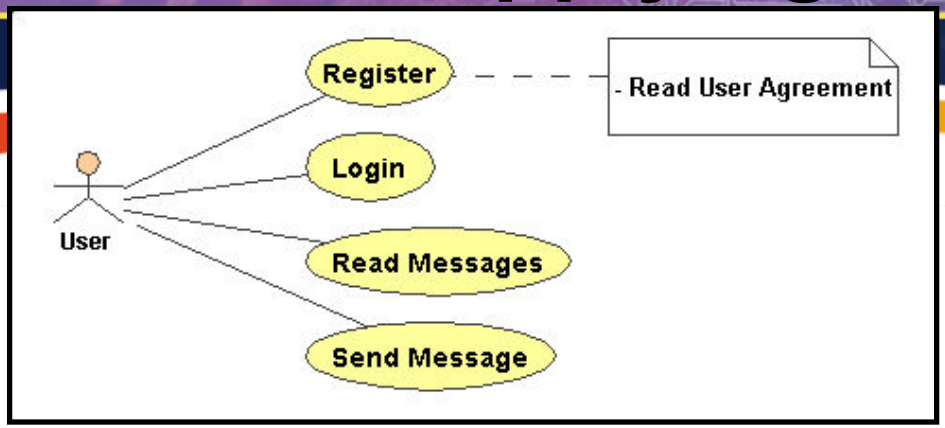
Consent

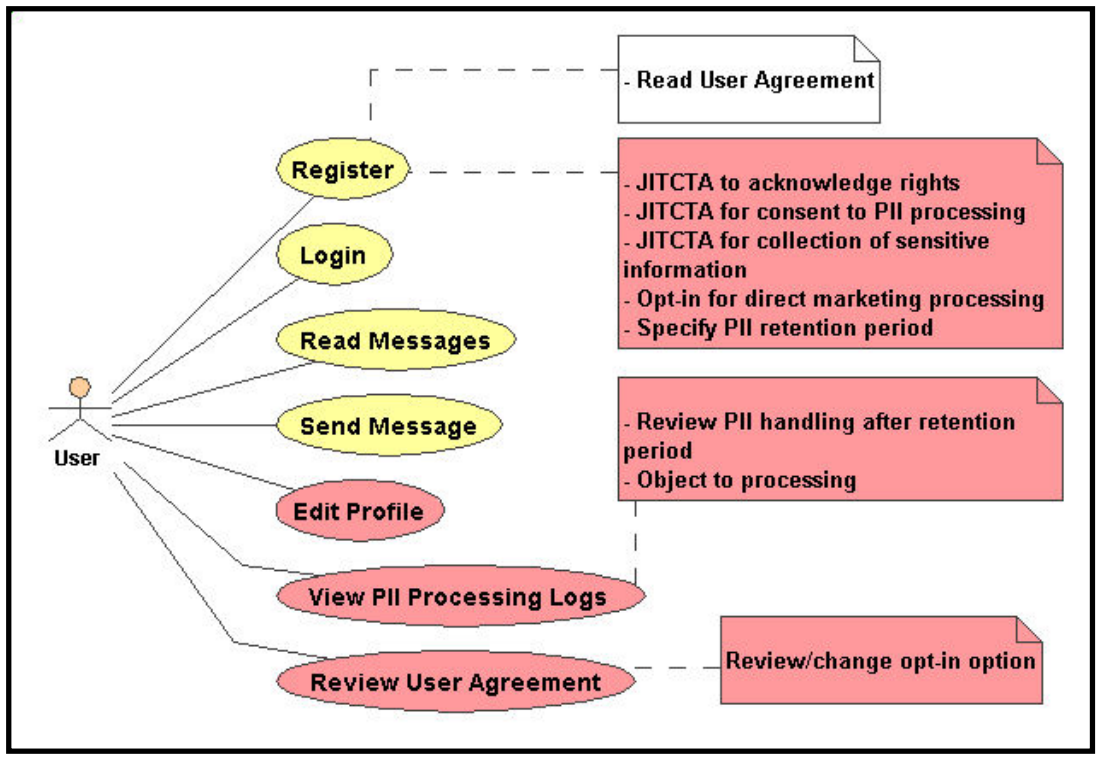
Requirements	Possible Solutions
• give **informed consent** to the processing of PII • give **explicit consent** for a Controller to perform the services being contracted for • give **specific, unambiguous consent** to the processing of sensitive data • give **special consent** when information will not be editable • **consent** to the automatic collection and processing of information	• user agreement • click-through agreement • **"Just-In-Time Click-Through Agreements"**

Just-in-Time Click-Through Agreements



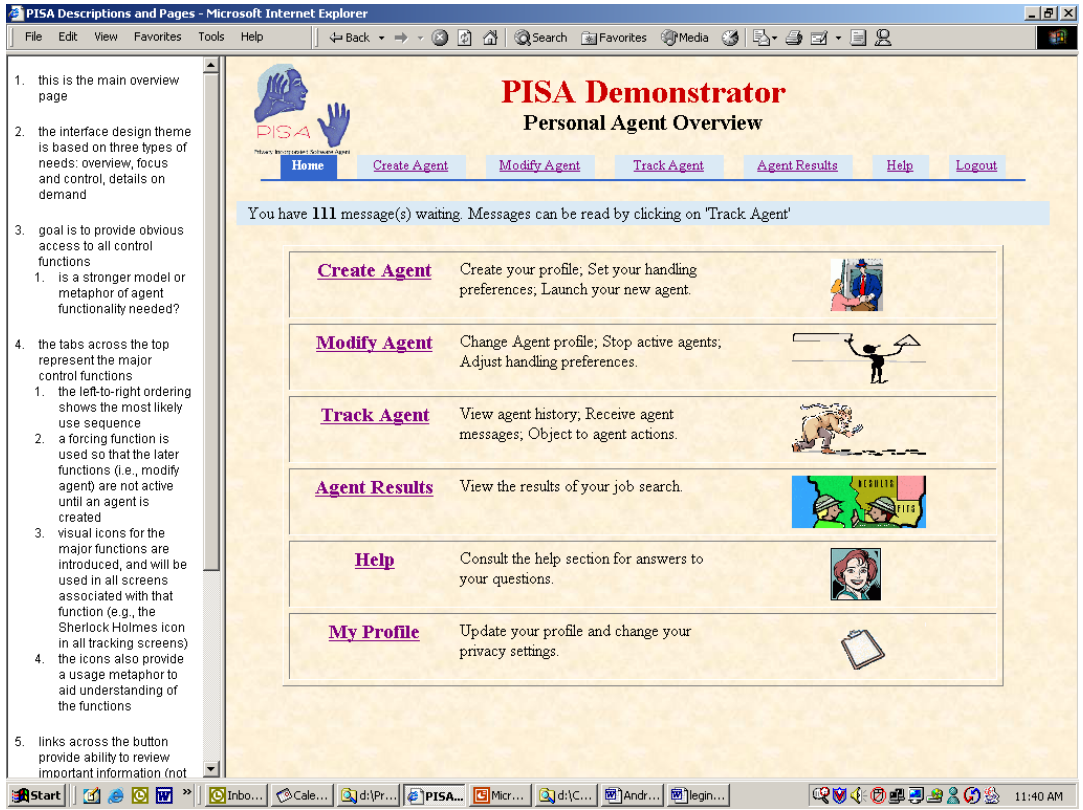
Applying the Solutions





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



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.