

# Human Factors of Privacy Protection

**Andrew Patrick, Ph.D.**

**Network Computing Group**

**Institute for Information Technology**

**E-mail: [Andrew.Patrick@nrc-cnrc.gc.ca](mailto:Andrew.Patrick@nrc-cnrc.gc.ca)**

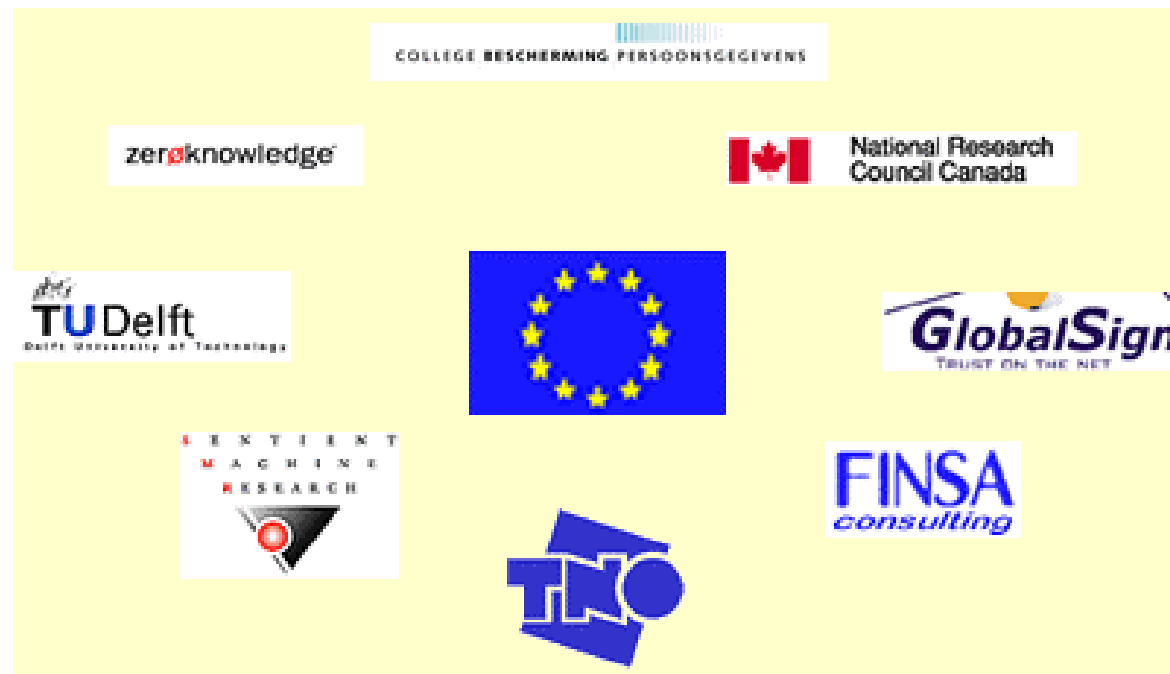
**WWW: [www.andrewpatrick.ca](http://www.andrewpatrick.ca)**

January 28, 2003

# PISA: Privacy Incorporated Software Agent

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

- international R&D consortium
- 3.2 M Euros over 3 years
- [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

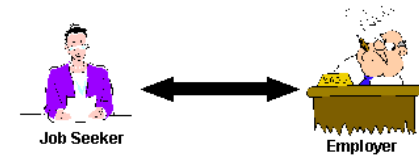
# HCI Approach Summary

- **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

# Trust and Agents

- **trust is...**
  - users' thoughts, feelings, emotions, or behaviors that occur when they feel that an agent can be relied upon to act in their best interest when they give up direct control.
- **trusting agents is hard because...**

Non-Removed Transaction



Once-Removed Transaction

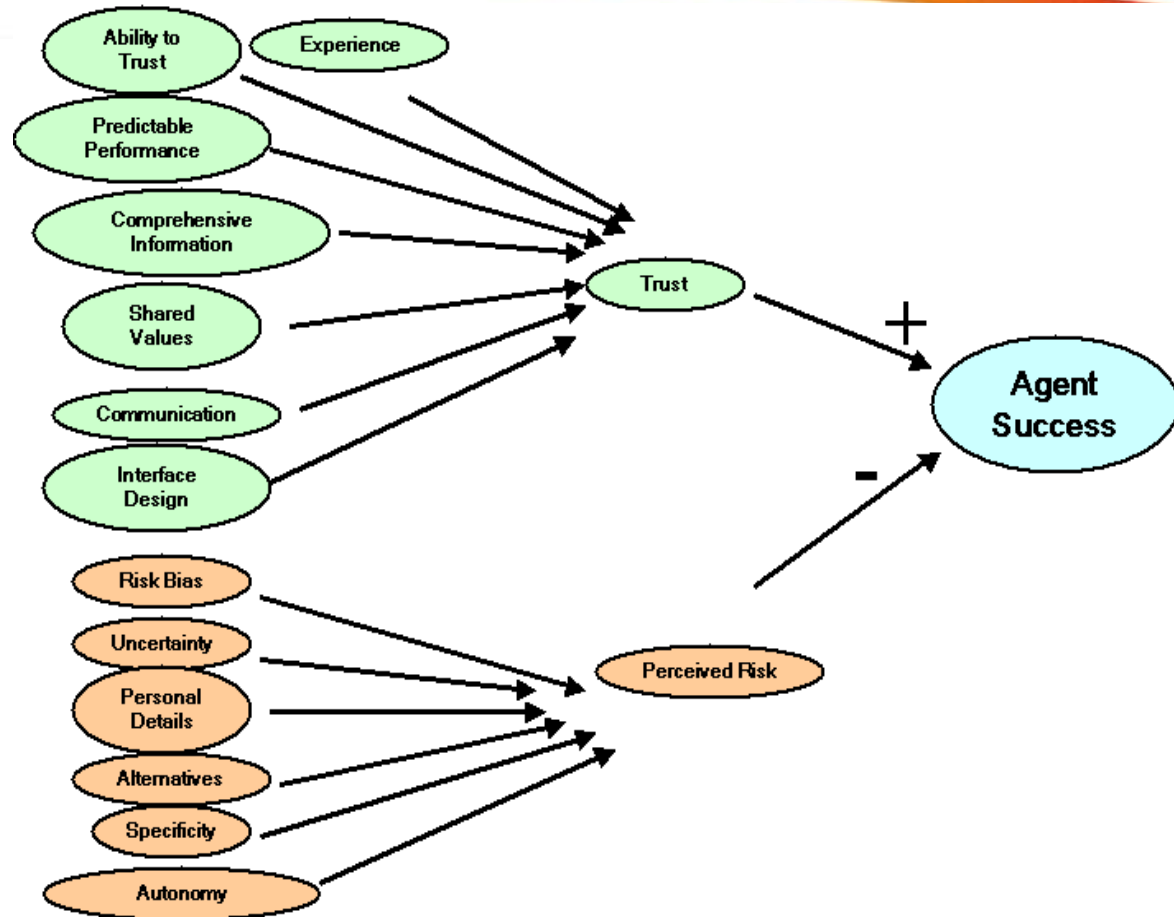


Twice-Removed Transaction



# Building Trustworthy Agents

- model of agent acceptance:
  - **design factors** contribute to feelings of trust & perceptions of risk
  - **trust** and **risk** together determine final acceptance



# Major Trust Builders/Busters

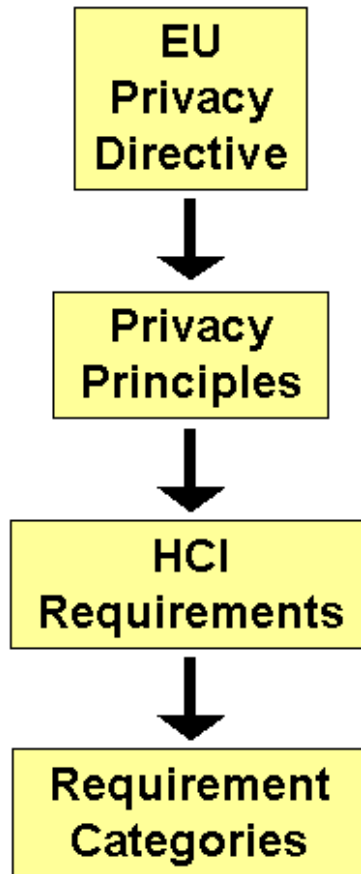
- **ability** to trust/risk perception **bias**
- **experience**: direct and indirect
- **performance**: consistency, integrity, stability
- **information** about operations, feedback, tracking; reduce uncertainty
- interface **appearance**: brand, navigation, fulfillment, presentation, colors, brightness, graphics
- **perceived risk**: personal details, alternatives, autonomy

# Usable Compliance

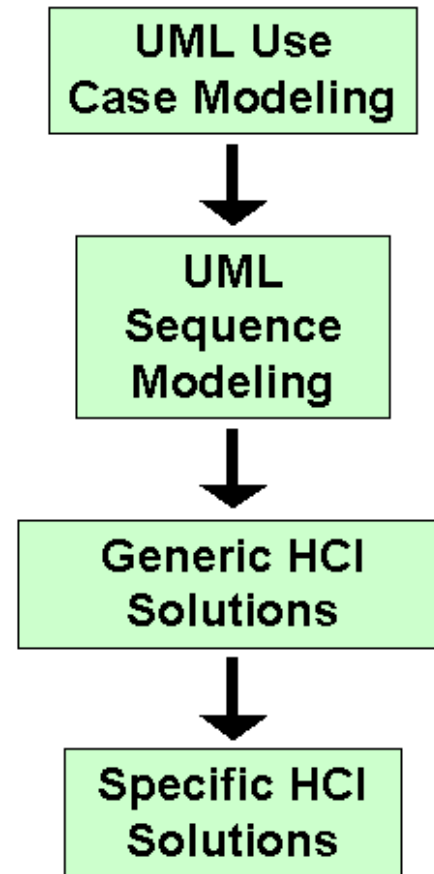
- in collaboration with **Steve Kenny**, Dutch Data Protection Authority (now independent contractor)
- use “**engineering psychology**” approach: use knowledge of cognitive processes to inform system design
- translate **legislative causes** into **HCI** implications and **design** specifications
- 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**

**Consent**

**Control**



# Comprehension

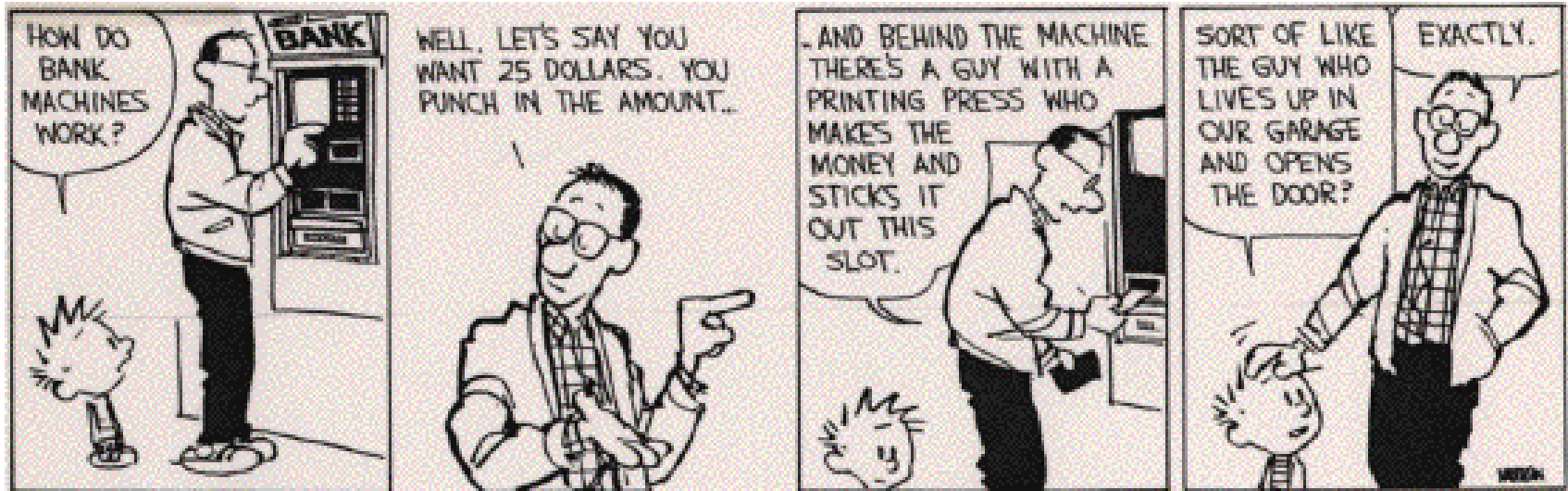
## Requirements

- **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

## Possible Solutions

- training
- documentation
- user agreements
- help
- tutorials
- **mental models**
- **metaphors**
- layout
- feedback

# Mental Models



# Consciousness

## Requirements

- 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

## Possible Solutions

- messages
- pop-up windows
- assistants
- **layout**
- **highlight by appearance**
- alarms

# Control

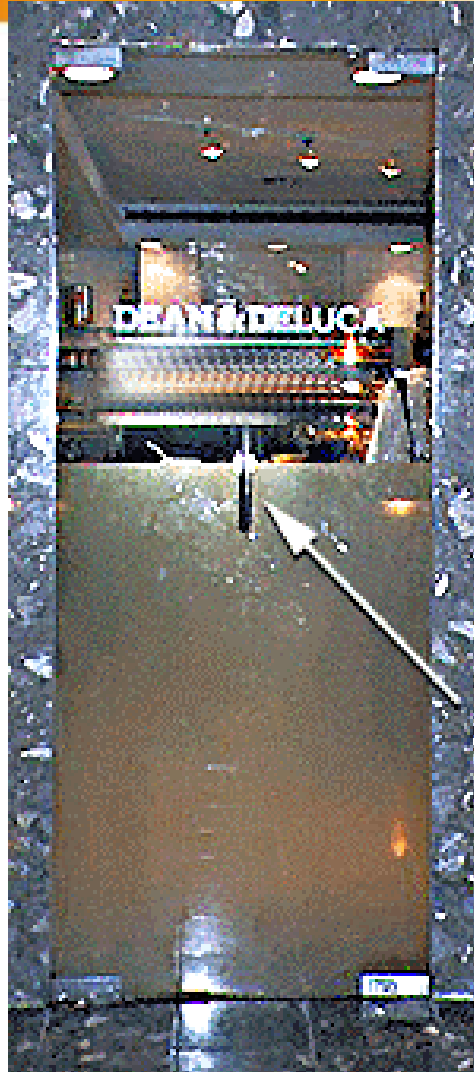
## Requirements

- **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

## Possible Solutions

- **affordances**
- **obviousness**
- **mapping**
- **analogy**

# When Control is Hard



# Consent

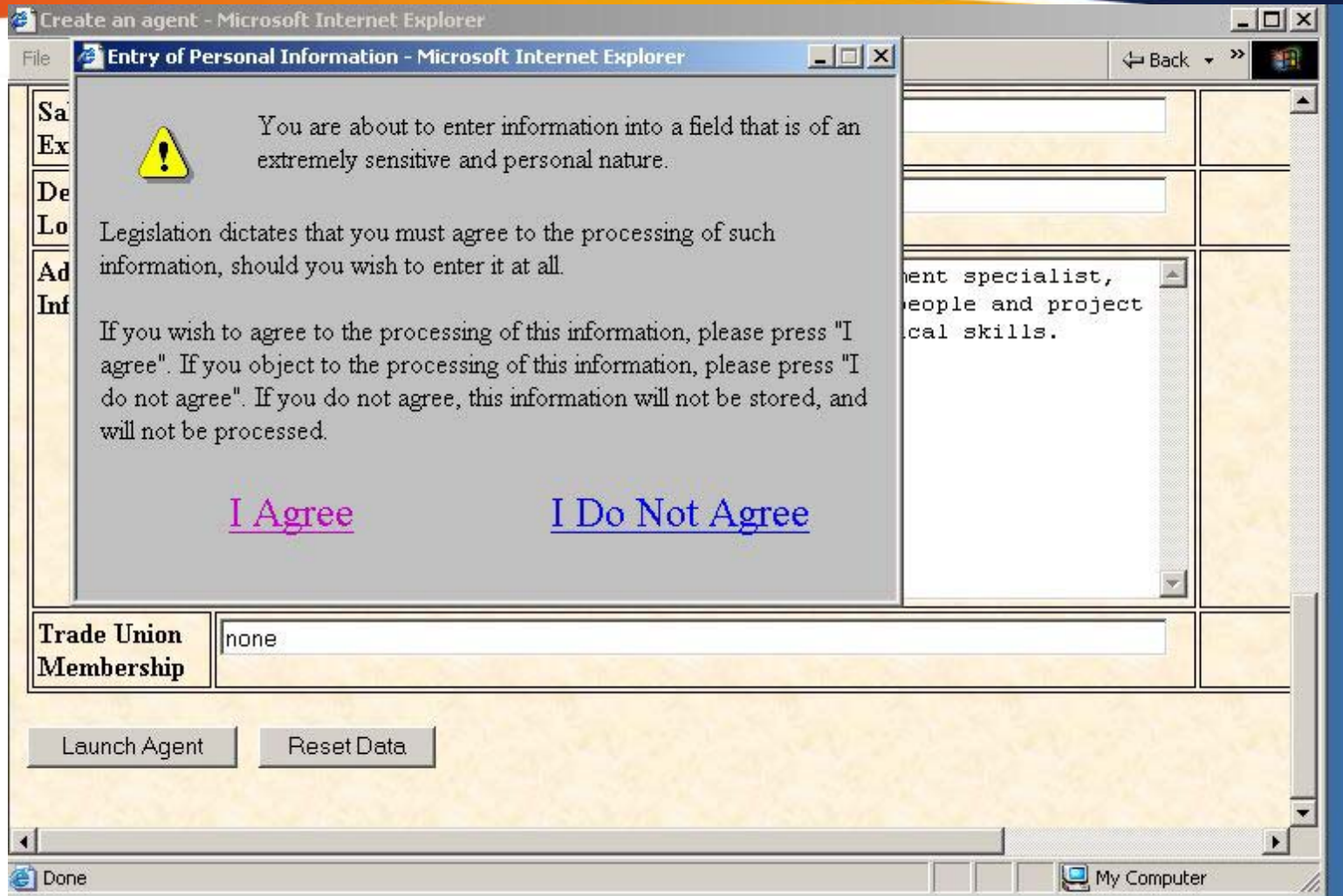
## Requirements

- 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

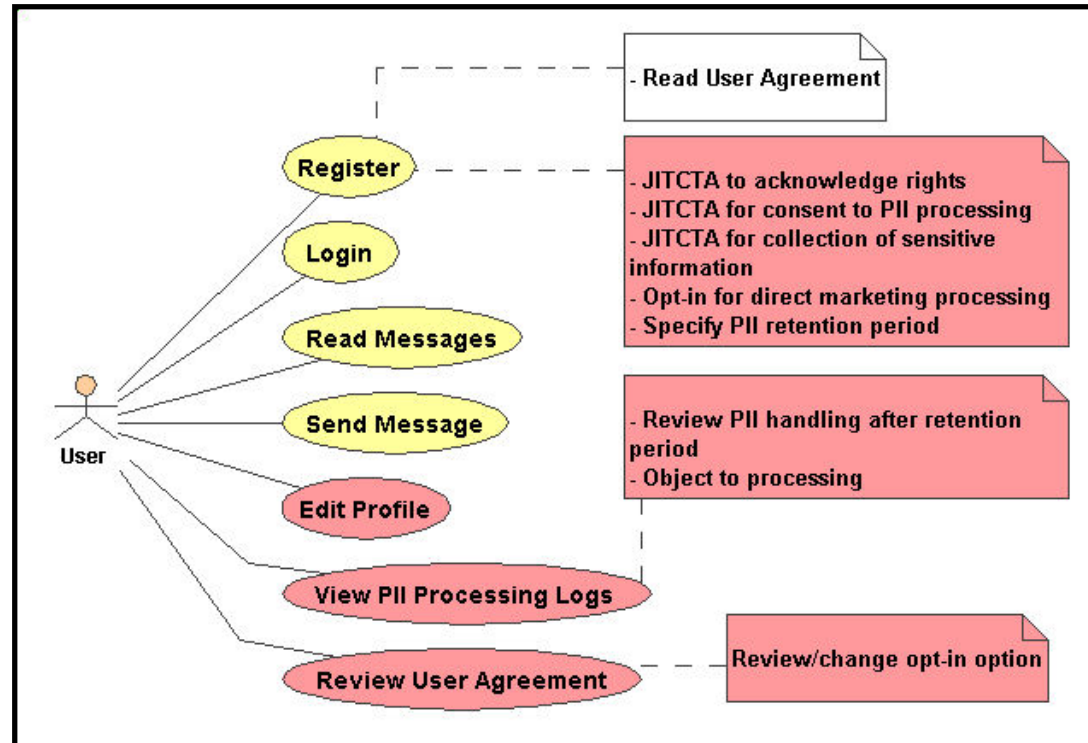
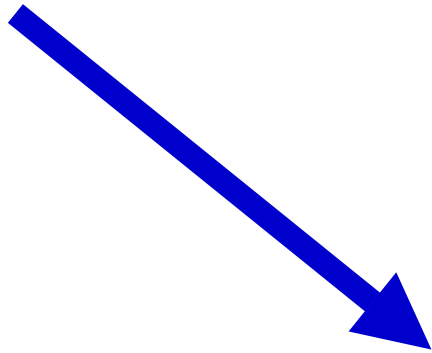
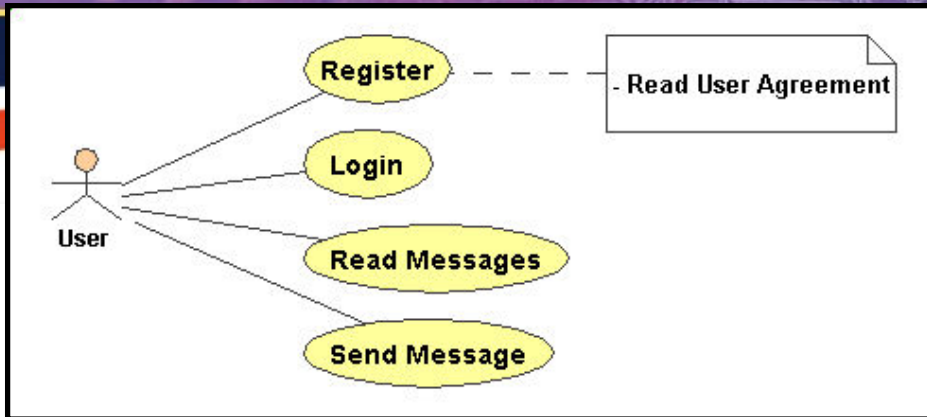
## Possible Solutions

- user agreement
- click-through agreement
- “**Just-In-Time Click-Through Agreements**”

# Just-in-Time Click-Through Agreements

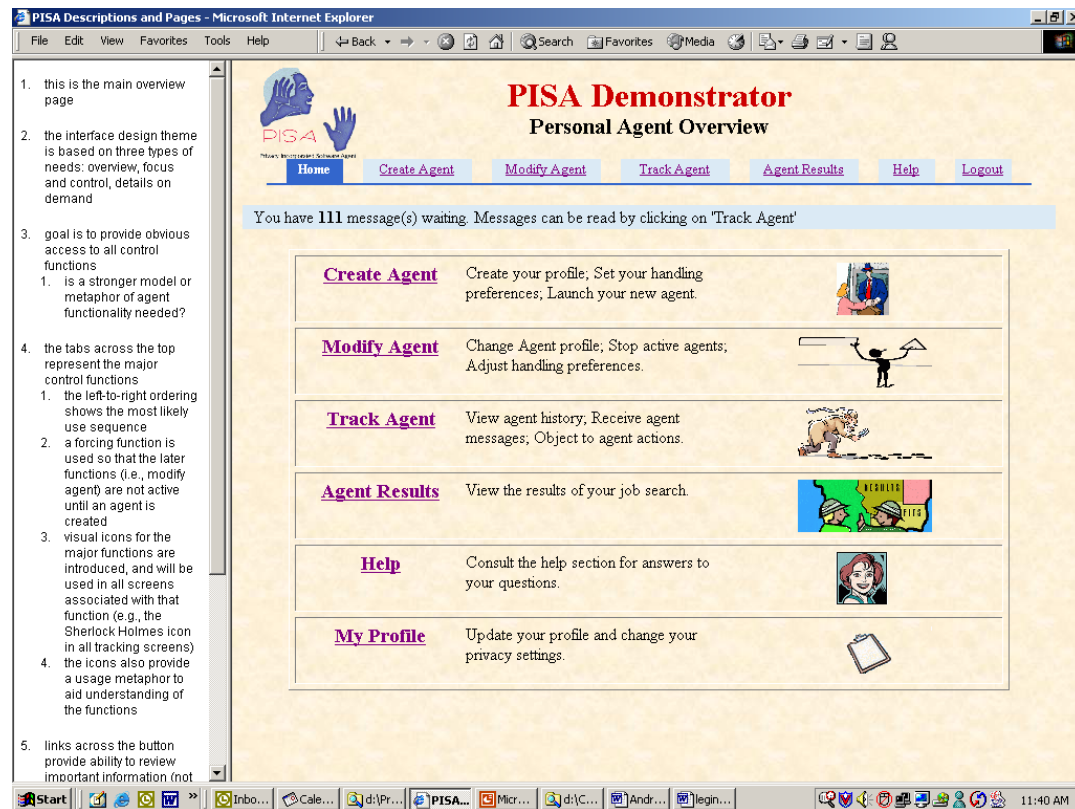


# Applying the Solutions



# 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