NRC · CNRC

From Discovery to Innovation...

Protecting Privacy in Software Agents: Lessons from the PISA Project

Andrew Patrick

National Research Council of Canada

http://www.andrewpatrick.ca

PISA Project

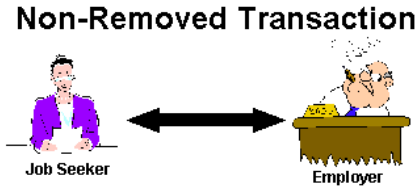
- Privacy Incorporated Software Agents (www.pet-pisa.nl)
- 3 years, 3 million Euros, 7+ partners, 20 researchers

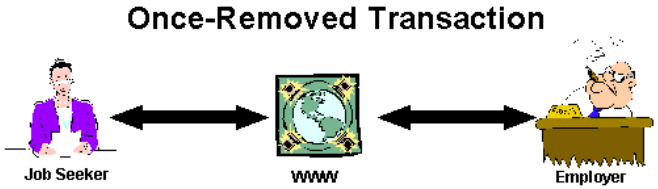
PISA Topics

- **privacy: definitions, types of data, legal roles, preferences and policies, privacy principles, privacy threat analysis**
- **privacy-enhancing technologies (PETs): types, legal grounds, Common Criteria, privacy-by-design**
- **agent technologies: definition, types, intelligence, control, integrating agents and PETs**
- **agents in an untrustworthy environment: confidentiality, integrity, theoretical boundaries**
- **design methods: prevention or minimization, privacy regulations**
- **PKI for agents: architecture, functional descriptions**
- **PISA architecture: anonymity, pseudo-identities, agent practices statements**
- **anonymous communications: network scaling**
- ***building trustable agents: factors contributing to trust, factors contributing to perceived risk***
- ***human-computer interaction: from privacy legislation to interface design, usability testing***
- **data mining: fair information practices, data recognizability, data mining threats, data mining to defend privacy, mining anonymous data**
- **evaluation and auditing: privacy audit framework, legal requirements**
- **PISA Demonstrator: job searching agents, implementation of privacy concepts, software components, ontology**

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.

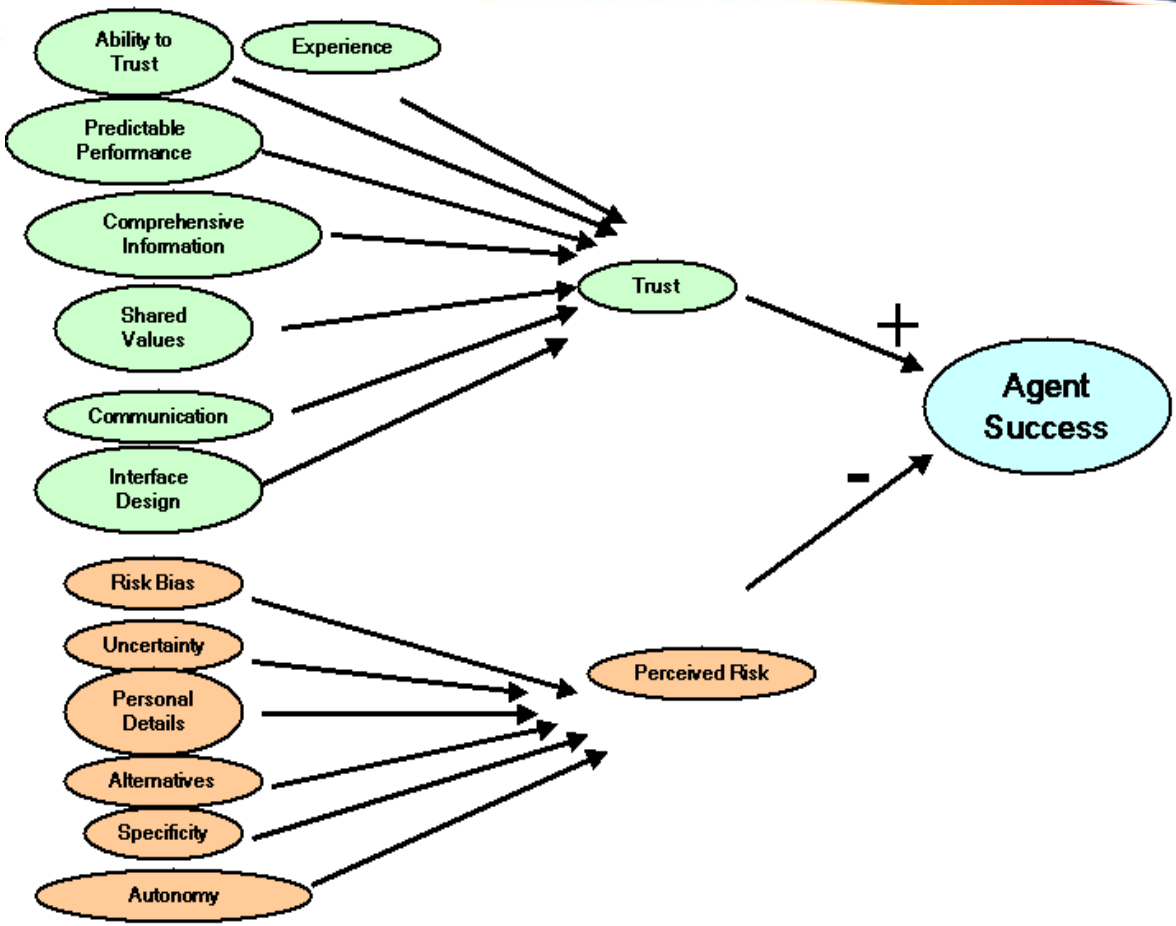




- **trusting agents is hard because...**

Building Trustworthy Agents

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



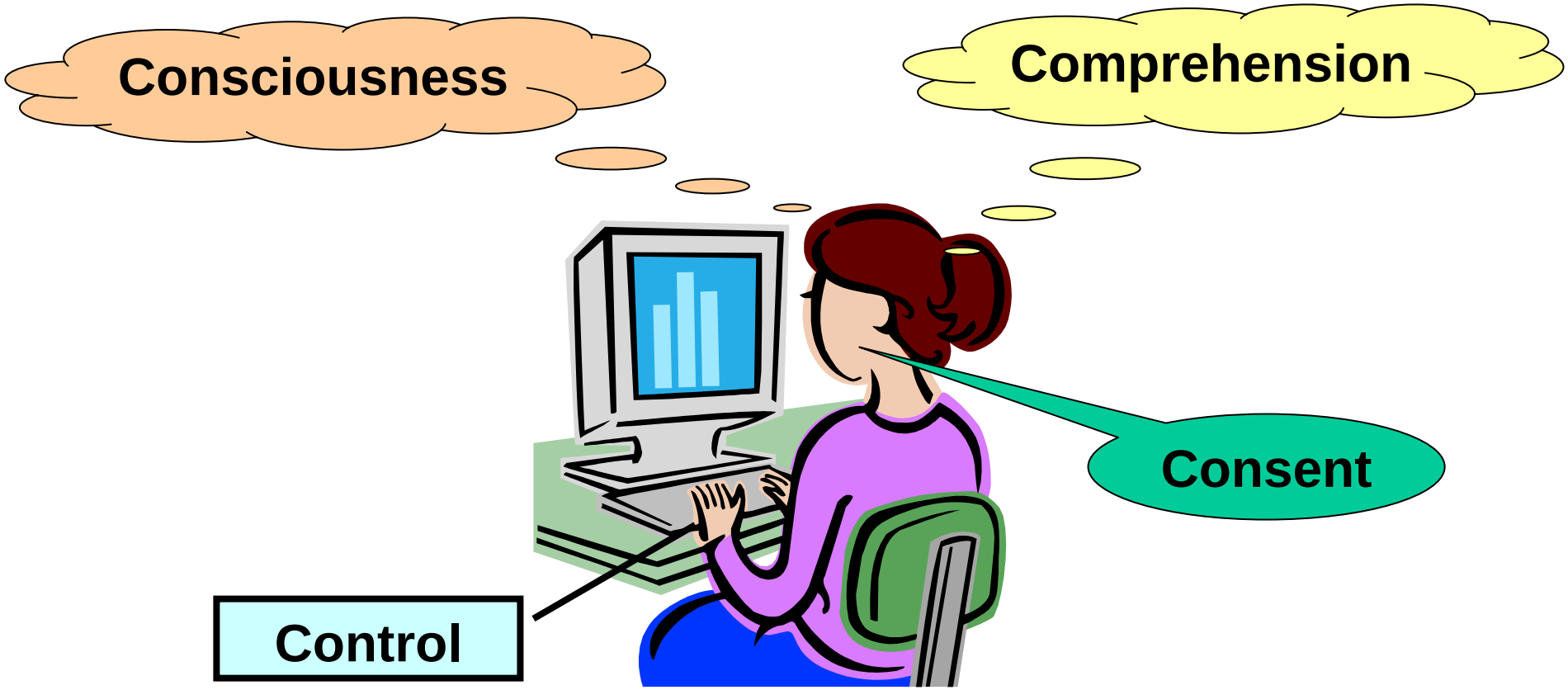
Major Trust Builders/Busters

- 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

HCI Requirement Categories



Design Highlights

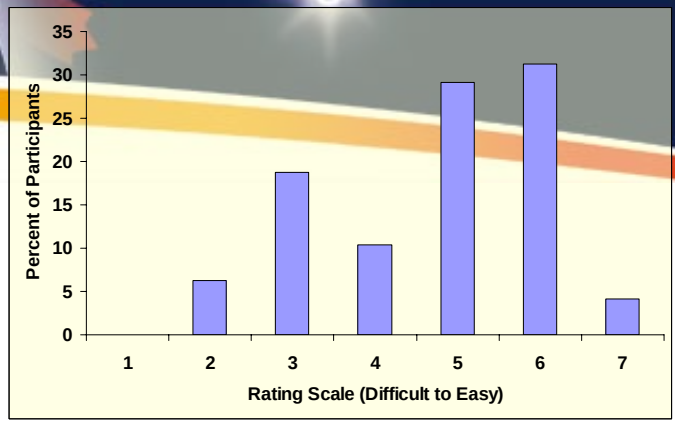
- security/trust measure obvious (logos of assurance)
- consistent visual design, metaphors
- conservative appearance
- functional layout
- overview, focus & control, details on demand
- sequencing by layout
- embedded help
- confirmation of actions
- reminders of rights, controls
- double JITCTA for 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

User Interface Testing Method

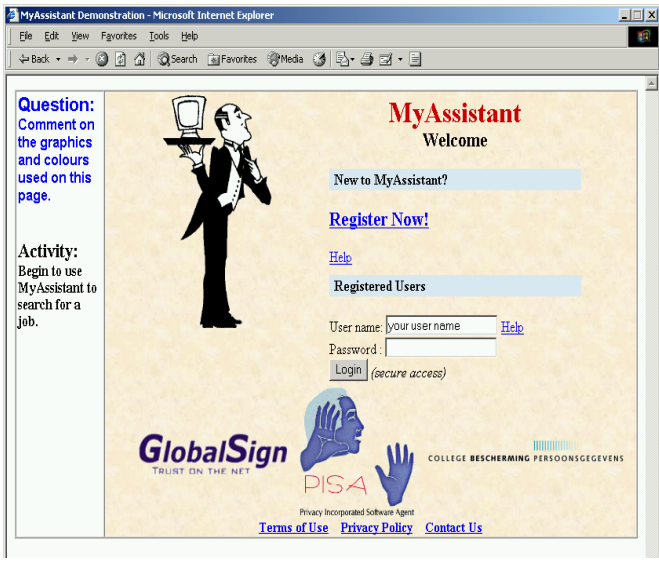
- M.A. thesis on remote usability testing (Cassandra Holmes, Carleton U)
- 50 participants tested either in same room, or different room communicating via audio or text channels
- task information and usability probes presented in left-hand frame of browser
- trustability questionnaire completed after usability test

Human Oriented Technology Lab

Usability Results



- the prototype worked fairly well (72%) and was easy to navigate (76%), but it had poor visual appeal (42%)
  - 42% did not like colors
  - 38% did not like graphics
  - 88% liked the fonts
- users understood the concept of a personal assistant who could provide services (92%)
- users understood (>90%) the major functions (create, modify, track, results)



Usability of Privacy Controls

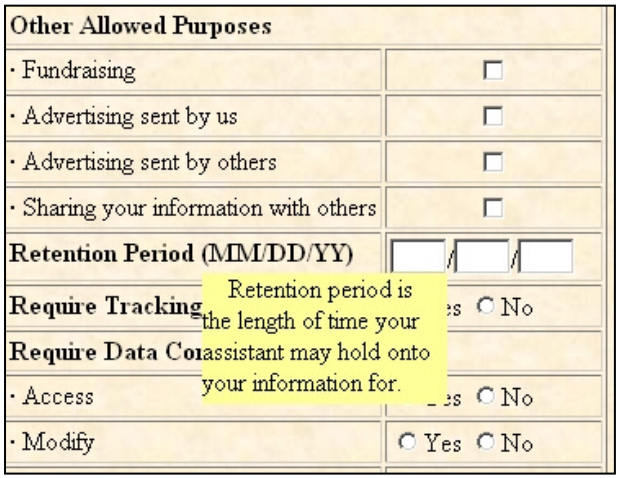
- users had trouble associating the privacy protection options with the information they entered, but this improved by the time contact information was entered (third input screen)

- roll-over help worked (86%)

- with help, users generally understood (>80%) privacy control terms (retention period, require tracking)

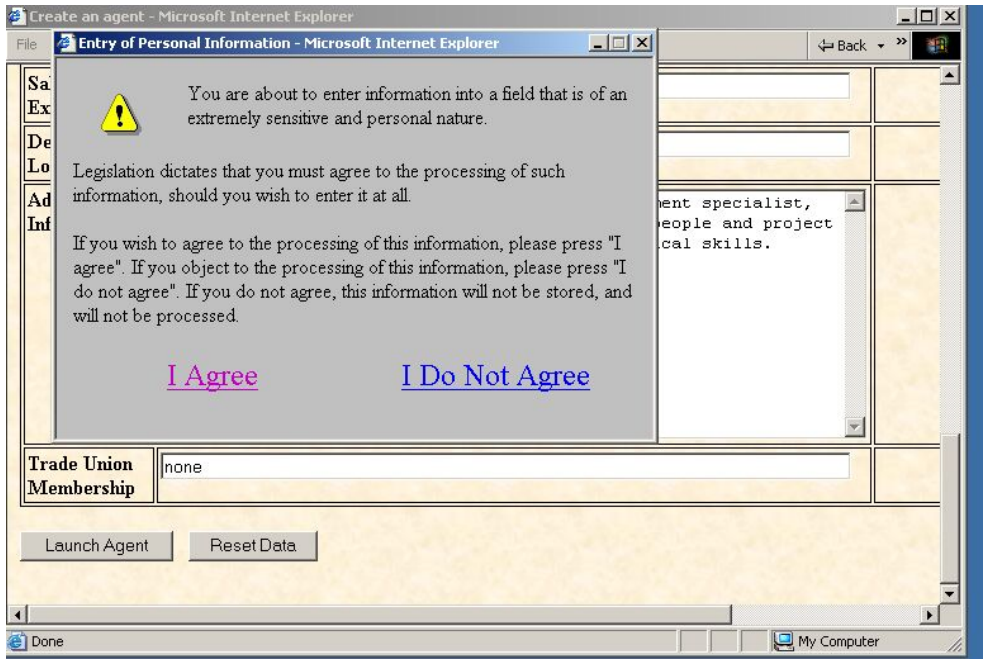
- result of checkboxes and fields not always clear (opt-in or out?)

- pre-set combinations were not noticed or were confusing



Just-in-Time Click-Through Agreements

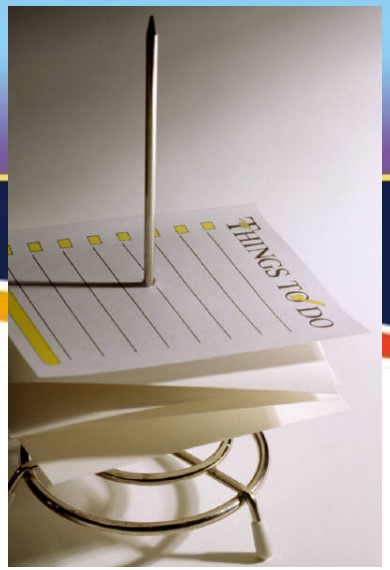
- **mixed results with JITCTAs: some appreciated pop-up agreement when sensitive information entered, others found it annoying, or ignored it ("*all pop-up windows are advertisements*")**



Trustability Questionnaire

- some evidence of increase in trustability:
- Whereas only 54% of participants were 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.
- 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.
- but are participants telling us what they think we want to hear?

UI Recommendations



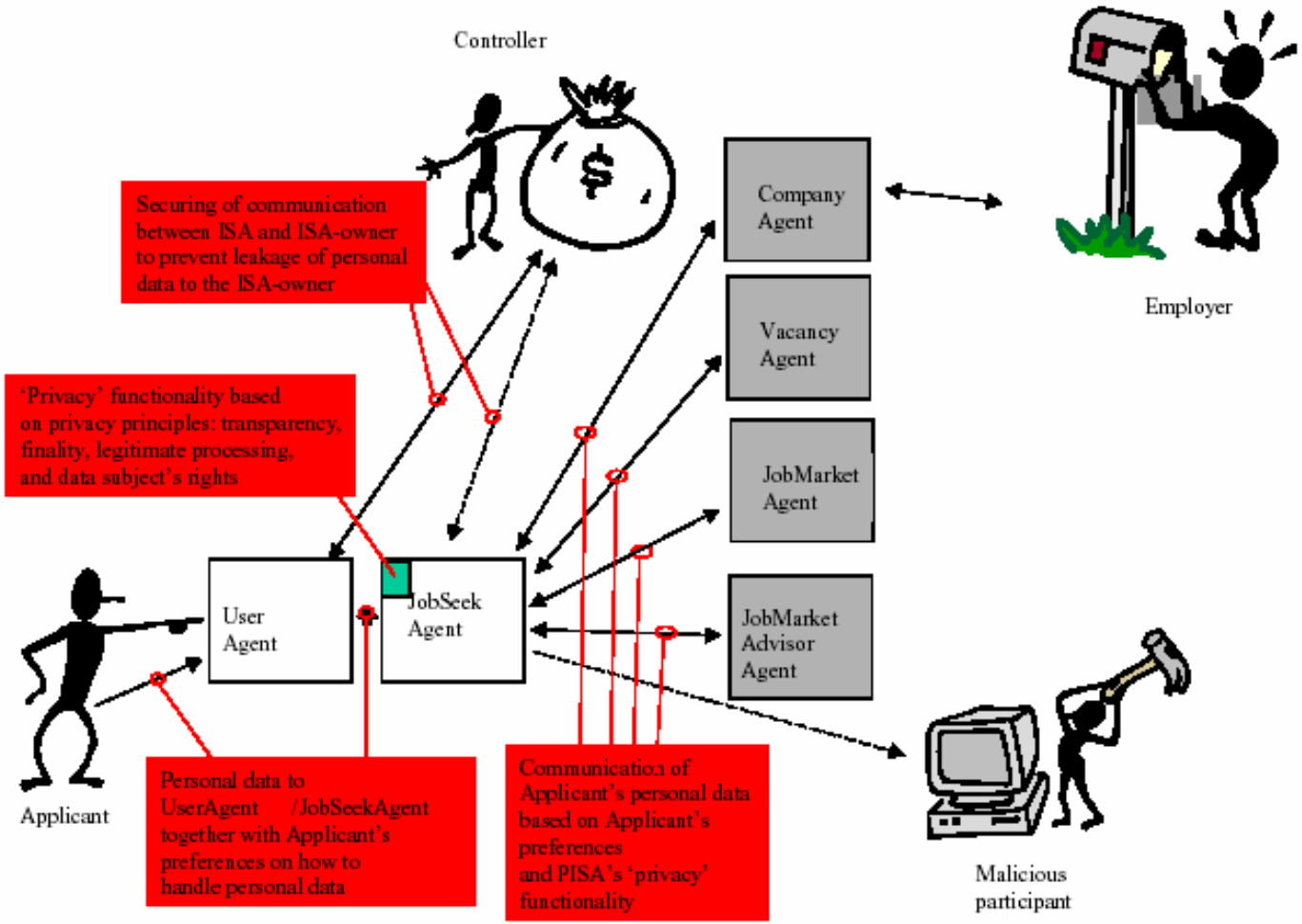
- improve terminology
- rework visual design
- improve registration and login
- rework privacy control screens
  - make association with private information more obvious
  - enter most-sensitive contact information first
- rework JITCTAs
  - change appearance so they are not confused with advertisements
- focus future testing on tracking and objecting

Back-Up

Privacy Protection by…

- anonymity and pseudo-identities
  - pseudonymous task agents
- secure environments
  - agent PKI and digital signatures
  - confidential communication (encryption)
  - anonymous networking with onion routing
- actions according to EU Privacy Directive
  - 3 types of personal identifiable information
  - 10 privacy principles
  - transfer law to technology by ontology

PISA Demonstrator



Privacy Interface Analysis

Analysis Development Sequence

EU Privacy Directive

↓

Privacy Principles

↓

HCI Requirements

↓

Requirement Categories

Analysis Application Sequence

UML Use Case Modeling

↓

UML Sequence Modeling

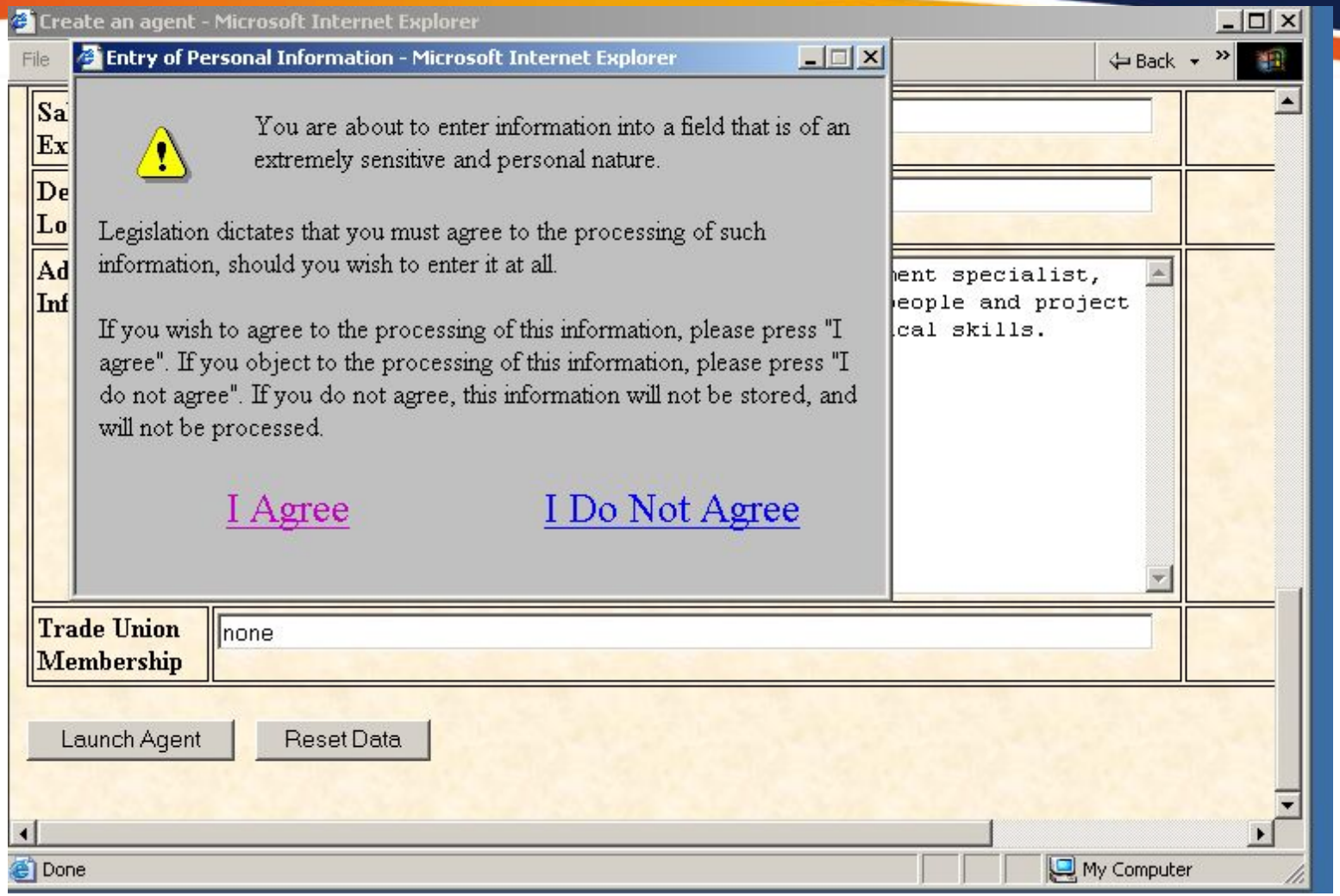
↓

Generic HCI Solutions

↓

Specific HCI Solutions

Just-in-Time Click-Through Agreements



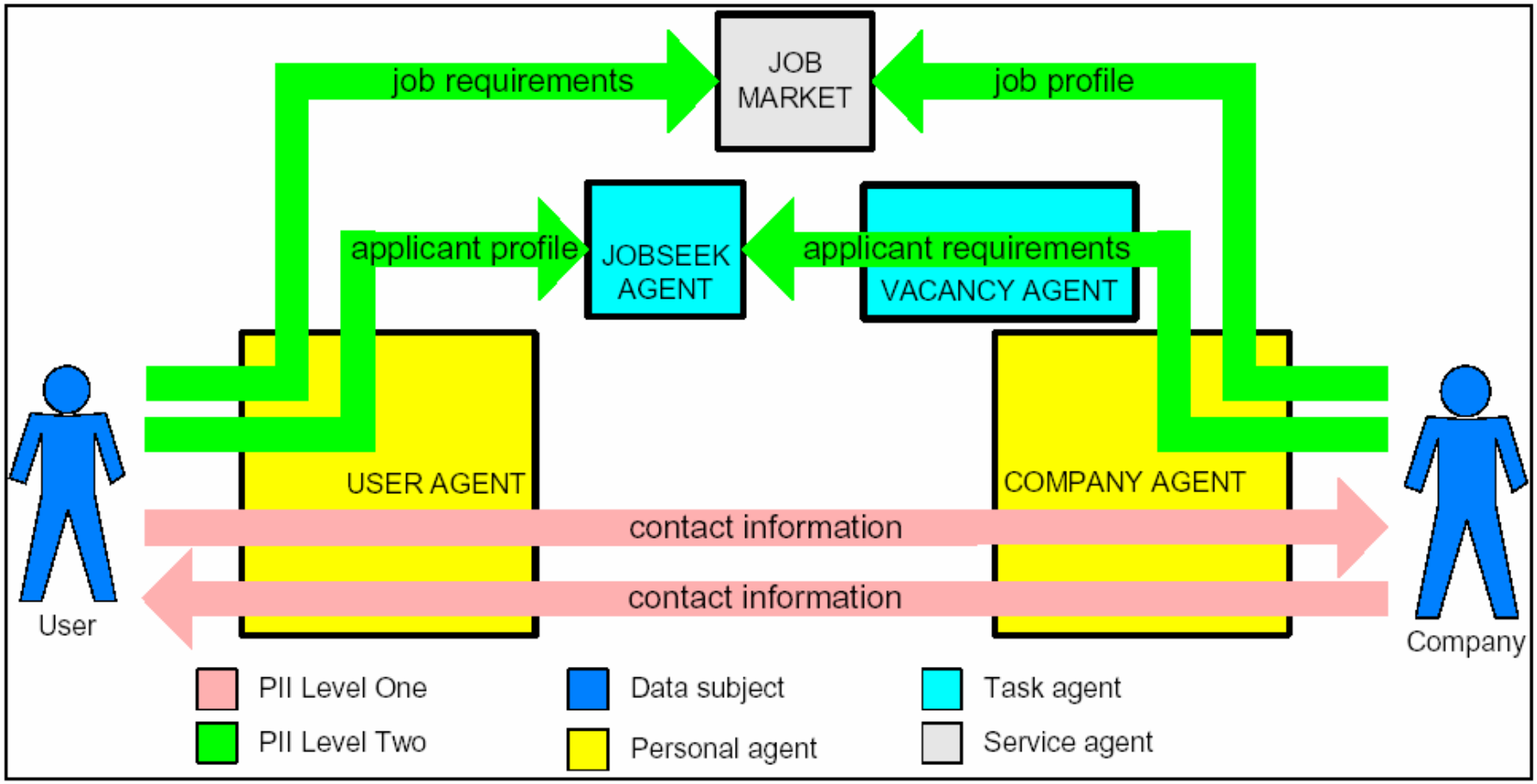
3 Types of Personal Information

- **Type I: contact info (name, address, etc.)**

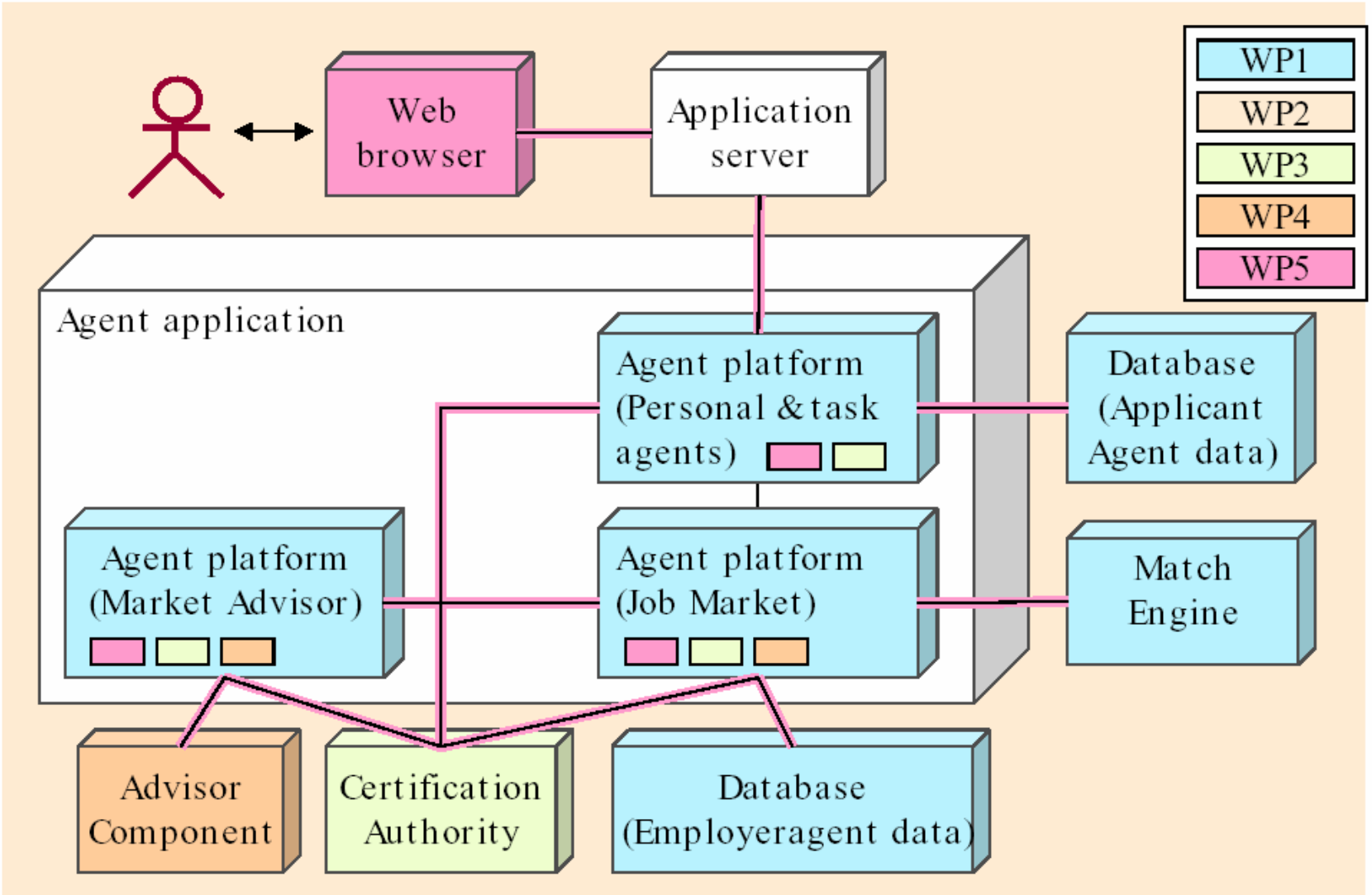
- **Type III: special categories defined in law**
  - **racial or ethnic origin**
  - **political opinions**
  - **religious or philosophical beliefs**
  - **trade union membership**
  - **health**
  - **sex life**

- **Type II: everything else**

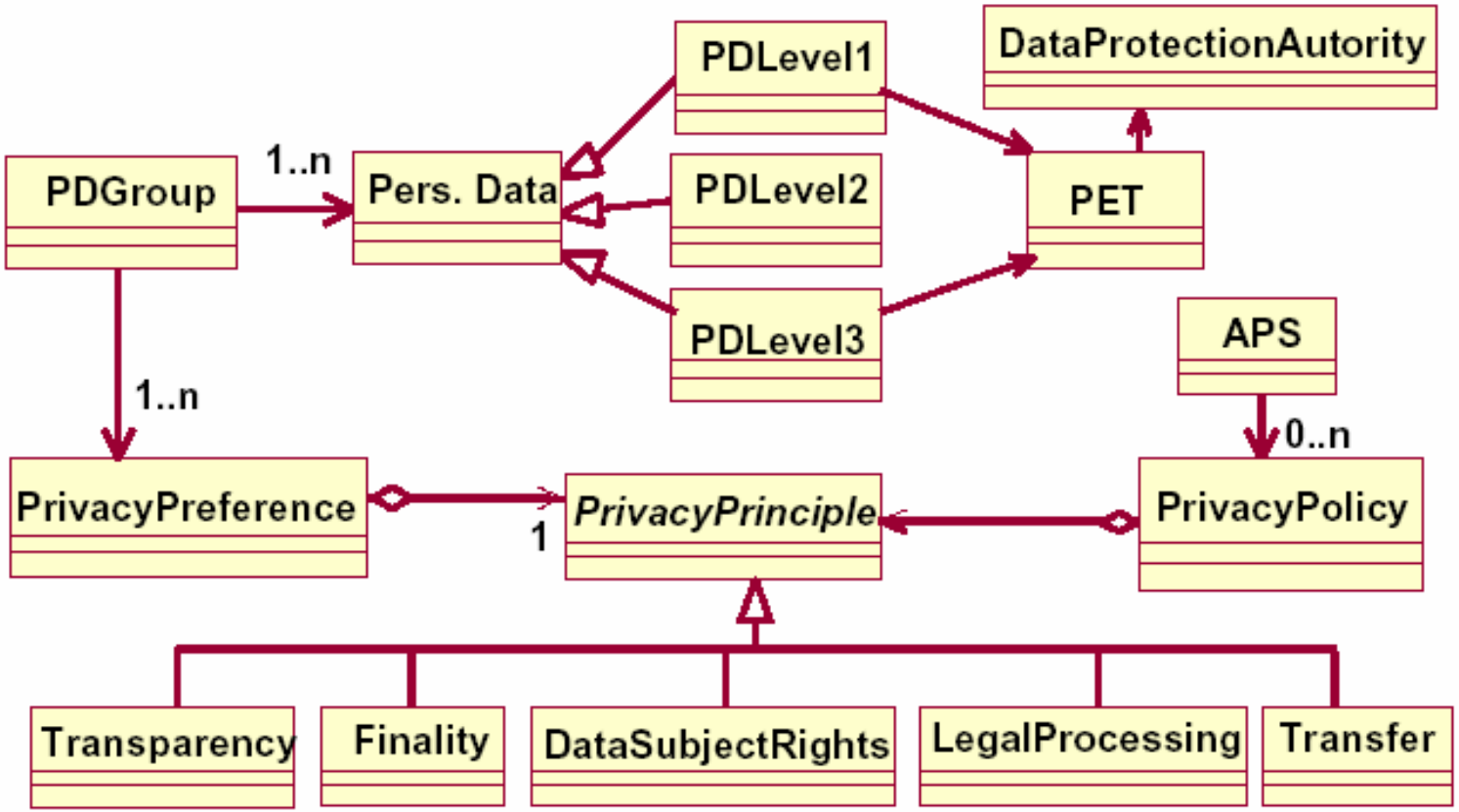
PISA Agents & Data Flows



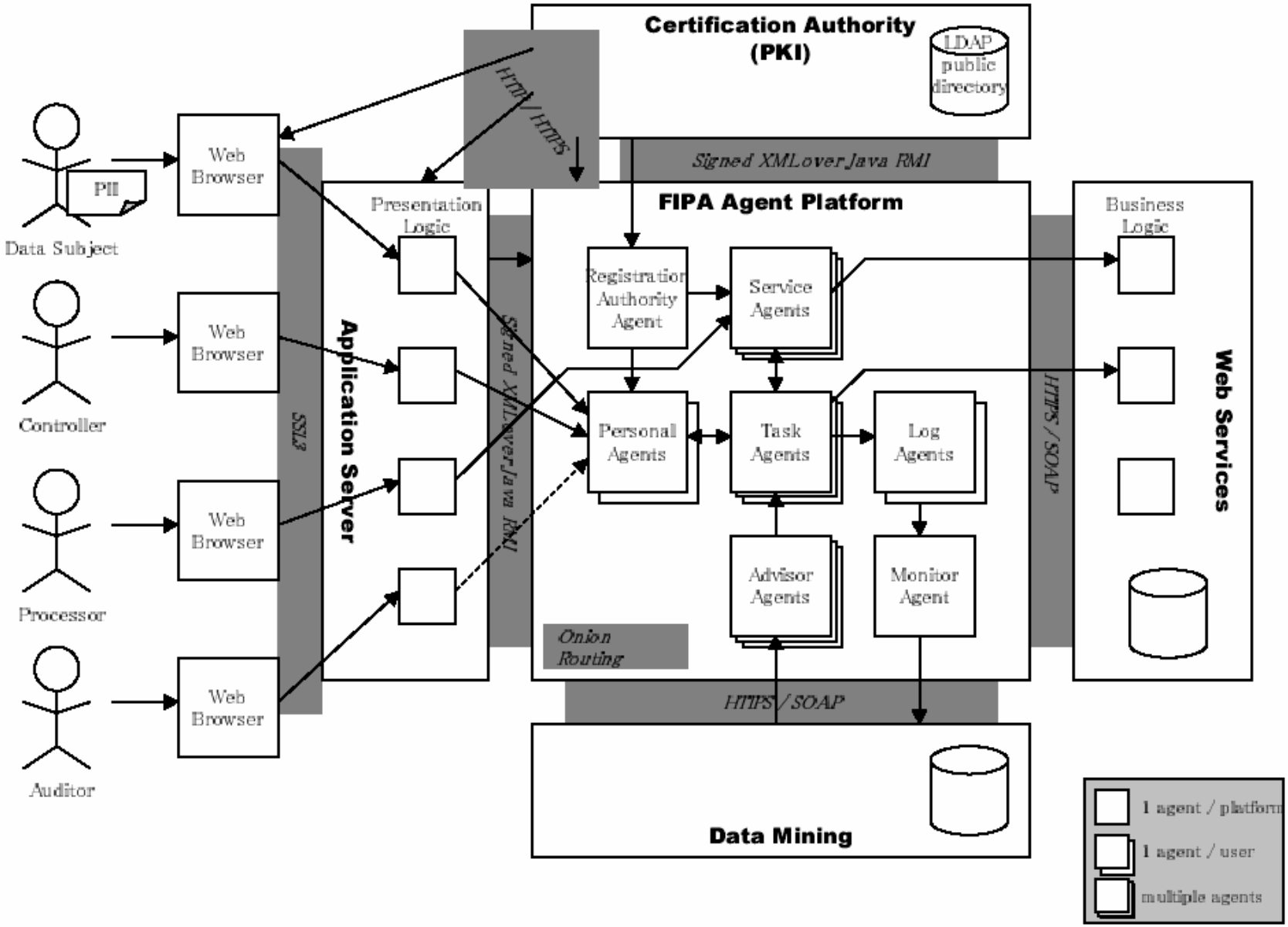
PISA System Components



Privacy Ontology Concepts



PISA Architecture



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

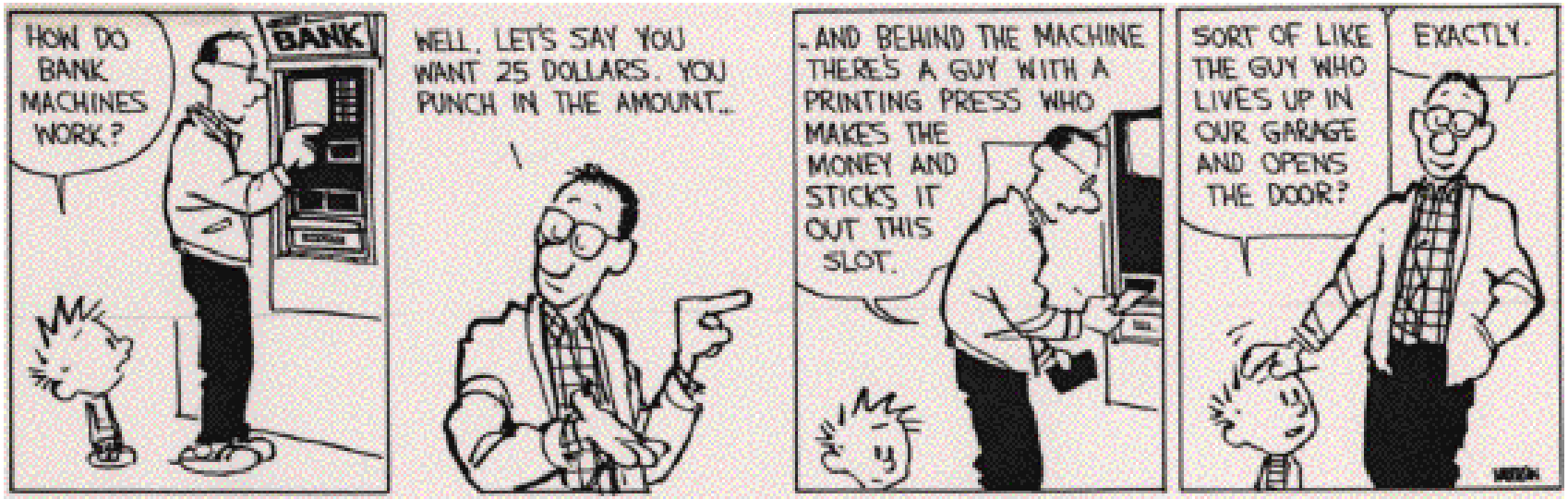
Detailed Analysis Examples

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

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"