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
European Commission 5th Framework Project
• international R&D consortium
• www.pet-pisa.nl
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.
• 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

- 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
## Ten Privacy Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting the processing</td>
<td>All non-exempt processing must be reported in advance to the National Data Protection Authority.</td>
</tr>
<tr>
<td>Transparent processing</td>
<td>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.</td>
</tr>
<tr>
<td>Finality &amp; Purpose Limitation</td>
<td>Personal data may only be collected for specific, explicit, legitimate purposes and not further processed in a way that is incompatible with those purposes.</td>
</tr>
<tr>
<td>Lawful basis for data processing</td>
<td>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.</td>
</tr>
<tr>
<td>Data quality</td>
<td>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.</td>
</tr>
<tr>
<td>Rights</td>
<td>The Data Subject has the right to acknowledge and to improve their data as well as the right to raise certain objections.</td>
</tr>
<tr>
<td>Data traffic outside EU</td>
<td>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.</td>
</tr>
<tr>
<td>Processor processing</td>
<td>If data processing is outsourced from Controller to Processor, controllability must be arranged.</td>
</tr>
<tr>
<td>Security</td>
<td>Protection against loss and unlawful processing</td>
</tr>
<tr>
<td>Number</td>
<td>Basic Principle</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>1</td>
<td>Transparency: Transparency is where a Data Subject (DS) is empowered to comprehend the nature of processing applied to her personal data.</td>
</tr>
<tr>
<td>1.1</td>
<td>Data Subject (DS) inform: DS is aware of transparency opportunities</td>
</tr>
<tr>
<td>1.1.1</td>
<td>For: Personally Identifiable Information (PII) collected from DS. Prior to DS PII capture: DS informed of: controller Identity (ID) / Purpose Specification (PS)</td>
</tr>
</tbody>
</table>
| 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 secure | 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

Consciousness

Comprehension

Control

Consent
<table>
<thead>
<tr>
<th>Requirements</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• comprehend how PII is handled</td>
<td>• training</td>
</tr>
<tr>
<td>• know who is processing PII and for what purposes</td>
<td>• documentation</td>
</tr>
<tr>
<td>• understand the limits of processing</td>
<td>• user agreements</td>
</tr>
<tr>
<td>• understand the limitations on objecting to processing</td>
<td>• help</td>
</tr>
<tr>
<td>• be truly informed when giving consent to processing</td>
<td>• tutorials</td>
</tr>
<tr>
<td>• comprehend when a contract is being formed and its implications</td>
<td>• mental models</td>
</tr>
<tr>
<td>• understand data protection rights and limitations</td>
<td>• metaphors</td>
</tr>
<tr>
<td></td>
<td>• layout</td>
</tr>
<tr>
<td></td>
<td>• feedback</td>
</tr>
</tbody>
</table>
Mental Models

How do bank machines work?

Well, let's say you want 25 dollars. You punch in the amount...

And behind the machine there's a guy with a printing press who makes the money and sticks it out this slot.

Sort of like the guy who lives up in our garage and opens the door?

Exactly.
<table>
<thead>
<tr>
<th>Requirements</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• be aware of transparency options</td>
<td>• messages</td>
</tr>
<tr>
<td>• be informed when PII is processed</td>
<td>• pop-up windows</td>
</tr>
<tr>
<td>• be aware of what happens to PII when retention periods expire</td>
<td>• assistants</td>
</tr>
<tr>
<td>• be conscious of rights to examine and modify PII</td>
<td>• layout</td>
</tr>
<tr>
<td>• be aware when information may be collected automatically</td>
<td>• highlight by appearance</td>
</tr>
<tr>
<td></td>
<td>• alarms</td>
</tr>
</tbody>
</table>
### 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

Control
When Control is Hard
## Consent

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• give <strong>informed consent</strong> to the processing of PII</td>
<td>• user agreement</td>
</tr>
<tr>
<td>• give <strong>explicit consent</strong> for a Controller to perform the services</td>
<td>• click-through agreement</td>
</tr>
<tr>
<td>being contracted for</td>
<td>• “Just-In-Time Click-Through Agreements”</td>
</tr>
<tr>
<td>• give <strong>specific, unambiguous consent</strong> to the processing of sensitive data</td>
<td></td>
</tr>
<tr>
<td>• give <strong>special consent</strong> when information will not be editable</td>
<td></td>
</tr>
<tr>
<td>• <strong>consent</strong> to the automatic collection and processing of information</td>
<td></td>
</tr>
</tbody>
</table>
Just-in-Time Click-Through Agreements

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, legislation requires you to 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
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
• 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.