Protecting Privacy in Software Agents: Lessons from the PISA Project

Andrew S. Patrick
National Research Council of Canada
Andrew.Patrick@nrc-cnrc.gc.ca
http://www.andrewpatrick.ca

The Privacy Incorporated Software Agents (PISA; www.pet-pisa.nl) project was a European Fifth Framework project whose goal was to develop and demonstrate Privacy-Enhancing Technologies (PET) that will protect the privacy of individuals when they use services that are implemented through intelligent software agents. An integral part of the project was to examine the human-computer interaction (HCI) implications and develop interface specifications. The goal of these HCI activities was to build an agent-based service that people will trust with sensitive, personal information and one that will operate according to privacy-protection requirements coming from legislation and best practices.

To meet these goals, three different research activities have been conducted. The first was to carefully examine the concept of "trust" and review what is known about building trustworthy systems. It was found that intelligent, autonomous agents have the potential to facilitate complex, distributed tasks and protect users' privacy. However, building agents users will trust with personal and sensitive information is a difficult design challenge. Agent designers must pay attention to human factors issues that are known to facilitate feelings of trust. These include providing transparency of function, details of operation, feedback, and predictability. They must also consider factors that lead to feelings of risk taking. This means reducing uncertainty, collecting the minimal amount of information, and carefully considering the amount of autonomy an agent will have.

The second research activity was to examine the privacy legislation and principles to determine the human-factors implications and consequences. The goal of this work was to document a process that begins with privacy legislation, works through derived privacy principles, examines the HCI requirements, and ends with specific interface design solutions. This research involved a phrase-by-phrase analysis of the European Privacy Directive (95/46/EC) to determine the human behaviour requirements that were implied by the legal constructs. Interface design techniques were then outlined for each of the requirements, and specific design solutions were developed for the PISA Demonstrator. The result was a set of recommendations for implementing "usable compliance" with privacy legislation and principles.

The third research activity was to conduct a preliminary usability test of portions of a PISA interface design prototype. The purpose of the testing was to determine if the design concepts in the prototype were successful in constructing an agent technology that (1) users can use, (2) users can understand, and (3) users can trust with secure and private information. Fifty people were asked to interact with the software system on a computer and answer questions about the features and performance that they experienced. After completing the usability test, participants were given a 16-item questionnaire to assess the overall usability of the prototype. In addition, this questionnaire enquired about their attitudes towards the trustability of the Internet in general, Internet services, and the PISA prototype that they had just tested.

The research results indicated that users could use the major features of the interface, such as creating a job-searching agent. However, some of the specific features, such as controlling specific privacy preference parameters, were in need of more attention. Concerning understanding, the results clearly indicated that users had difficulty understanding the privacy preference terms used in the interface, and this was the most important characteristic to improve. Finally, users found the service to be trustable, although it is clear that, with the problems in understanding the interface, the maximum possible trust was not created.