

# Intelligent software agents and privacy

## 6 Conclusions and recommendations

This chapter contains the conclusions and recommendations that emerged from this study.

**Conclusion:** ‘Intelligent’ agents are the near future. They are being studied and developed in quite a number of research & development laboratories. Nevertheless, the agents that are available today still require a lot of user-initiated actions to produce the right results.

**Recommendation:** In spite of the fact that agents are not yet as sophisticated as researchers claim, the implications of the use of (intelligent) agents for the privacy of individuals already need to be taken into account. This is necessary to control both today’s consequences and consequences that may arise in the (near) future.

**Conclusion:** Future intelligent agents might have advanced computing powers, which enable them to take over human tasks, and to interact with people in human-like ways. ‘Some agents have the potential to form their own goals and intentions, to initiate actions on their own without explicit instruction or guidance, and to offer suggestions to people’ (Norman, D.A., 1994). This could lead to certain privacy threats.

**Conclusion:** To ensure a smooth introduction of agent technologies two aspects are relevant. The first aspect deals with the way people feel about agents. The second aspect deals with the comfort and acceptance of the agent’s automatic, autonomous actions (Norman, D.A., 1994).

**Recommendation:** Developers of agents need to make sure that people do not lose control over their computational systems and information contained therein. Adding control and feedback mechanisms and safeguards to prevent runaway computation will help agent-users to increase trust in using agent technologies.

**Conclusion:** Privacy and confidentiality of actions will be amongst the major issues confronting the use of intelligent agents in the future, when the society will be fully automated and interconnected.

**Conclusion:** The exchange of personal data is only necessary in some cases, for example for the authorisation or accounting of the individuals who want to access a system, environment or service. In all other cases, the exchange of personal data is not necessary.

**Conclusion:** Unprotected agents will jeopardise the privacy of individuals. Agents can exchange personal data of their owners with others, but it is also possible that agents collect personal data of individuals in the interest of their owners. This could lead to the following potential threats to privacy:

- loss of control;
- agent-providers;
- the exchange of personal data with the environment:
  - agents that are in disguise;
  - agents that are more powerful;

- traffic flow analysis performed by agents;
- the collection of personal data of individuals, by:
  - entering the privacy domain of the individual;
  - entering databases that contain information about the individual;
  - entering the user-profile of an individual's agent.

**Conclusion:** Measures have to be taken to reduce the impact of the privacy threats. These measures are:

- certification of the agent's working method;
- logging of all internal and external actions of the agent itself;
- identification and authentication of all agents;
- access control mechanisms;
- logging of all actions performed by other agents that collect personal data;
- mechanisms to audit the logged activities;
- integrity mechanisms to control the integrity of stored or exchanged data and to control the integrity of working methods of agents or trusted components, like digital signatures;
- the Identity Protector: implemented with existing Privacy-Enhancing Technologies (PETs) such as: digital pseudonyms, blind digital signatures, and Trusted Third Parties (TTP's).

**Recommendation:** These measures can be wrapped around the agent or they can be integrated in the agent. A combination of integrating and wrapping is also possible. The measures can also be used to build an infrastructure of trusted components.

**Conclusion:** The consequence of using identification, authentication and access control mechanisms is that all agents that want to co-operate in the environment need to have a unique identity. To obtain a unique identity the agents all need to be registered.

**Conclusion:** When a high degree of protection is required the measures that are implemented in the agent need to be enforced, and must therefore be impossible to bypass. Enforcing the measures will have an impact on some of the agent's properties and attributes, like mobility and cloning. The agent will not be allowed to be mobile and to clone itself. This will lead to reduced performance of the agent.

**Recommendation:** Due to the fact that the research is in the early stages, the results of this research may change, because of new developments or new views on the use of agents. The results need to be discussed with developers of agents, agent-technologies and privacy-enhancing technologies.

**Recommendation:** By using a checklist of design criteria during the design process, the user, designer, developer, supplier, or provider of an agent have a tool to help them develop an agent or an agent-environment with proper privacy-enhancing technologies.

**Recommendation:** Privacy Commissioners and Data Protection Authorities should ask designers and developers of agents if they used the design criteria during the development of their agents.