ARE LAW-ABIDING AGENTS REALISTIC?

Frances Brazier[1], Onno Kubbe[1], Anja Oskamp[2] and Niek Wijngaards[1]

[1] Intelligent Interactive Distributed Systems, Faculty of Sciences
Vrije Universiteit Amsterdam, de Boelelaan 1081a, 1081 HV, Amsterdam, The Netherlands
Email: {frances,kubbe,niek}@cs.vu.nl
Phone: +31 - 20 - 444 7737, 7756, 7756; Fax: +31 - 20 - 444 7653

[2] Computer and Law Institute, Faculty of Law
Vrije Universiteit Amsterdam, de Boelelaan 1105, 1081 HV, Amsterdam, The Netherlands
Email: a.oskamp@rechten.vu.nl
Phone: +31 - 20 - 444 6215; Fax: +31 - 20 - 444 6230

Abstract. Software agents are an inherent extension to the current Internet. They are, however, without a legal status. They autonomously roam the Internet, perform transactions, and gather information. The legal implications of their actions are, however, not well understood. This paper presents some of the issues involved, viewed from the perspective of Artificial Intelligence, Computer Systems and Law.

1. Introduction

Internet technology is changing society. The physical distribution of services, processes, and data, is no longer necessarily the same as the perceived location. The Internet society is not restricted to geographical, legal, or corporate boundaries. Agent technology is a key enabling technology in this society; software agents are autonomous and pro-active, can autonomously (Castelfranchi, 2001) roam the Internet, perform transactions, and gather information.

Wide-area distributed (agent) systems are no longer fiction, they are a fact. Existing forums such as W3C and FIPA propose standardisation to pave the way for the development of such applications. A growing concern is, however, the legal status of agents and the (legal) implications of their use. Developers of agent-based applications require an understanding of the legal status of agents and the implications of their use. Unfortunately, little is known about the legal issues involved. Research is required for determining implications for the development of agents and the support for agents (Sartor and Branting, 1998; Oskamp and Brazier, 2001; Weitzenboeck, 2001). Agent developers need to know how to design an agent that abides to specific laws (corresponding with the intended use of the agent). In addition, developers of agent operating systems (which support running or active agents) need to know which legal issues play a role.

Section 2 briefly sketches related research areas and advocates the need, and set-up, for an interdisciplinary research. Section 3 presents legal issues related to the design and support for (law-abiding) agents. Section 4 concludes this paper with a brief discussion.

2. Relevant research

A number of research areas are related to researching legal aspects of agents. First, and foremost, is legal research applied to computer systems. Second, scientific research in Computer Systems (CS) and Artificial Intelligence (AI) on agents and their support. And thirdly, arguments for an interdisciplinary approach are given.

From the AI perspective agents are (1) autonomous and pro-active, (2) may be mobile, (3) are capable of communication with other agents, (4) are capable of interaction with the outside "world," and (5) are most often intelligent (meaning that they may be capable of learning, have knowledge, can perform complex tasks, and can reason about and with this knowledge). In this respect, a well-known example of an agent is a human being. An agent (either human or automated) has its own

environment, consisting of other agents and a (material) world. The agent metaphor offers a means to model situations with distributive activity on a conceptual level (e.g., Jennings, 2000).

From a Computer Systems perspective an agent is often considered to be just a process (Tanenbaum and Steen, 2002), a (possibly multi-threaded) piece of running code with data and state. Research in both disciplines (i.e. AI and CS) is concerned with support for agents (by means of agent platforms or agent operating systems, security architectures, etc.) and the use of agents (reasoning, argumentation, negotiation, profile-building, learning, adaptation.

Research on legal aspects of agents requires more expertise than is currently available within AI, CS and/or Law. These research areas form the basic blocks, from which a new multi-disciplinary research area can be constructed.

Interdisciplinary research requires recognition of cultural and language problems: some concepts have quite different interpretations in different disciplines. One approach to overcome these ambiguities is to engage in discussions and develop a shared framework, with explicit mappings to frameworks used in individual disciplines (Apistola, Brazier, Kubbe, Oskamp, Schellekens and Voulon, 2002). The interdisciplinary research on legal aspects of agents is to the benefit of all participants: Law obtains understanding in technological advances and (im)possibilities, AI and CS obtain understanding in legal requirements on agents and agent operating systems.

3. Legal Issues

During the design and development of agents and their supportive agent operating system, a number of legal issues play a role. For agents, legal issues can be identified, such as:

- transaction capabilities: when has an agent performed a transaction? Is an agent allowed to perform all legal transactions?
- identity: does an agent have one identity, or several? Can the identity of an agent change? Can an agent be anonymous? What are the legal implications?
- privacy: can an agent have private data, and protect this data? Can an agent be allowed to carry personal data or combine personal data? How does this comply with Acts on Personal Data protection?
- audit trails: can an agent be audited?
- liability: who is liable if an agent makes a (deliberate) mistake? The agent, the owner of the agent (can he or she always be identified?), the last location of the agent, … ?

For agent operating systems, and especially in the case of large-scale systems, legal issues can be identified, such as:

- resource guarantees: can agents depend on their allocated resources?
- authentication: how to provide a distributed, scalable, authentication mechanism not including one single trusted third party?
- audit trails: can locations in an agent operating system be audited?
- security: what levels of security are legally required (while not conflicting with, e.g., an agent's privacy).
- fault tolerance and reliability: can an agent operating system give any guarantee concerning fault tolerance and reliability?
- warranty and liability: what happens to a location in an agent operating system when something goes wrong. Who is liable?

For human society, legal issues can be identified such as

- software agents vs. human agents: is it important in transactions to know that an agent is a software agent, and not a human agent? And how can we tell the difference in a digital world?
- liability: who is liable for mistakes made by software agents?

During the design of the AgentScape framework, including an agent operating system and services, a number of more specific questions with respect to legal issues have arisen. Section 3.1 describes the

legal issues with respect to the agent operating systems. Section 3.2 describes the legal issues with respect to two services of the AgentScape framework: an agent factory and generative migration.

3.1 Agent Operating System

Large-scale distributed systems are often heterogeneous systems: heterogeneous with respect to the host architecture (Sun SPARC, Intel x86/i64), the supported operating system (Solaris, Linux, Windows NT), and the communication infrastructure (bandwidth and latency). The major technological challenge is to build scalable, secure, and fault tolerant systems, that supports multiple distributed applications, heterogeneity, and multiple qualities of services.

The AgentScape framework (Wijngaards, Overeinder, Steen and Brazier, 2002) is a world-wide scalable distributed agent platform. The framework aims to include: (i) the AgentScape operating system (AOS), (ii) services, and (iii) support for application developers. Prototype implementations of the AOS, a number of services, and a programming environment (i.e. MANSION by Noordende, Brazier and Tanenbaum, 2002) show that this concept is feasible.

AgentScape specifically deals with large-scale distributed systems on which, mobile, *autonomous* processes run. The mobile, autonomous processes are called *agents*, the passive, possibly distributed, entities are called *objects*. An important characteristic of agents, which distinguishes them from traditional processes, is autonomy: agents are in control of their own behaviour.

Management of AgentScape sites (i.e. *locations* within AgentScape) is a distributed problem. Each location management system (human or automated) manages a dynamic artefact (the configuration or allocation of resources available to agents, objects and services) on the basis of frequently changing requirements. The human administrator (c.q. the organisation (s)he represents) of the location is the most important stakeholder. Other stakeholders include other locations and the locally hosted agents and their owners. Information and commands from (remote) locations and unknown (owners of) agents may be suspicious: the source and authenticity of the information and commands need to be verified, as well as the usefulness and reliability. Knowledge about trust in other entities (such as locations and agents) needs to be made explicit, to adequately manage a location.

Legal issues arising from the management perspective include:

- can a management system "kill" an agent (without or with notification to the (anonymous?) owner of the agent)?
- can a management system refuse resources to an agent (e.g. thereby impeding or preventing its successful functioning)?
- can a management system relocate agents without their consent to other locations?
- is a management system responsible for the uniqueness of identity of agents?
- is a management system responsible for aiding in an audit? And how does a remote auditing authority know how to trust the audit information in a specific location? Is it feasible to maintain audit logs in an open system: the volume of audit logs may be enormous.
- scalability: when thousands of agents communicate, migrate, and interact with objects and services, how can any controlling mechanism be reliable, efficient, and real-time? What are the legal implications when they are not, and things go wrong.

3.2 Services

Legal implications of two services of AgentScape are discussed in this section: an agent factory and generative migration (which uses an agent factory).

The *Agent Factory* (Brazier and Wijngaards, 2001a; 2002) automatically (re-)designs agents, which in this context are designed to be re-designed. Everything inside an agent may be replaced, deleted or modified, including its internal process structure, knowledge structure, data, ontologies, etc. To this end, a compositional structure is assumed, and re-usable agent components are identified in advance. The design of an agent within the agent factory is based on specifications of building block configurations: blueprints. Building blocks include cases and partial (agent) designs (cf. generic models / design patterns), knowledge bases, and instantiated models. Building blocks are either components with open slots, fully specified components, or a combination of both.

Legal issues arising from the use of an agent factory concern, e.g.,

- physical identity: is the identity of an agent linked to its 'body'? The agent factory may adapt the body of an agent (on the agent's request), even to the extent of changing its code-base from Java to C++. Does this change the (legal) identity of the agent?
- (im)mutability of the body of the agent: if an agent factory can change the body of an agent, how does an agent know it has been changed in the right way? without adding 'spy code', or 'viruses', or severely damaging the agent, cutting out awareness of the agent that it wanted to be *different*?
- privacy: an agent factory can probe into an agent's innermost thoughts and thought processes. Is this allowed? If so, under what circumstances? Does it for instance make a difference whether an agent contains Privacy Enhancing Technologies? What if an agent factory abuses its power? How can an agent notice any abuse?
- security: it is difficult for agents to transport cryptographic keys, as they can be easily distilled by an agent factory (or an agent operating system). Key cloaking is not simple, and may not be 100% proof. To which extent do these issues need to be solved?

Agents, and in particular mobile agents, offer a means for application developers to build distributed applications. In current agent systems, mobility of agents is constrained by the environment of the agents: the agent platform (which supports agents) and the agent's code base (e.g., DESIRE or Java). *Generative migration* is needed to adapt an agent to conform to its destination agent platform and code base (Brazier, Overeinder, Steen and Wijngaards, 2002) by employing agent factories. Generative migration is described as a process of "transparently adapting" an agent so that the agent can continue to function at its new location on a completely different agent platform. In a sense an agent has multiple 'incarnations'. Generative migration has a number of advantages, including an interesting security advantage: an agent can be re-incarnated at, e.g., a bank, by an agent factory using only trusted building blocks containing trusted code.

Legal issues arising from the use of generative migration concern, e.g.,

- identity of an agent: when an agent switches from one incarnation to another, is it legally still the same agent?
- privacy: how can an agent be protected from tampering? How can a system/platform guarantee that, e.g. in the example of the bank, that the bank's agent factory does not pass on sensitive information (e.g., concerning when to stop bidding for specific equities) to other parties?
- liability: what happens if an agent's current incarnation is faulty? Who is responsible (can this be determined)?

4. Discussion

Agent technology is progressing at a fairly steady pace. Current research does not often include reflections on legal aspects and implications on the use of agents. This may affect their usability. Legal researchers need to exert influence on (directions of) agent research, and now is the time to act. Numerous complex legal issues need to be resolved before agent technology can be safely, and legally, applied. A multi-disciplinary approach is advocated, as each of the research areas of Law, Computer Systems and Artificial Intelligence cannot research these legal issues on their own.

The ALIAS project (see Appendix) is a multi-disciplinary project in this sense, specifically aimed at exploring the legal status of agents and the implications of their use. It is clear that the issues involved are broad and manifold and that much more collaborative research is needed! All input is valued.

Acknowledgements

This research is supported by NLnet Foundation, `http://www.nlnet.nl/`. The authors wish to acknowledge the contributions made by the participants of the ALIAS project: Corien Prins, Erik Schreuders, Maurice Schellekens, Marten Voulon and Martin Apistola; `http://www.iids.org/alias/`.

References

Apistola, M., Brazier, F.M.T., Kubbe, O. Oskamp, A., Schellekens, M.H.M. and Voulon, M.B.: 2001, Legal aspects of agent technology, *in Proceedings of 17th Bileta conference*, Amsterdam, March 2002 , pp. 11, http://www.bileta.ac.uk/.

Brazier, F.M.T., Overeinder, B.J., Steen, M. van and Wijngaards, N.J.E.: 2002, Generative Migration of Agents, *in* E. Alonso, D. Kudenko and D. Kazakov (eds), *Proceedings of the AISB'02 Symposium on Adaptive Agents and Multi-Agent Systems*, pp. 116-119.

Brazier, F.M.T. and Wijngaards, N.J.E.: 2001, Automated Servicing of Agents, *AISB Journal*, **1**(1): 5-20, Special Issue on Agent Technology.

Castelfranchi, C: 2001, Again on Agents? Autonomy: A Homage to Alan Turing, *in* C. Castelfranchi and Y. Lespérance (eds), *Intelligent Agents VII*, Lecture Notes in Artificial Intelligence, **1986**, Springer-Verlag, Berlin Heidelberg, pp. 339-342..

Jennings, N. R.: 2000, On agent-based software engineering, *Artificial Intelligence*, **117**(2): 277–296.

Noordende, G. van 't, Brazier, F.M.T. and Tanenbaum, A.S.: 2002, A Security Framework for a Mobile Agent System, *in Proceedings of the SEMAS at AAMAS2002*, to appear.

Oskamp, A. and Brazier, F.M.T.: 2001, Intelligent agents for lawyers, *in Proceedings of the Workshop Legal Knowledge Systems in Action: Practical AI in Today's Law Offices*, pp. 5.

Sartor, G. and Branting, L.K.: 1998, Introduction: Judicial Applications of Artificial Intelligence, *Artificial Intelligence and Law*, **6**(2-4): 105-110.

Tanenbaum, A.S. and Steen, M. van: 2002, *Distributed Systems: Principles and Paradigms*, Prentice Hall, Upper Saddle River, New Jersey 07458.

Weitzenboeck, E. M.: 2001, Electronic Agents and the Formation of Contracts, *International Journal of Law and Information Technology*, **9**(3): 204 - 234.

Wijngaards, N.J.E., Overeinder, B.J., Steen, M. van and Brazier, F.M.T.: 2002, Supporting Internet-Scale Multi-Agent Systems, *Data and Knowledge Engineering*, **41**(2-3): 229-245.

Appendix

The ALIAS project (`http://www.iids.org/alias`) is an explorative study into the legal and technical implications of the use of software agents. This research is partly motivated by the assumption that social acceptability of agent technology will increase if the legal context is more clearly identified. Also the realisation that interdisciplinary research can be of help in drawing a more realistic picture of the possible applications of agent technology is a motivation of this research.

In this project the research areas of Computer Science, Artificial Intelligence, and Law are combined to analyse legal possibilities and limitations of agent technology and so be able to try and find technical solutions to meet legal requirements. The aim of this project is to provide guidelines for both AI-researchers and Legal-researchers.

For discussion purposes the ALIAS group has a web-discussion forum available. The Web-discussion site (`http://soapbox.cs.vu.nl/ALIAS/`) brings issues that are of interest both to technicians and lawyers.