ARE ANONYMOUS AGENTS REALISTIC?

Frances Brazier[1], Anja Oskamp[2], Corien Prins[3], Maurice Schellekens[3] 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, niek}@cs.vu.nl
Phone: +31 - 20 - 444 7737, 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

[3] Center for Law, Public Administration and Informatization, Faculty of Law
Tilburg University , P.O. Box 90153, 5000 LE, Tilburg, The Netherlands
Email: {J.E.J.Prins, M.H.M.Schellekens}@uvt.nl
Phone: +31 - 13 - 466 - 8044; Fax: +31 - 13 - 466 8149

Abstract. Software agents are involved in Internet applications such as E-commerce and may contain identificatory information about their human user such as credit cards and bank accounts. This paper discusses whether human users and software agents are allowed to be anonymous and whether anonymity is technically realisable from the perspective of Artificial Intelligence, Computer Systems and Law.

1. Introduction

In daily life, many situations occur in which humans may be anonymous. For example, a human buyer may wish to be temporarily anonymous during an auction by employing a middleman, as to not influence the price. At some (later) moment in time he may need to reveal his identity to complete the transaction. With the advent of the Internet, it becomes possible for software agents to electronically make transactions, e.g. at electronic auctions. Similar to the previous example, there may be situations in which agents may wish to remain anonymous, for example when searching the Internet for medical information. One way to accomplish this is to use middle agents (Wong and Sycara, 2002), but other options exist.

In general , there is not much known about the legal status of agents and their actions (e.g., Brazier, Kubbe, Oskamp and Wijngaards, 2002). There is even less knowledge about anonymous agents specifically: are agents, for example, allowed to be anonymous, and is this feasible? These issues are closely related to legal and technical identities of human counterparts of agents: owners, users, deployers, organisation, designer, producers, etc. In the near future legal and technical decisions with respect to these issues will greatly influence the use of software agent applications and -support. If agents have no legal status they will never be used in practice.

In theory, anonymity holds for both agents and humans. Human anonymity can be arranged by an agent keeping identificatory information about humans confidential. In specific situations it may be desirable to have agents be 'anonymous', i.e. not be (easily) traceable in their actions, nor (easily) relateable to a human owner or user. To this end, an agent may strategically employ a number of identities: pseudonyms. This implies that various levels of anonymity exist, ranging from brief temporal anonymity to absolute

anonymity; although the latter cannot be guaranteed (no techniques are known to the authors).

This paper provides a view on identity and anonymity by discussing legal issues in Section 2 and a technical perspective in Section 3, and concludes with a discussion in Section 4. Legal issues are dealt with according to Dutch law and – where appropriate – EU legislation.

2. Legal Issues for Identity and Anonymity

2.1 Legal obligations to reveal ones identity

Legal obligations to identify oneself in online environments are relatively scarce. The Dutch Identification Duty Act imposes a passive identification obligation in certain situations, such as fare dodging or visiting a soccer match. The Act requires identification by means of one of the prescribed means of identification, such as a passport. For the time being, the prescribed means of identification do not lend themselves for on line use. The Act is thus only of theoretical value for on line situations.

With respect to the use of software agents, the obligations to identify oneself formulated in the directive on electronic commerce and the distance-selling directive are especially relevant. The user of a software agent acting as a provider of services of the information society, as a person making commercial communications, or supplying goods at a distance (as defined in the latter directive) has to make his identity actively known. The user of a software agent must adhere to the following obligation with respect to self-identification:

- The active identification obligation of art. 5 Directive 2001/31/EC imposes requires of the service provider that identification information is permanently available; a website is an adequate means to make the information 'permanently' known. A single message to a software agent's human counterpart is not conform the permanency requirement.
- The active identification obligation of art. 6 Directive 2001/31/EC requires of the sender of commercial communication, also known as spam that identification information is clearly indicated or referred to in the (spam)message; this requirement does not seem to be problematic with respect to agents, even if the (spam)message is delivered to a software agent's human counterpart.
- Dutch National legislation requires certain contracts to be in writing. On line, this form requirement may be met by using an electronic functional equivalent to traditional writing (art. 9 Directive 2001/31/EC). According to the Dutch Implementation Bill, the electronic equivalent of writing must be such that the identity of the contracting parties is determinable to a sufficient degree. This means that a software agent used to close contracts must be able to reliably pass on the identity of its user (i.e. one of the contracting parties), so that this can be 'incorporated' in the contract. This may mean that the agent must be able to use the electronic signature of its user.
- Identification on the basis of Directive 97/7/EC (on distance selling): the supplier must make identification data available to the consumer in writing or in another durable medium available and accessible to the consumer. This means that delivery to a consumer's mobile agent is not enough. After all, an agent may – if it is mobile – not be accessible at all times by its user. Furthermore, it seems difficult to guarantee storage on a durable medium.

2.2 Anonymity

Sometimes a person wants to hide his identity or participate under a pseudonym in social life. The bidders at an auction may, e.g., want to hide their identity in order to avoid a negative influence on the price-formation. A person may thereto make use of a software agent that hides his 'true' identity.

Seeking anonymity

Legally, the status of anonymity is rather subtle. On the one hand, a right to anonymity does not exist. On the other hand, a person is not prohibited to try and find anonymity with the help of organisational, technical or contractual means. The use of a software agent hiding the identity of its user while acting on the Internet is therefore allowed.

This also holds for contracting. The key principle of the Dutch contract law is that contracts can, in principle, be entered into without prescribed form: 'unless stipulated to the contrary, declarations, including notifications, can be given in any form and can be incorporated in behaviour', reads Article 3:37, paragraph 1, of the Dutch Civil Code. Unless opposed by imperative law, the parties are free to incorporate in the contract the obligation that their mutual identity is specified based on the principle is that the parties themselves determine the method used to declare their intent. This could, therefore, be an absolutely anonymous one. This makes absolutely anonymous electronic legal transactions possible. Thus, it also allows for the use of agents that do not reveal the identity of its user.

Anonymity is, however, limited in that a person cannot deny identification duties that rest upon him. The mere existence of an identification duty does, however, does not imply a lack of anonymity. The anonymity is only lifted by observance to the identification duty. Someone wishing to protect his anonymity may, therefore, want to evade situations in which such a duty must be fulfilled.

Attempting to identify an anonymous person

As noted above, a person may seek anonymity using the means he sees fit. The reverse however may also hold: other people may, in principle, try to find out the identity of someone who is anonymous. Someone trying to unveil the identity of an anonymous person must observe the law in doing so: he may e.g. not infringe upon the privacy of the anonymous person, he is not allowed to hack into computers or wiretap tele-communications. From these examples it appears that a number of legal rules exist that can be helpful in protecting ones anonymity, although 'anonymity' is not the prime object (rechtsgoed) that is protected by the rules. One could say that those rules provide 'flanking' protection to anonymity. Any acts aimed at finding out a person's identity that are not unlawful, may thus be used. One may e.g. ask a third person to disclose the identity of an anonymous person. In general, the third person is of course under no duty to disclose the identity.

2.3 A Software Agent protecting anonymity

With respect to software agents the most pressing problem with respect to anonymity may very well be the following. A software agent contains information that identifies or could help to identify its user, which information it needs to fulfil its task. Nonetheless, the agent is programmed to maintain the anonymity of its user. If the agent is also mobile, it may often reside on computer systems 'far from home'. These systems may not be sympathetic to the idea of maintaining a user's privacy. The question thus is the following: are the data in a software agent legally protected against inspection by the

owner of the system on which the agent finds itself? If so, under what conditions? In this respect, the Dutch Computer Crime II Bill is relevant [Tweede Kamer 1998/99, 26671, nrs. 1-2]. In this Bill the following provision (art. 273d Dutch Criminal Code) can be found:

> With imprisonment of at most one and a half year or a fine of the fourth category (i.e. Euro 11250,-) will be punished a person employed by a provider of a public telecommunications network or –service:
>
> a. who wilfully and without right inspects data that have been stored or are processed or transmitted with the help of such network or service and that are not destined for him, or who wilfully and without right copies, taps or records such data for himself or another.
>
> b. […]

If and when this provision is enacted, data inside a software agent are protected against unwanted inspection. Two of the conditions that must be met, are discussed in this section: what does 'without right' mean? What is a provider of a public telecommunications network or –service?

Without right: according to the explanatory memorandum this addresses the situation that a provider of telecommunication without authorization of the person concerned inspects personal data of his customers that are stored in the provider's computers (e.g. e-mail in an e-mailbox) [Tweede Kamer 1998/99, 26671, nr. 3, p. 47]. So the protection only seems to extend to 'personal data'. The example mentioned (e-mail) further seems to highlight that the personal data must be recognisable as such. In case of a mailbox this is clear: a mailbox is recognisable as such and everybody expects to find personal data in a mailbox. That a software agent contains personal data is however not self-evident. So if an agent contains personal – especially identification – information it is relevant that the information is recognisable as such and cannot be inspected 'by accident'. So, in order to qualify for legal protection under this provision, it is necessary to store these data in encrypted form. However, it is unlikely that the encryption needs to be especially elaborate. Probably, it suffices to use a rather simple form of encryption.

The second condition to keep in mind is that the provision is only applicable to providers of public telecommunication networks or –services. Telecommunication is not restricted to just traditional telecommunications operators (e.g. KPN, BT etc.) but all telecommunications providers are covered by the term: thus also e.g. Internet Access Providers. However, the networks or services they provide must be public, meaning it must be available to the public. In closed networks, the provision is not applicable. It is then up to the parties to agree on the confidentiality of the data in agents, if they desire to do so.

3. Technical Issues for Identity and Anonymity

The subjects of identity and anonymity play a double role for agents: agents themselves usually have an identity, and an agent may carry confidential information which can be used to identify one or more humans. Examples of confidential information include personal information and identification information such as banking information, credit cards, money, information about its organisation, information about its owner, logins and passwords, and information about its user. Legal duties may require to safeguard *any* confidential information from unwanted disclosure and traceability, including information which may identify humans. The identity of agents is commonly used for communication

purposes and is usually made public in location services (cf. yellow pages).

Agent platforms host agents, i.e. they offer environments in which agents run, supporting services such as communication and mobility. A number of agent platforms currently exists, including FIPA-OS (FIPA, 2001), OAA (Martin, Cheyer and Moran, 1999), Jade (Bellifemine, Poggi and Rimassa, 2001), ZEUS (Nwana, Ndumu, Lyndon and Collis, 1999), and AgentScape (Wijngaards, Overeinder, Steen and Brazier, 2002).

Confidential information in an agent is only to be disclosed to other agents and agent platforms in specific situations and under given conditions. Other agents may, however, fool an agent into revealing confidential information. Agent platforms may also have the ability to fully inspect an agent. Confidential information thus needs to be protected from untrusted agent platforms and other agents.

Protecting confidential information not only depends on techniques but also on protocols and standards. Techniques imply technical measures to protect agents from ill willing subjects. Protocols have to do with general agreements and standards on how to use the agents and information contained therein. Using protocols does not imply that protection on a technical level (e.g. see the legal requirements about encryption in an open system) is not needed. Below is a brief description of common techniques for information protection (Anderson, 2001; Tanenbaum and Steen, 2002):

- Cryptography is based on the principle that information can be encrypted with a key which results in unintelligible information, which in turn can be restored to its original form when it is decrypted with the same key (symmetric cryptosystem).
- Public key infrastructures are based on the principle that a unique pair of encryption and decryption keys is employed (asymmetric cryptosystem). The effect is that information encrypted with the public key, can only be decrypted via the private key, and *vice versa*. Commonly, a certification authority is used to assert that a specific public key is owned by a specific entity.
- Digital signatures are based on the principle that on the basis of information, a unique number can be computed by an irreversible mathematical function (a hash-function) and is usually signed by the owner of the information. Commonly, digital signatures are employed to verify the integrity of the information: the receiver can also compute the unique number, and compare this with the received number in the decrypted signature (e.g. using PKI).
- Split keys are based on the principle that an agent is given part of a private key, while the other part remains, e.g., with the user. To use the private key, the agent needs to obtain the other part of the private key, e.g. from its user or a trusted third party.
- Cloaking and watermarking are based on the principle of steganography, i.e. hiding information in cover-information: an agent may hide its private keys in, e.g., its code.
- Certificates are based on the principle that a trusted third party can provide digitally signed information, e.g. for permissions and electronic money (Sherif, 2000).

An important issue related to these techniques concerns distributing keys: how to know which key belongs to which entity? Approaches are being developed involving both trusted public systems (centralised) or webs of trust (decentralised), e.g. to verify an agent's identity.

Confidential information and agent identities play a role in the following situations:

- *Mobility*: software agents may migrate to locations, some of which may be malicious or non reliable for other reasons. Confidential information in mobile agents has always a risk of being disclosed unless encrypted.
- *Cloning*: software agents may be cloned, i.e. a copy is made which is completely the

same as the original (including confidential information). It is debatable whether a clone has the same identity as the original; in some definitions of cloning the clone is always the same as the original, to the extent that one can give information to the clone and obtain it from the original: they're indistinguishable (note that some agent platforms may not support multiple agents with the same identity). In other cases, when the clone of an agent "runs its own life", a different identity is assigned. This issue requires more research.

- *Aggregation*: software agents which are grouped together may also have a collective identity. Examples include all agents of one user or agents that currently work on a shared problem. A collective identity may be used for communication purposes, but also for acting. In the latter case, usually a specific agent assumes the collective identity and is able to act. This issue requires more research.

Protecting confidential information also depends on protocols, which may specify when confidential information is revealed, to whom, how it is to be used, and what is to be logged. However, an agent implicitly trusts the agent platform it runs on: a computer has complete control over all agents it hosts, but not necessarily all information contained in agents. Although tracing techniques may be used to detect whether an agent platform disobeys protocols, damages may still occur. This also applies to other agents, whether they act according to protocol, and whether tracing can be useful for detection and prevention. Traceability or logging of actions is commonly part of both agent protocols and technical protocols. Traceability involves logging information about agent actions, a process which leads to large amounts of tracing data, possibly distributed among multiple agent platforms in different legal domains. Determining the granularity of the actions logged, the reliability of tracing data, and storing and processing such tracing data may not be easily accomplished and requires more research.

Agent platforms use access control policies to decide which agents to host. Such access control policies may favour agents which have an identity of their own (i.e., can be traced), and e.g. whether the identity of their human designer, human owner, and/or human user is known or traceable (e.g. via trusted-third parties). This may conflict with the needs of some human users, who may wish to remain anonymous at all times.

Based on the current technological situation, options are to

- place minimal confidential information in a software agent.
- use appropriate techniques to hide confidential information.
- use appropriate protocols when interacting with other agents and agent platforms.
- place appropriate protective strategies in a software agent.
- reflect on the consequences when confidential information becomes (semi-)public.
- use appropriate access control policies in agent platforms.

Research is needed to determine what 'appropriate' entails: to this end protocols and techniques need to be analysed and tested to verify their robustness and reliability in terms of computational expense, temporality, and legality.

Possible approaches to avoid using a software agent with confidential information:

- send agents without any confidential information to report back with information upon which the user can take action, e.g. an agent searches for a book in a bookstore, while the human user buys the book.
- use (e.g.) electronic cash which gives legitimacy to a specific action to be undertaken by an agent and which does not require information about a human, e.g. an agent searches for, and buys, a digital book and brings it to the human user.

4. Discussion

Software agents on the Internet are part of an open, changing, system in which anonymity of humans and agents may sometimes be useful. This paper discusses whether anonymous agents are realistic from a legal and technical point of view. In theory only human beings may perform transactions. To perform transactions for a human counterpart, an agent may need to carry identification information. A distinction can be made between legal and technical identity. Whether the legal identity of a human and an agent can or even should be the same needs to be further researched. The technical identities will differ; the human's identity may or may not be carried by an agent. The agent's identity is commonly used to trace the agent's actions and for inter-agent communication.

If the information carried by an agent is confidential it needs to be protected in an open system. A number of techniques for protecting confidential information have been introduced. Anonymity hinges on the principle that information is kept confidential: if at some moment in time an entity discloses the human user of an agent this can be combined with traces of the agent and disclose privacy sensitive information. In addition, anonymity is usually used temporarily, often with a good reason, e.g., when concluding negotiations to finalise a transaction after anonymously gathering information. The consequence of disclosing an identity depends not only on current conversation partners, but also indirectly on the availability of tracing data. Note also that results in mathematics and computer science will most likely make it possible to decrypt currently encrypted information in the future.

Although a number of techniques for protection of confidential information exist, more research is needed about the applicability (when is it most useful), robustness and reliability (when will it fail), and temporality (when will it be deciphered)?

Issues for further research:

- analysis of legal and technical identities of humans and agents
- traceability: analysis of large amounts of tracing data from distributed sources, e.g. in co-operation with analysis of DNS tracing data (http://www.nlnetlabs.nl/dns-analyzer),
- develop realistic, secure environments for agents, including experiments to assess reliability, security, scalability, and feasibility.
- develop identity management models.

Acknowledgements

The ALIAS project is supported by NLnet Foundation, `http://www.nlnet.nl/`. The ALIAS project is a multi-disciplinary project specifically aimed at exploring the legal status of agents and the implications of their use. The authors wish to acknowledge the contributions made by the participants of the ALIAS project: Martin Apistola, Onno Kubbe, Erik Schreuders and Marten Voulon; `http://www.iids.org/alias/`.

References

Anderson, R. (2001), *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, New York.

Bellifemine, F., Poggi, A. and Rimassa, G. (2001), Developing Multi-Agent Systems with a FIPA-Compliant Agent Framework, *Software: Practice and Experience*, **31**(2), pp. 103-128.

Brazier, F.M.T., Kubbe, O., Oskamp, A., and Wijngaards, N.J.E. (2002), Are Law-Abiding Agents Realistic? Sartor, G. and Cevenini, C. (Eds.), *Proceedings of the workshop on the Law of Electronic Agents (LEA02)*, pp. 151-155.

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.

FIPA, (2001). *FIPA agent platform*, http://www.fipa.org.

He, M. and Leung, H-F. (2002), Agents in E-Commerce: State of the Art, *Knowledge and Information Systems*, **4**, pp. 257-282.

Martin, D., Cheyer, A., and Moran, D. (1999), The open agent architecture: A framework for building distributed software systems. *Applied Artificial Intelligence*, **13**(1-2), pp. 91-128.

Nwana, H., Ndumu, D., Lyndon, L., and Collis, J. (1999), ZEUS: A toolkit and approach for building distributed multi-agent systems, *Proceedings of the Third International Conference on Autonomous Agents (Autonomous Agents'99)*, pp. 360-361.

Tanenbaum, A.S. and Steen, M. van (2002), *Distributed Systems: Principles and Paradigms*, Prentice Hall, New Jersey.

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), pp. 229-245.

Wong, H. and Sycara, K. (2000), A Taxonomy of Middle-agents for the Internet, *proc. of the Fourth International Conference on Multi-Agent Systems (ICMAS'2000).*