ANONYMITY AND SOFTWARE AGENTS: AN INTERDISCIPLINARY CHALLENGE[1]

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: {FMT.Brazier, NJE.Wijngaards}@few.vu.nl
Phone: +31 - 20 - 444 7737, 7634; 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] TILT, Tilburg Institute for Law, Technology and Society, 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 8199; Fax: +31 - 13 - 466 8149

Abstract. Software agents that play a role in E-commerce and E-government applications involving the Internet often contain information about the identity of their human user such as credit cards and bank accounts. This paper discusses whether this is necessary: whether human users and software agents are allowed to be anonymous under the relevant legal regimes and whether an adequate interaction and balance between law and anonymity can be realised from both the perspective of Computer Systems and the perspective of Law.

1. Introduction

Practitioners in the field of AI and Law study how information and communication technology can be used to support legal activities. Models and theories have been devised and tested for diverse applications (e.g. Voermans, 1995). In this paper a relatively new technology is studied: agent technology. Software agents' adaptability, mobility, intelligence and interactivity make them a versatile technological instrument. This paper focuses on the role software agents can play in acquiring anonymity (of a human user) on the Internet.

Anonymity plays a vital role in many activities of a legal nature. In preparing legal advice it is essential that a legal practitioner can search anonymously on the Internet for legal information. This may be information about statutory law or case law, but also e.g., information about the policies of a governmental body. The legal practitioner wants to be able to gather this information without compromising his or her case by having the legal body know in which information has (or has not) been reviewed in preparation of a particular case. Anonymity is also relevant for the ordinary citizen. He or she may, e.g., want to express his or her views on governmental plans, policies and other issues of public interest, without exposing his or her identity. Or he or she may want to report a criminal offence to the authorities. In the Netherlands several hotlines for anonymously reporting exist. The 'Nationaal Platform Criminaliteitsbeheersing' followed the 'Meld

[1] This paper is an extended and fully revised version of (Brazier, Kubbe, Oskamp and Wijngaards, 2002) and (Brazier, Oskamp, Prins, Schellekens and Wijngaards, 2003).

Misdaad Anoniem' initiative; from being a pilot, it has now become a structural facility (http://www.meldmisdaad.nl/). The Business Software Alliance has had a telephone number for reporting software copyright infringements for years. It is also possible to report software piracy online (http://global.bsa.org/netherlands/report/report.php). Software agents may possibly provide the means to guarantee the anonymity of the person reporting the offence by electronic means.

This paper investigates the legal and technical considerations that play a role when designing an anonymity preserving software agent. In analysing the legal requirements, first the legal framework in which anonymity preserving software agents have to function is discussed. In doing so we demonstrate that it is too simple to ask what 'the' legal requirements are for 'the' anonymity preserving agent. Technology is not a datum to which the law is applied. Instead there is a complicated interaction between technology and law in which technology also influences the law. This point is illustrated by showing that designing an anonymous software agent involves many multi-faceted design decisions. Choices made during the design process may dramatically influence which legal issues arise. This paper has been written from the perspective of Dutch Law to illustrate the interaction between law and technology. The paper is structured as follows. Section 2 addresses technical issues for identity and anonymity while section 3 addresses legal issues for identity and anonymity. Technical and legal issues pertaining to the design of law-abiding anonymous agents, are addressed in section 4. This paper ends with a discussion in Section 5.

2. Technical Issues for Identity and Anonymity

This section defines the concepts of identity and anonymity and clarifies the role of software agents in relation to these concepts. Techniques for establishing (relative or absolute) anonymity are discussed and a number of applications for preserving anonymity are presented.

2.1 Identity & Anonymity

The meaning of the term identity can be set off against 'anonymity'. Anonymity is characterised by the fact that other parties do not know the other's identity. Froomkin (Froomkin, 1995; 1996) distinguishes four types of anonymity and pseudoanonymity in electronic communication: communication in which the sender's physical (or 'real') identity is at least partly hidden:

1. Traceable anonymity: the recipient does not have any clue as to the identity of the sender. This information is in the hands of a single intermediary;
2. Untraceable anonymity: the sender of an electronic message is not identifiable at all;
3. Untraceable pseudonymity: the pseudonym used be the sender of an electronic message is not identifiable. This is similar to untraceable anonymity, however, the sender uses a pseudonym. A pseudonym differs from an anonymous denotation in that pseudonyms can be used to build up an image and a reputation just like any other online personality. Therefore, pseudonyms are used consistently over a certain period of time, while an anonymous denotation might be used only once, for a single message;
4. Traceable pseudonymity: the pseudonym of the sender can be traced back to the sender although not necessarily by the recipient. Within the category of traceable pseudonyms, a distinction can be made between pseudonyms that have been assigned 'formally' to somebody by a 'third party' or pseudonyms that have been chosen by the holder of the pseudonym himself or herself.

Apart from these four types of communication where the sender's identity is hidden in some way, there is the situation in which the sender uses his/her 'real' identity: there is no anonymity or pseudonymity.

2.2 Anonymity & Agents

The subjects of identity and anonymity play a double role for agents: agents themselves have an identity, and an agent may act on behalf of one or more humans. In the second role an agent may carry confidential information which can be used to identify one or more humans. Also the behaviour of a software agent can shed light on the identity of a human, e.g., if an agent is seen to often visit one specific IP-address, this may give away the human on whose behalf the agent is performing a task. 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, including the identity of the user or owner. Legal duties may require safeguarding of *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 through directory 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 exist, 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).

In the rule these platforms assure that 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 be able to fully inspect an agent's code and data. Confidential information thus needs to be protected from untrusted agent platforms and other agents.

2.3 Technical measures

Protecting confidential information not only depends on techniques but also on protocols and standards. Techniques make it possible for a software agent to protect itself and its data content against ill willing subjects. Below is a brief description of common techniques and protocols 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 (i.e., encrypted) by the owner of the information. Commonly, digital signatures are employed to verify the integrity of the information (Brazier, Oskamp, Prins, Schellekens and Wijngaards, 2004): 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.

A software agent is clearly dependent upon its environment: on other software agents and the agent platform on which it runs, but also on services both from trusted and untrusted third parties (e.g. certificate authorities or directory services).

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. It must be remarked that cloning is a recent technology that still has to come fruition.
- *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. Just like cloning, aggregation is not yet a fully developed and ripened technology.

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 needs to implicitly trust the agent platform on which it runs: a computer has complete control over the 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, often 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 is not easily accomplished.

Agent platforms use access control policies to decide which agents to host. Such access control policies may favour agents which identify themselves and their human designer, human owner, and/or human user. This may conflict with the needs of human

users, who may wish to remain anonymous at all times.

Based on the current technological situation, options are to

- place only 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,
- implement appropriate protective strategies in a software agent,
- reflect on the consequences of confidential information becoming (semi-)public,
- use appropriate access control policies provided by agent platforms.

Further research is needed to determine what 'appropriate' entails and how it can be obtained. 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.

It should be noted that encryption and other techniques only provide temporary confidentiality: in the (near) future, new technologies may make it possible to decrypt previously confidential information. Although adjusting the 'key length' may provide some protection against new technologies, advances in mathematics and quantum computing may invalidate techniques and protocols entirely.

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.

2.4 Anonymity facilitation

The above shows that anonymisation is technically complex. Most users of anonymisation technology do not build their anonymisation software themselves. They rely on third parties who supply them with the software and in certain cases on third parties who provide services. These third parties can then be said to facilitate anonymisation. Current services facilitating anonymity and pseudonymity that have been designed for human users are services for anonymous email and surfing. Below, a number of these services are listed:

- anon.penet.fi was a centralised double blind remailing service until ca. 1996, when it was legally forced to disclose identities of users, after which it was shut down (Martin, 1998).
- www.anonymizer.com offers centralised anonymous surfing, but may disclose information about users during their surfing session or afterwards on the basis of logs (Martin, 1998).
- rewebber.com (formerly JANUS), also offer centralised anonymous surfing, but is designed for anonymous publishing (Martin, 1998; Rieke and Demuth, 2001).
- www.onion-router.net; onion routing is a decentralised approach (based on mixing, used by, e.g., MixMaster), in which a message is transmitted over a number of intermediate nodes, each of which have their own PKI-pairs. The 'onions' are the layered encrypted messages; the 'onion routers' are the forwarding nodes. The last node is able to unpack the message, and send it to its destination. Onion routing obfuscates message content, message origin and destination, and its implementation impedes traffic analysis (Martin, 1998; Goldschlag, Reed and Syverson, 1999).

- Crowds is an alternative to onion routing, more akin to a peer-to-peer approach, in which each participant is a node (Martin, 1998; Reiter and Rubin, 1998;1999). Messages are not wrapped in encrypted layers, but encrypted once.
- lpwa.com, the Lucent personal web assistant (a.k.a. ProxyMate), offered pseudonym services, via which users can easily obtain user names, passwords, and email addresses to be used to access websites which require user registration (Gabber, Gibbons, Matias and Mayer, 1997). Lucent has sold this technology to NaviPath.
- www.zeroknowledge.com: Zero Knowledge Systems is an example of a company offering software to enhance privacy (i.e., provide forms of anonymity and pseudonymity).

For humans, two of the most commonly used anonymity services are Internet cafés and throwaway web-based email addresses.

3. Legal Issues for Identity and Anonymity

3.1 Legal obligations to reveal ones identity

Legal obligations to identify oneself in online environments are relatively scarce. In the real world this obligation differs from country to country. The Dutch Identification Duty Act imposes a passive identification obligation in certain situations, such as fare dodging or visiting a soccer match. In June 2004, an Act received royal assent that widened the existing identification duties. According to this Act, every person over the age of fourteen is obliged to show his or her 'means of identification' at first request to a police officer in any situation (Wet van 24 juni 2004 tot wijziging en aanvulling van de Wet op de identificatieplicht, het Wetboek van Strafrecht, de Algemene wet bestuursrecht, de Politiewet 1993 en enige andere wetten in verband met de invoering van een identificatieplicht van burgers ten opzichte van ambtenaren van politie aangesteld voor de uitvoering van de politietaak en van toezichthouders (Wet op de uitgebreide identificatieplicht), Stb. 2004, 300). 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 online use. The Act is thus only of theoretical value for online 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 (1) a provider of services of the information society, (2) as a person involved in commercial communication, or (3) as a person supplying goods at a distance (as defined in the latter directive), has to make his or her identity actively known. The user of a software agent must adhere to the following obligations with respect to self-identification:

- The active identification obligation of art. 5 Directive 2000/31/EC requires of the service provider that identification information is easily, directly and permanently accessible; a website is an adequate means to make the information 'permanently' known. A single e-mail message to a software agent's human counterpart may not meet this requirement: it may not be available directly and if it is not stored it may be too transitory in nature.
- The active identification obligation of art. 6 Directive 2000/31/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. Online, this form requirement may be met by using an electronic equivalent to a traditional writing (art. 9 Directive 2000/31/EC). According to the Dutch Implementation Act, the electronic equivalent of a 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.

3.2 Anonymity

Sometimes a person wants to hide his or her identity or participate under a pseudonym in social life (Grijpink and Prins, 2001). A legal practitioner may want to collect data without other parties knowing what kind of information he or she is actually seeking. A person may thereto make use of a software agent that hides his or her 'true' identity.

Seeking anonymity

Legally, the status of anonymity is rather subtle (See Nicoll and Prins 2003). 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 basically 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 (Grijpink and Prins 2003, p. 256). The principle that the parties themselves determine the method used to declare their intent implies that they can declare their intent also in an absolutely anonymous way. 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 of course not imply a lack of anonymity. The anonymity is only lifted by observance to the identification duty. Someone wishing to protect his or her anonymity may, therefore, want to evade situations in which such a duty must be fulfilled.

Identifying an anonymous person

As noted above, a person may seek anonymity using the means he or she sees fit. The reverse, however, may also hold: other people may 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 or she may, e.g., not infringe upon the privacy of the anonymous person, he or she is not allowed to hack into computers or wiretap telecommunications. From these examples it appears that a number of legal rules

exist that can be helpful in protecting one's anonymity, although 'anonymity' is not the prime object 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. In special circumstances an obligation to identify may exist. In this respect the recent discussion about the conditions under which an ISP must make the identity of a subscriber known can be mentioned (See: A. Sims, 2003, A. Ekker 2003 and W.A.M. Steenbruggen 2002). In literature, it has been advocated that the interests favouring divulgement of the identity and the rights and interests that oppose divulgement must be determined. Subsequently the proportionality and the subsidiarity of the divulgement must be judged (W.A.M. Steenbruggen 2002).

Facilitating Anonymity

Is it illegal to provide anonymity software or anonymizing services? As a general rule, a person supplying means, facilities or services to another is basically not liable for the use another makes of the means, facilities or services. Outside the field of identity and anonymity, there are a few clear exceptions to this rule; provision of means to circumvent technical measures to protect copyrighted software has, e.g., been criminalised (See art. 32a Dutch Copyright Act and art. 7.1.c Software Directive). With respect to the facilitation of anonymity such a clear exception does not exist. In principle it is thus not illegal to help someone to remain anonymous. But there is a general limitation. The freedom to supply means etc. that are susceptible to misuse is not unconstrained. If the supplier of the products or services knows that the receiver of the products or services will use them for criminal activities he or she may not supply them. If he or she does, he or she runs the risk of being termed the accomplice to the offence the receiver commits. So a software engineer who knows that the receiver of his anonymizing software plans to use it for, e.g., fraudulous purposes must not supply it. In criminal law there is 'knowledge' even if the supplier merely accepts the not as imaginary discardable chance that the receiver will use the software for criminal purposes. Such acceptance will only be present if the supplier has concrete indications that such is to happen. The mere provision of software that – theoretically - could be misused does not make him an accessory or accomplice.

Third party access to identifying data

Those who facilitate anonymity often have data on their systems that could help third parties – such as the police - identify those who seek anonymity. This triggers a whole new set of issues that have legal implications. The nature of the function of the server entails that the systems containing personal information must be secured against unauthorised access. Without such security it will probably be impossible to convince prospective users to use the technology. Apart from this, there is also a legal duty to take reasonable measures to protect the confidentiality of the information if the software agents contain personal data and the manager of a system can be qualified as a 'controller' or 'processor' of these data as defined in Directive 95/46/EC.

Perhaps more interesting than the unauthorised access is the question of authorised access and issues related to that. What rights do the police have to access data that are transported, stored or processed in the system? What are the obligations of the manager of the system that correspond to the police's rights?

Certain obligations rest on providers of public telecommunication networks and

services. Telecommunication services are broadly defined as all services that consist completely or partly in the transmission or routing of signals across a telecommunications network. The services of an anonymizing server are covered by this definition. It may only be that the manager does not provide a public service (which is rather tautologically defined as a service that is available to the public) . This could be the case if the service were to be offered in a closed network. But in other cases, it seems that our manager has to comply with the Telecommunications Act. So, what obligations has the Telecommunications Act in store for our manager?

- According to art. 13.1 Dutch Telecommunications Act a provider of a public telecommunications network or service must make it possible to wiretap their network or service. This means that the technical arrangements to wiretap must be in place.
- According to art. 13.2 Telecommunications Act a provider must cooperate with the police or the secret service if the competent authorities have authorised them to 'wiretap' or acquire traffic data.
- According to art. 13.4 Telecommunications Act a provider must supply the police or the secret service with certain administrative data concerning a user, if they need these data to apply with the competent authorities for a mandate to wiretap or acquire traffic data. In certain special cases a provider must retain data about a user for a period of three months.
- If a provider has cooperated with the police and possibly has given the police data with respect to a subscriber the provider must keep confidential his cooperation and the information he or she got through it about the subscriber. The provider may especially not inform the subscriber about the interest the police has shown.
- Apart from these obligations the Dutch Code of Criminal Procedure has some additional obligations. The most important seems to be the obligation to decipher data that are encrypted; anyone who can reasonably be assumed to 'know', the key for deciphering can be ordered to decipher (with a few exceptions for those that have a duty of non-disclosure, such as doctors etc.).

3.3 Software agents and anonymity

In the foregoing, anonymity has been described, the question whether it is legal has been addressed as has the question how anonymity by software agents can technically be achieved. An outstanding question is however why it is at all desirable that people can act anonymously. What stance do we take with respect to anonymity?

By acting anonymously an actor withholds information from others, such as (potential) contract partners, readers of posted messages, senders of newsletters etc. It is unknown to them who is acting. Bentham once coined the famous catch phrase that 'knowledge is power' (Bentham, 1791). If this principle is applied to the situation at hand this means that anonymity shifts power from others to the person acting anonymously. Assuming that anonymity gives power to the person acting anonymously, why would such a state of affairs be desirable? At this time in which threats of terrorism abound and anonymity almost immediately is suspect. It is all too easy to imagine for what detrimental purposes 'power by anonymity' could be used.

On the other hand, current technology driven developments increase transparency of persons. Whoever enters the Internet releases information about him or herself. Often more than is apparent to the average Internet user. Many of the examples are well-known. When visiting websites, cookies are left on ones hard disk for the website-software to inspect when visiting the website anew. Browsing through websites may

mean that the website owner records a click-trail. The number of websites no longer open to the public without any formality is. Registration is an access-condition that becomes ever more pervasive. Buyers at online auctions must identify themselves, even if this is to the detriment of their bargaining position. Of course, one could object that laws about informational privacy guard against over-processing of our personal data.

Each processing of personal data in Europe must comply with the standards set in directive 95/46/EC. When personal data 'pass' the European border, adequate safe-harbour guarantees must be in place. But the reality is that in view of the technical possibilities the data subject is losing out. Transparency about where ones personal data are stored and processed is lacking. The grounds for processing personal data (see art. 8 WBP) allow for the processing of personal data in a wide variety of situations, i.e. a necessary concession to the fact that personal data are often a necessity for the performance of, or at least a very welcome lubricant of, all kinds of societal processes. Why is it then that the laws of informational privacy appear so inadequate? Is that because they are set up in an inadequate way? This is not necessarily the case. Under these laws a reality has developed in which the initiative lies almost exclusively with the processors of personal data. This 'factual' situation makes that processors of personal data are in a much better position to 'play their cards' under the prevailing privacy regulations.

If one considers the situation that has developed to be undesired what then should be the answer? One could consider the modification of privacy laws. It does, however, seem that not much is to be expected from a change in legislation. It is not so much the legislation that is the problem, but the way in which the parties involved are able to materialise their goals and desires under the legislation. To bring about a change in this situation by changing the law would probably lead to legislation that ties everyone down. That cannot be the solution.

A solution should in our view be found much more in bringing back the initiative to the data subject. As long as the data subject has to hand over his or her personal data and must trust that the receiver processes his or her data with reticence the data subject will always be in the arrears. So it is only if the data subject can keep data to himself or herself that he or she returns to a situation in which he or she can retake control over his or her personal data. This is where anonymity and pseudonymity enter the equation. Anonymity and pseudonymity can no longer be considered a toy for privacy-forerunners. It is not a luxury anymore; it is almost becoming something of a necessity, a basic toll for whoever enters the Internet.

In the previous section we saw that the law leaves in principle enough room to act anonymously, although no right to anonymity exists or is likely to emerge in the foreseeable future. We also saw that software agents can easily be combined with technologies that preserve an agent owner's anonymity to various degrees.

We must however warn that the legal and technical domains are not the only ones that are to be considered when deploying anonymity preserving software agents. There is also something like market acceptance to be considered. It is e.g. no use being anonymous if you cannot do anything. If a prospective contracting partner does not want to contract with an anonymous person, anonymity preserving technology is to no avail for this purpose. Will such a hostile attitude towards anonymity become the rule? Such a negative stance need however not be taken. The attitudes towards anonymity are to some extent 'makeable'. If anonymising software agents are around and start being used a period of habituation can commence. Without anonymisation technology being available, habituation to the other alternative, i.e., identifiability, may grow.

What does the foregoing mean for anonymity preserving software agents? The development of software agents should be guided by the principles of transparency and choice.

The principle of choice means that users of software agents must have the possibility to use anonymity preserving agents if they so desire. This means that these software agents must be available on the marketplace. The law should not prescribe what anonymity preserving features software agents should have, nor how anonymity preservation is technically realised. It is up to the market to decide upon these issues. The market would ideally develop many different types of anonymity preserving software agents. It is up to a user to select specific agents that fit his or her needs and desires.

The second principle, the principle of transparency, means that developers of software agents should explain to users the anonymising capabilities of their software agents. Some technologies are more expensive to implement and use. E.g. technologies that make it more difficult to analyse the traffic of software agents may be useful, but slower and potentially cumbersome. It cannot be assumed that the technically better anonymising technology is also the technology that will be adopted by the marketplace. There is most likely not one technology that provides the answer to all needs. The user should however be able to make an informed choice.

A second aspect of transparency is the transparency after the fact. If a breach of anonymity has occurred a software agent should be able to report its user about the breach. This gives the user the possibility to take measures that limit the damage that might occur as a result of the breach, and it also enables a user to judge the capabilities of anonymisation technology. Thus a user can make a better-informed choice the next time he is to use a software agent for anonimising purposes.

In conclusion, one can say that anonymity is a means needed to restore the balance in the way personal data are dealt with on the Internet. Software agents have an important part to play in the provision of anonymity on the Internet. Nonetheless, setting up a system for anonymity preserving software agents is no sine cure. By way of example, the next section shows some of the intricacies one has to deal with when designing these software agents.

4. Law abiding anonymous agents

Although anonymity and pseudonymity raise many interesting issues, this section focuses on one hypothetical design issue. This hypothetical example illustrates the intricate ways in which technical and legal considerations interact. This section first describes the design choice and then shows its relevance for computer scientists and lawyers.

4.1 A design choice

Given the legal starting point that providing the means for anonymity is in itself not prohibited, software engineers can decide to build an anonymity preserving software agent and the necessary infrastructure. The conclusion of section 3.3. is that it is desirable that anonymity preserving software agents are developed. This section focuses on the following design decision: software engineers may at one point or another be faced with the issue of where to have anonymization take place.

As stated above anonymization is technically not just a matter of removing all information from a software agent that could give clues about the identity of the user of the software agent. An individual or an organisation trying to trace the identity of the user could also try to analyse how the software agent travels across the Internet. It is clear that traffic analysis could shed light as to who the user of the software agent is: if

the software agent often returns to the same IP-address it seems to be a safe bet to assume that this is the address of its user.

To counter the risk that traffic analysis shows who the user of the software agent is, the anonymity infrastructure could be extended to include an additional server purely for the purpose of anonymization. The function of the server is to complicate and ideally frustrate any attempt to perform traffic analysis. The server could, e.g., work in the following way: it transforms (the bits making up) an incoming software agent and its technical identity in such a way that an outside observer has a hard time relating a software agent that leaves the server to a software agent that entered it at some earlier time. This can, of course, only work if the volume of incoming and outgoing traffic is sufficiently large. For the platform that hosts the software agent in the end, it would seem as if it came from the anonymizing server; making it impossible to see where the software agent has been before. Alternatively, a simpler approach without a server could be chosen. If an anonymizing software agent changes its (software agent) identity and works from varying IP-addresses and does not 'go home' to its user too often, traceability can also be counteracted. Other alternatives without a server are the following:

- to use an agent only once; a new agent is generated for each new job (while re-using experiences from old agents), e.g. by using a big personal agent that sends out small helper agents, which are killed when they've finished their job,
- to re-use agent identities or the agents themselves,
- to make use of a 'rent-an-agent' principle: very useful agents exist, and can be rented/hired to perform a task for you. The agent can be traced, but, by using secure communications, the client cannot be (easily) traced. Furthermore, observers cannot easily distinguish the current, temporary, user. Needless to say, that the user needs to trust the company providing the agent for hire.
- to employ agents from other users / owners to do your jobs: you are not traceable, but they are.

4.2 Technical considerations

A system designer has at least two alternatives in this situation: he or she can create an infrastructure with an additional server with the prime purpose of erasing an agent's tracks, or one without. This is the design choice that is leading in the rest of this paper. There are of course many additional technical considerations that could play a role (e.g. commercial or organisational consideration), but these are not given any further attention in the context of this example. Considerations for an anonymity infrastructure without an additional server could be:

- It is less complicated and therefore easier to program, easier to make robust etc.
- The absence of the server makes for faster traffic. The necessary time that a software agent is inside the server in the other option is not needed.
- There are advantages in scalability. Since all functionality is performed in a distributed way, the software can function well with both small and large volumes. The alternative with the server seems to be rather critical on volumes: too little traffic and it is easy to relate outgoing agents to incoming ones, too much traffic and the server becomes a bottleneck.

As considerations for an anonymity infrastructure with a server, the following can be mentioned:

- The server makes it much harder (and ideally impossible) to trace a user by way of a

traffic analysis: although the agent is known to be affiliated with this server, its real user / owner remains unknown.

- Updates of the software are easier to perform; the number of servers is limited and they can function as a base to perform the updates of the software agents that pass through them.

4.3 Relevance of legal considerations

Clarity about the legal implications is a necessary precondition for making 'technical' design decisions. A short legal analysis shows that legal aspects have a bearing on the following aspects that a system designer would need to take into account when designing a system:

- The effectiveness of the software (agent): the effectiveness of protection of the anonymity using an additional server, may in part be lost the judicial rights to authorised access are frequently exercised.
- The law may require certain extra functionality to be included, e.g., to choose for the alternative with the additional server may imply the need to be able to tap the wire.

The system manager is assigned a specific role in his or her interaction with the authorities.

Legal analysis contributes to insight in the requirements imposed on a system. Legal considerations include:

- What duties rest on the actors in light of diverging design decisions? What duties to inform and to warn rest, e.g., on the providers of information technology? How can these duties be fulfilled?
- What legal infrastructure is needed in the different scenarios? If a trusted third party (TTP) is needed what clauses must be in the contract the TTP closes with third parties?
- What issues of public interest are raised when choosing one alternative or the other?

If this hypothetical design choice were to have been made in reality, what choice would have been made? Although a choice would depend upon many circumstances of the field of application, it seems that simplicity would point in the direction of a system without a server. Both technically and legally, many complications can be avoided by choosing the simpler approach. Furthermore, for many legal applications of anonimizing software agents trust plays a vital role: the existence of a server that plays a central role in the actual anonymization could have a detrimental effect on the perception of trustworthiness given the possibilities of authorised access by the police. Imagine that the police would seek access to the logfiles of such a central server for finding out who reported a certain crime. The trust of the public in the 'hotline' would collapse immediately.

On the other hand, however, legislation may be imposed which requires the use of servers. A trade-off is required between the level of anonymity needed and the desireability to remove the anonymity of perpetrators.

5. Discussion

Anonymity is of increasing importance for shielding one's personal information when going online. Section 3.3 indicated that anonymity may even become a necessary tool to preserve a human's informational privacy. Software agents can technically facilitate anonymity although there is not one self-evident way to design anonymity preserving software agents. Many alternative designs are possible.

Highlighting a number of options for a specific design choice demonstrated how technical and legal issues are closely interwoven. Developers of technology are free to choose alternatives that suit certain parties (e.g. users and providers) and make life difficult for others (e.g. the police). To increase insight in these mechanisms at an early stage, it is not only necessary that lawyers are involved in the development of technology, but also that there is discussion on how the co-operation between lawyers and technicians should take place. Difficult issues seem to be the following:

- How can legal aspects e.g. with respect to anonymity be contemplated in an early stage of technical development? Who is to determine what design choices are desirable and undesirable from a legal perspective? How 'weighty' should legal considerations be in the entirety of considerations that govern design choices?
- Are design decisions e.g. regarding anonymity made sufficiently explicit during software development? How can legally relevant aspects of design decisions be discovered and identified.
- How to structure the field once relevant design options and a multitude of legal aspects have been identified?

One way to handle the latter could be to identify a number of exemplary scenarios with interrelated design decisions for further study. Once the technical and legal merits of different aspects have been identified possibly more can be said about more general guidelines.

Acknowledgements

The ALIAS project is supported by NLnet Foundation, `http://www.nlnet.nl`. The ALIAS project is an inter-disciplinary project specifically aimed at exploring the legal status of agents and the implications of their use. The authors 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): 103--128.

Bentham, J. (1791), *Panopticon*, Dublin.

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

Brazier, F.M.T., Oskamp, A., Prins, J.E.J., Schellekens, M.H.M. and Wijngaards, N.J.E. (2003), Are anonymous agents realistic?. In Oskamp, A. and Weitzenboeck, E. (eds.), *Proceedings of the LEA 2003: The Law and Electronic Agents*, Edinburgh, NRCCL: 69--79.

Brazier, F., Oskamp, A., Prins, C., Schellekens, M., and Wijngaards, N. (2004). Law-abiding & integrity on the Internet: a case for agents, *AI&Law journal*, in this special issue.

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: 339--342.

Ekker, A. (2003), Comment about Voorzieningenrechter Rechtbank Haarlem 11 september 2003 (Pessers/Lycos) *Computerrecht* **22**: 363--367.

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

Froomkin A.M. (1995), Anonymity and Its Enmities, *Journal Online Law*, art. 4, June.

Froomkin A.M. (1996), Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, Journal of Law and Commerce*, **15**: 395--479.

Gabber, E., Gibbons, P., Matias, Y. and Mayer, A. (1997), How to Make Personalized Web Browsing Simple, Secure, and Anonymous. In R. Hirschfeld (ed.), *Financial Cryptography, Proceedings of the First International Conference, FC '97*, 17—32, Springer-Verlag.

Goldschlag, D.M., Reed, M.G. and Syverson, P.F. (1999), Onion Routing for Anonymous and Private Internet Connections, *Communications of the ACM*, **42**(2):39--41.

Grijpink, J.H.A.M. and Prins, J.E.J. (2001). New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity, *Journal of Information, Law & Technology*, **2**.

Grijpink, J.H.A.M. and Prins, J.E.J. (2003). New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. *In* Nicoll, C., Prins, J.E.J. and Dellen, M.J.M. van (Eds.), *Digital Anonymity and the Law. Tensions and Dimensions*. (Information Technology & Law Series, 2), 249—269, Den Haag: T.M.C. Asser Press.

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

Martin, D. (1998), Internet Anonymizing Techniques. In: *;login: Magazine,* May, http://www.usenix.org/publications/login/1998-5/martin.html

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): 91-128.

Nicoll, C. and Prins, J.E.J. (2003), Anonymity: challenges for politics and law. In Nicoll, C., Prins, J.E.J. and Dellen, M.J.M. van (eds.), *Digital Anonymity and the Law. Tensions and Dimensions*. (Information Technology & Law Series, 2), 287—297, Den Haag: T.M.C. Asser Press.

Nicoll, C., Prins, J.E.J., and van Dellen M.J.M. (2003), *Digital anonymity and the law: tensions and dimensions*, T.M.C. Asser Press, The Hague.

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)*, 360—361, Seattle, Washington: Association for Computing Machinery.

Reiter, M.K. and Rubin, A.D. (1998), Crowds: Anonymity for Web Transactions, *ACM Transactions on Information and System Security*, **1**(1):66--92.

Reiter, M.K. and Rubin, A.D. (1999), Anonymity Loves Company: Anonymous Web Transactions with Crowds, *Communications of the ACM*, **42**(2):32--38.

Rieke, A and Demuth, T. (2001), JANUS: Server Anonymity in the World Wide Web. In Gattiker, U.E. (ed.), *Conference Proceedings EICAR International Conference*, 195-208, München, Deutschland.

Sims, A. (2003). Court Assisted means of Revealing Identity on the Internet. In Nicoll, C., Prins, J.E.J. and Dellen, M.J.M. van (eds.), *Digital Anonymity and the Law. Tensions and Dimensions*. (Information Technology & Law Series, 2), 271--286. Den Haag: T.M.C. Asser Press.

Steenbruggen, W.A.M. (2002). Annotatie bij Voorzieningenrechter Rb. Utrecht 9 juli 2002 (Teleatlas/Planet Media Group), *Computerrecht*, **21**: 297--298.

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

Voermans, W.J.M. (1995), *Sturen in de mist…, maar dan met radar. Een onderzoek naar praktisch haalbare vormen van computerondersteuning bij het ontwerpen van regelingen*, Tjeenk Willink, Zwolle.

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.

Wong, H. and Sycara, K. (2000), A Taxonomy of Middle-agents for the Internet. In P*roceedings of the Fourth International Conference on Multi-Agent Systems (ICMAS'2000*, pp. 149--161, Boston, Massachusetts, USA: IEEE Computer Society*).*

The Council of the European Communities, Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, Official Journal L 122 , 17/05/1991, 42--46.