

Privacy Incorporated Software Agent (PISA)

Proposal for building a privacy guardian for the electronic age

By: Drs. John J. Borking, vice-president Dutch Data Protection Authority

Introduction

In the coming years, electronic commerce (E-commerce) and electronic government (E-government) will become more and more part of citizens' every day life. Many transactions will be performed by means of computers and computer networks. However, several hurdles have to be taken before E-commerce and E-government can develop its full potential.

An essential element of E-commerce and E-government is the collection of information on large computer networks, where either the information itself is the product sought, or information about products and services is being retrieved. Currently the retrieval of information on large computer networks, in particular the Internet, is getting more and more complicated. The volume of the stored information is overwhelming, and time and capacity needed for retrieval of information is growing strongly. Congestion in computer networks is a serious problem.

Numerous services are currently available to ease these problems, ranging from simple push technologies such as "PointCast" which brings information to your doorstep by "narrow-casting" or filtering information based on an individual's specified interests; to sophisticated systems that allow for the "personalization" of network user sessions and the tracking of user activities. Collaborative filtering of a user's "clickstream" or history of Web-based activity, combined with neural networks, which look for detailed patterns in a user's behavior, are just beginning to emerge as powerful tools used by organizations of all kinds.

While the majority of these technologies are at the moment essentially being in design and utility, they are indicative of the types of products that are being developed. The end result culminates in the creation and development of Intelligent Software Agent Technologies (ISATs). Intelligent Software Agents are software programs, at times coupled with dedicated hardware, which are designed to complete tasks on behalf of their user without any direct input or supervision from the user.¹ Agents for that purpose contain a profile of their users. The data in this profile are the basis for the actions an agent performs: searching for information, matching this information with the profile and performing transactions on behalf of its user.

Specific technology objectives

At first glance, intelligent agent technologies (ISAT) appear to hold out great promise for automating routine duties and even conducting high level transactions. However, upon greater reflection, it becomes clear that ISATs could present a significant threat to privacy relating to the wealth of personal information in their possession and under their control. Accordingly, it is highly desirable that their development and use reflect European privacy standards (i.e. European Union Directives 95/46/EC and 97/66/EC) in order to safeguard the personal information of their users.

The functionality and utility of user agents, lies in what they can do for the user. Remember their whole *raison-d'être* is to act on one's behalf and function as one's trusted personal servant, serving one's needs and managing one's day-to-day activities.

Their powers are constrained by a number of factors: the degree of software sophistication, the number of services with which they can interact, and, most importantly, the amount of personal information that they possess about the user.

User Profiling

It is this issue of "user profiling" that is at the core of the privacy risk associated with the use of ISATs. Typically, an ISAT user profile would contain a user's name, contact numbers and e-mail addresses.

Beyond this very basic information, the profile could contain a great deal of additional information about a user's likes and dislikes, habits and personal preferences, frequently called telephone numbers, contact information about friends and colleagues, and even a history of Web sites visited and a list of electronic transactions performed.

Because agents could be requested to perform any number of tasks ranging from downloading the daily newspaper to purchasing concert tickets for a favorite singer, the agent is required to know a great deal of information about the user.

In order to function properly, ISATs must also have the following characteristics²:

- Mobility, or a connection to a communications network;
- Deliberative behavior, or an ability to take an action based on a set of criteria;
- The following three abilities -- to act autonomously, co-operatively, and to learn.

Depending upon the levels of security associated with the user profile, this information may be saved in a plain text file or encrypted. However, the security of the data residing within the agent is only one part of the concerns regarding privacy.

The arguably more significant concern is the dissemination of information during transactions, and in the general conduct of the agent's activities on behalf of the user.

As an agent collects, processes, learns, stores and distributes data about its user and the user's activities, the agent will possess a wide variety of information which should not be divulged unless specifically required for a transaction. In the course of its activities, an agent could be required, or be forced to divulge information about the user that he or she may not wish to be shared.

The most important issue here is one of openness and transparency. As long as it is clear to the user exactly what information is being requested, what purpose it is needed for, and how it will be used (and stored), the user will be in a position to freely make decisions based on informed consent.

Of even greater concern is the situation where the ISAT may not be owned directly by the user but is made available (rented, leased) to the user by an organization in order to assist in accessing one or more services³.

Privacy Threats of ISATs

Summarizing, there are two main types of privacy threats that are posed by the use of ISATs:

1) Threats caused by agents acting on behalf of a user (through loss of control over the activities that are executed to get the right results, through the unwanted disclosure of the user's personal information and when an agent runs into a more powerful or an agent in disguise),

And;

2) Threats caused by foreign agents that act on behalf of others (via traffic flow monitoring, data mining and even covert attempts to obtain personal information directly from the user's agent or by entering databases and collecting personal data)⁴.

Resuming, the user is required to place a certain degree of trust in the agent -- that it will perform its functions correctly as requested. However, this trust could well come with a very high price tag, one that the user may have no knowledge or awareness of -- the price to his or her privacy. Failing to ensure such trust may prove to be a mayor hindrance for the development of electronic transactions and commerce.

Most Member States in the European Union have by now implemented the European Directives 95/46/EC and 97/66/EC. The first mentioned Directive provides a general legal framework for the protection of personal data. The second one contains specific privacy requirements for telecommunication. The current challenge is to implement the EU based national legislation in such a way that effective consumer and citizen privacy protection is the result.

Privacy-Enhancing Technologies (PET)

Conventional information systems generally record a large amount of information. This information is often easily linked to an individual. Sometimes these information systems contain information that is privacy-sensitive to some individuals. To prevent information systems from recording too much information the information systems need to be adjusted.

There are a number of options to prevent the recording of data that can be easily linked to individuals. The first is not to generate or record data at all. The second option is not to record data that is unique to an individual (identifying data). The absence of such data makes it almost impossible to link existing data to a private individual. These two options can be combined into a third one. With this third option, only strictly necessary identifying data will be recorded, together with the non-identifying data.

In PISA we will study how this Privacy Enhancing Technology (PET) can be implemented in software agents.

The conventional information system contains the following processes: authorization, identification and authentication access control, auditing and accounting. In the conventional information system, the user's identity is often needed to perform these processes. The identity is used within the authorization process, for instance, to identify and record the user's privileges and duties. The user's identity is thus introduced into the information system. Because in a conventional information system all processes are related, the identity travels through the information system.

The main question is: is identity necessary for each of the processes of the conventional information system? For authentication, in most cases, it is not necessary to know the user's identity in order to grant privileges. However, there are some situations in which the user must reveal his identity to allow verification of certain required characteristics.

For identification and authentication, access control and auditing the identity is not necessary. For accounting, the identity could be needed in some cases. It is possible that a user needs to be called to account for the use of certain services, e.g. when the user misuses or improperly uses the information system.

Identity Protector (IP)

The introduction of an Identity Protector (IP)⁵, as a part of the conventional information system, will structure the information system in order to protect the privacy of the user. The IP can be seen as a part of the system that controls the exchange of the user's identity within the information system.

The Identity Protector offers the following functions:

- 1 Reports and controls instances when identity is revealed;
- 2 Generates pseudo-identities;
- 3 Translates pseudo-identities into identities and vice versa;
- 4 Converts pseudo-identities into other pseudo-identities;
- 5 Combats misuse.

An important functionality of the IP is conversion of a user's identity into a pseudo-identity. The pseudo-identity is an alternate (digital) identity that the user may adopt when consulting an information system.

The user must be able to trust the way his personal data is handled in the domain where his identity is known.

The IP (as system element), can be placed anywhere in the system where personal data is exchanged.

This offers some solutions for privacy-compliant information systems.

Techniques that can be used to implement an IP are: digital signatures, blind digital signatures, digital pseudonyms, and trusted third parties.

In PISA the technological objective is to solve the problems of design and implementation of an IP in software agents to be used on the electronic highway for privacy issues.

PET-Agent (PISA)

The challenge is to design an PET-agent that independently performs these tasks, while fully preserving the privacy of the persons involved, or at least up to the level specified by the persons themselves. The agent should for that purpose be able to distinguish what information should be exchanged in what circumstances to which party. The challenge here is to implement privacy laws, specifically the European Directive 95/46/EC (being the highest privacy standard at this moment in the world) and other rules into specifications for a product. Next the specifications have to be implemented by software programming. Also there should be appropriate (cryptographic) protection mechanisms to ensure the security of the data and prevent 'leakage' to third parties.

PET-agents (PISA) will enable the user in its quality of consumer or citizen in e-commerce and e-government transactions and communications to protect himself against loss of his informational privacy contrary to systems like P3P where an asymmetric situation exists to the benefit of the web site owner. PISA empowers the consumer and citizen to decide at any time and in any circumstance when to reveal his or her identity.

Specific Demonstration Objectives

Thus, if the use of agents could lead to so many potential privacy risks, one wonders if it could be possible for anyone to use ISATs safely. I believe this still remains within the realm of possibility, and that the answer lies in the use of so-called privacy-enhancing technologies (PET). The tracking and logging of a person's use of computer networks is a major source of potential privacy violation. Conventional information systems perform the following transactions: authorization, identification and authentication access control, auditing and accounting. At each phase, a user's identification is connected with the transaction. However, by means of a system element (filter) called the "Identity Protector" (IP) the design of a system will go a long way to protecting privacy. The introduction of an IP into an information system can improve the protection of the user's information by structuring the system in such a way as to remove all unnecessary linkages to the user's personally identifying information.

The Identity Protector filter can be placed either between the user and the agent; this prevents the ISAT from collecting any personal data about the user without the knowledge and prior consent of the user. Conversely, the IP can be located between the agent and the external environment, preventing the ISAT from divulging any personal information unless specifically required to do so in order to perform a particular task or conduct a specific transaction. Additional technical means may also be integrated into the ISAT in order to bring even more transparency to the user in the operation of the agent, thus ensuring the user's knowledge, and if necessary, informed consent.

An international team consisting of the Dutch Physics and Electronics Laboratories (TNO), The Dutch Technical University of Delft, Sientient, a Dutch company designing data mining systems, Italsoft from Roma (Italy), CIME-Labs and Toutela from Paris, the Canadian National Research Council and the Registratiekamer (Dutch Data Protection Authority) will build a demonstrable PISA not later than 2003.

The main objectives of the demonstrator are to show the security of the privacy of the user in the types of processes that could be employed:

- Clearly detailed audit logging and activity tracking of agent transactions so that the user can monitor and review the behavior of the agent;
- The use of programs to render the user and/or the agent anonymous, or alternatively, the use of a "pseudo-identity" unless identification is specifically required for the performance of a transaction;
- The use of identification and authentication mechanisms such as digital signatures and digital certificates to prevent the "spoofing" of a user or their agent by a malicious third party intent on committing fraud or agent theft;
- The use of data encryption technology to prevent unauthorized "sniffing" or accessing of agent transaction details;
- The use of trusted sources: the agent can be instructed to only visit sites that have been independently verified (through a variety of means such as trusted seals, audits, etc.) as having proper privacy provisions in place;
- Placing limitations on an agent's autonomy so they only perform a certain range of activities -- limited activities will be permitted to be freely conducted without additional authorization; any requests for unauthorized transactions will be flagged for the user to scrutinize.

The integration of these technologies into the core of the ISAT, combined with a process that places similar technology between the agent and the external environment would result in a demonstration system PISA that shows and enjoyed the maximum protection against threats to the user's privacy enabling users protecting themselves not being dependent systems like P3P or on other privacy seals. The international team hopes to get a subsidy of the European Commission under EU Technology program.

Contribution to EU Technology programme and key action objectives

The PISA-project contributes to EU - IST-programme and key action line II4.1 and II4.2 objectives:

II4.1: " To develop and validate novel, scalable and interoperable technologies, mechanisms and architectures for trust and security in distributed organizations, services and underlying infrastructures".

With the focus on:

" Building technologies to empower users to consciously and effectively manage and negotiate their "personal rights" (i.e. privacy, confidentiality, etc.). This includes technologies that enable anonymous or pseudonymous access to information society applications and services, for example by minimizing the generation of personal data. "

II4.2: To scale-up, integrate, validate and demonstrate trust and confidence technologies and Architectures in the context of advanced large-scale scenarios for business and everyday life. This work will largely be carried out through trials, integrated test-beds and combined RTD and demonstrations.

Focus on:

"Generic solutions that emphasize large-scale interoperability and are capable of supporting broad array of transactions (e.g. e-purses and e-money), applications and processes.

Development of solutions that reconcile new e-commerce models and processes with security Requirements, paying particular attention to the needs of SMEs and consumers

Validation should generally include assessing legal implications of proposed solutions, especially in the context of solutions aimed at empowering users to consciously and effectively manage their personal "rights and assets".

PISA contributes at building a model of a software agent within a network environment, to demonstrate that it is possible to perform complicated actions on behalf of a person, without the personal data of that person being compromised. In the design of the agent an effective selection of the presented privacy enhancing technologies will be implemented. We label this product as a Privacy Incorporated Software Agent (PISA).

The PISA demonstration model is planned to be a novel piece of software that incorporates several advanced technologies in one product:

- Agent technology, for intelligent search and matching;
- Data mining or comparable techniques to construct profiles and make predictions;
- Cryptography for the protection of personal data, as well as the confidentiality of transactions.

Additionally the project involves:

- Legal expertise to implement the European privacy legislation and the needed development of new legal norms in this field;
- System design knowledge in order to turn legal boundary condition into technical specifications;
- Advanced software programming skills to implement the privacy boundary conditions.

In order to prove the capability of the PISA-model, we propose to test it in a model environment in two cases in e-commerce that closely resembles a real-life situation.

Case 1: Matching supply and demand on the labor market

The demonstrator will be applied to a practical case, which is suitable to test several aspects of privacy protection. Testing of the demonstrator will be done in a local network environment. The proposed test object is the matching of supply and demand on the labor market. In the coming years it is expected that the matching on the labor market will increasingly be performed through such (Internet based) intermediaries. The agent on behalf of the consumer /citizen carries in this process the profile of a person, including sensitive information about his or her history, (dis) abilities, skills, labor history etc. When matching this information with the available functions, a match has to be made between the user profile and the demands of the party requiring personnel. In this process personal data will be exchanged in an anonymous way. After the match has been made successfully and has been reported so by the agent to its user, he or she may decide to reveal his / her identity.

Case 2: Matching supply and demand for vehicle and real estate markets

The second demonstrator will be an extension of an existing Web portal, providing a range of intermediation services oriented towards both individual consumers and business users, addressing areas like buying and selling of vehicles (cars, vans, boats, ...), buying, selling and renting of real estate, etc. Respecting and protecting privacy of the users posting requests on this site is a key aspect of user acceptance of the intermediation services proposed. Testing of the demonstrator will be done in a local network environment. The proposed test object is the matching of supply and demand on the vehicle and real estate markets.

In the coming years it is expected that the matching on these markets will increasingly be performed through such (Internet based) intermediaries. In the intermediation process, the agent matches requests and offerings posted by individuals, which may encompass confidential information not to be disclosed to the outside world.

Innovation

E-commerce/ E-government and other ICT developments introduce a fundamentally new modus of consumer-transactions with new challenges to data protection. A growing awareness exists that, next to a legal framework, effective privacy protection should be supported by technical and organizational measures. This is particularly needed in view of the difficulty to attach global electronic transactions to a particular jurisdiction.

In order to increase the visibility of privacy compliance websites involved in E-commerce activities apply so-called 'privacy seals' like P3P. These are mere visual statements of compliance, the credibility of which is difficult to judge for consumers.

Rather than relying on legal protection and self-regulation only, the protection of consumers' privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing. This group of technologies is commonly referred to as Privacy Enhancing Technologies (PET).

In the context of E-commerce on the consumers market, a major current initiative to increase privacy compliance is the so-called P3P, under development by the W3C consortium. Major players in the software industry back the W3C consortium. P3P provides for a standardized language and interface for both consumer and website to provide their personal data and privacy preferences. Transactions can be accomplished according to the specified level of openness given by consumers on their personal data.

The P3P, as being developed now, does not foresee any 'negotiation' between consumer and market party. It is basically a compliance check between consumer preferences and website policy, therefore relatively static and it needs active user input for each transaction. Given the limited capability of P3P it is also difficult to implement the privacy principles underlying the European Directive into this technology. Although an essential first step, P3P is not sufficient for effective and efficient privacy protection of consumers.

As will be demonstrated later E-commerce and E-government will only lift off if the search for matches of supply and demand and the accompanying negotiation on privacy preferences can be performed in a distributed way. This would both decrease the load on network capacity and on the time spent by a consumer. Intelligent agents are the right types of software for this task. In contrast to current systems like P3P, agents should be able to negotiate intelligently with the consumer, a website or with each other. Skills to negotiate privacy and a common platform for communication will have to develop. This level of sophistication will enable developers to implement more deeply the principles of privacy into the technology itself. Once equipped with these skills a 'PET-agent' will become an enabler of secure E-commerce and E-government and will provide a structural feed back and control of the user over his personal or to him identifiable data in cyber space preventing harmful privacy intrusions.

Dutch Data Protection Authority

The project results will be of importance to the Dutch Data Protection Authority and other privacy commissioners in several respects.

Firstly the resulting model software will be an element towards an effective and user-friendly implementation of the European Directive 95/46/EC. Parallel to the legal approach, the emergence of new forms of electronic business and interactions urges for a data protection approach that ties in more closely with the dynamic technological environment.

On a time scale of a few years, the software agents to be built, will become an important instrument for data protection, additional to the legal instruments used now. The results to be achieved will have a feedback on the legislative process within the EU as well.

For the DDPAs participating in the project helps the office to develop practical ways to make its task effective as well as a way to keep up its renowned high standard of expertise on the connection between ICT and privacy.

It is necessary to be within the arena of technology development and to translate the Directive 95/46/EC into design recommendations if the organization should retain its viability as authority, and to serve the consumers within the EU, in matters of data protection.

A fruitful collaboration between the DDPAs and the industrial partners, finally, will also help to keep up the competitive advantage of the European software industry in designing tools that provide trust and security as added values.