NRC·CNRC

NRC Publications Archive
Archives des publications du CNRC

Privacy in Distributed Electronic Commerce

Korba, Larry

This publication could be one of several versions: author's original, accepted manuscript or the publisher's version. / La version de cette publication peut être l'une des suivantes : la version prépublication de l'auteur, la version acceptée du manuscrit ou la version de l'éditeur.

NRC Publications Record / Notice d'Archives des publications de CNRC:
https://nrc-publications.canada.ca/eng/view/object/?id=130e83c0-6be5-4089-80e1-e37ab1ad8b7b
https://publications-cnrc.canada.ca/fra/voir/objet/?id=130e83c0-6be5-4089-80e1-e37ab1ad8b7b

Access and use of this website and the material on it are subject to the Terms and Conditions set forth at https://nrc-publications.canada.ca/eng/copyright
READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS WEBSITE.

L'accès à ce site Web et l'utilisation de son contenu sont assujettis aux conditions présentées dans le site https://publications-cnrc.canada.ca/fra/droits
LISEZ CES CONDITIONS ATTENTIVEMENT AVANT D'UTILISER CE SITE WEB.

Questions? Contact the NRC Publications Archive team at PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca. If you wish to email the authors directly, please see the first page of the publication for their contact information.

Vous avez des questions? Nous pouvons vous aider. Pour communiquer directement avec un auteur, consultez la première page de la revue dans laquelle son article a été publié afin de trouver ses coordonnées. Si vous n'arrivez pas à les repérer, communiquez avec nous à PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca.

National Research Council Canada | Conseil national de recherches Canada

Canada

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de Technologie de l'information

NRC·CNRC

*Privacy in Distributed Electronic Commerce**

L. Korba
January 2002

***published in** Proceedings of the 35th Hawaii International Conference on System Science (HICSS), Hawaii. January 7-11, 2002. NRC 44891.

Copyright 2001 by
National Research Council of Canada

Permission is granted to quote short excerpts and to reproduce figures and tables from this report, provided that the source of such material is fully acknowledged.

Privacy in Distributed Electronic Commerce

Larry Korba[1], *Member, IEEE*
National Research Council of Canada
Larry.Korba@nrc.ca

Abstract

In recent years there has been a movement toward deployment of distributed approaches for electronic commerce. Intelligent software agents, for instance, may be instructed to act on behalf of human users in electronic transactions. A challenge with this approach is that the agents would be entrusted with access to sensitive personal or business information. How can this sensitive information be protected from unauthorized access? How can agents negotiate across jurisdictional boundaries; both corporate, and country? The latter question is of particular concern when one considers the potential for considerable variance between the regulations and policies of different governments and corporations. This is especially evident with the disparity of legislation for privacy in different countries. How can disparate regulations be accommodated effectively? What technologies are appropriate for maintaining user privacy and for protecting sensitive information for agent-based e-commerce? In this paper, we describe the issues that provoke privacy challenges for agent-based e-commerce due to current and impending privacy legislation as well as an approach for policy-driven privacy negotiation for use in distributed agent-based systems.

***Index terms*—Privacy, Security, Privacy Law, Agent, Policy, Agent Negotiation.**

1. Introduction

Recent developments in electronic commerce explore the application of cooperating, distributed software rather than single, monolithic applications. One example of this approach is distributed agent-based systems. These approaches offer the advantage of problem partitioning and the potential for improving application scalability.

Several challenges face the developers of agent-based solutions in this domain. The key challenges include secure and efficient software agent deployment, secure communications and the difficulties of developing and monitoring agent systems deployed across a network. While there have been many approaches developed for dealing with these challenges, still other challenges persist. One of them involves protecting privacy of personal information throughout electronic commerce operation.

Protection of privacy and policies describing how organizations handle personal information may have a broad impact on whether and how networked applications are used. Indeed whether or not a company can do business may depend upon compliance with privacy of confidentiality regulations or requirements. Agent-based applications may not be accepted if it becomes evident that the privacy of personal information is not upheld. From an organizational perspective, the way in which technology is used is affected by how the organization deals with privacy issues. In a restrictive environment, individuals tend to be less likely to use email, let alone electronic commerce applications with abandon [1]; caution prevails.

Over the last few years privacy laws have been put in place in different jurisdictions. The European Union's 1995 adoption of the "Data Directive" ushered in a new era of data privacy regulated by government [2]. Other countries including Australia, Argentina and Canada, have more recently enacted privacy legislation. In the United States, though there is a consensus on the need for data privacy legislation. However movement has been very slow in that direction. The disparity of regulations for privacy between different countries may make it difficult or impossible for them to exchange data. For instance, it is possible for the EU to sanction a US company against data exchange with the EU according to the Data Directive. Even when all nations are operating on a level legislative playing field, technology implementing and proving adherence to privacy regulations will be required.

In this paper we examine recent developments related to the legal, social and technical aspects related to privacy in electronic commerce systems. This examination underscores why privacy management is important for the success of agent-based electronic commerce systems. We

[1]National Research Council, Room 286B, Building M-50, Montreal Road, Ottawa, Ontario K1A 0R6. (613)998-3967, NRC Paper # 44891

also describe our current work in the development of privacy enhancing technologies for distributed applications.

2. Problem statement

Distributed object or multi-agent technology offer many potential advantages for Electronic Commerce [3] and other domains [4], [5]. The benefits of agent-based systems include:

- Decrease network traffic by performing computational intensive processing near the server that is the source of information.
- Greater autonomy due to the asynchronous nature of operation of an agent.
- Ease transportability of services across providers.
- Increased network availability by autonomy and asynchronous agent operations.
- Reduce time and effort for installation, operation and management.
- Enable "on demand" provision of special services.
- Allow a more decentralized realization of management and service control thereby reducing the dependence on network availability, resulting in a more robust system.

In general, an agent-based approach provides the advantage of problem partitioning and the potential for application scalability. While all of these advantages have led to the accelerated development of new electronic commerce applications of agent-based systems, securing the operation of these systems remains a challenge [6]. Assuring and maintaining the privacy of the personal data exchanged and stored in the operation of these systems stresses the security requirements of the agent system design. There are both market and legal pressures for assuring privacy of electronic commerce system operation.

From a market perspective, privacy of personal information is becoming big business. Prominent on most web sites is the privacy policy for the web site. Organizations like Truste [7] offer assessment of the privacy practices of an online presence to assure level of conformance to their stated policy. It is a black eye for an online company to breach privacy policy guidelines. Indeed there is a growing list of companies becoming involved in the delivery of online privacy services for individual and corporate clients [8]. These include: Zero Knowledge Systems, Ziplip and Anonymizer. Companies like American Express are experimenting with anonymous on-line payment schemes [9]. A key element in offering online services nowadays includes offering privacy-enhanced services. For most of the World Wide Web, there is no legal requirement for privacy compliance. This situation is changing, led by the European Union's 1995 Data Directive.

2.1. EU 1995 Data Directive

In 1995 the European Union Parliament adopted

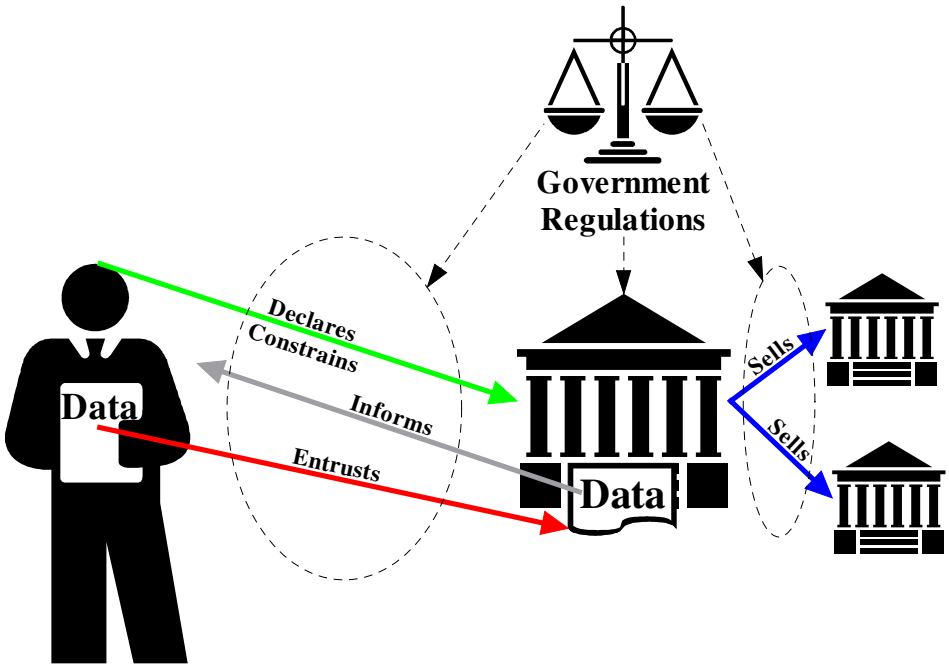

Figure 1. This Diagram indicates the intended roles of government regulations and the data protection agencies in the execution of electronic commerce.

Directive 95/46/EC. This legislation is now known as the Data Directive. The Data Directive imposes strict restrictions and requirements on the collection, use and disclosure of personal data of citizens of the European Union. There are four basic principles associated with this law: that privacy for personal information exists, that an individual may withhold personal data, that an individual may control dissemination of personal information, and that personal information is shared in a trusted situation.

The view of the operation of these government regulations is shown in **figure 1**. Effectively the law places restrictions on the interactions between individuals and organizations that either collect, purchase or use personal data. The basic tenets of the Data Directive include: no secret personal record system are kept, individuals have the right to access and amend their information, prior consent must be obtained any use of the data, notice must be given for any use of the data, managers of the data processing companies are accountable for the privacy of personal data held, the data protection authority in each country is responsible for dispute resolution, and, governments may intervene in the any dispute. In terms of enforcement, there are Data Protection authorities for each member country. The fines for breaching the data directive range from $3000 to $600,000 per offence (depending on country). Beyond fines, conviction may also result in sanctions against companies, seizure of data, and injunction against operation. Clearly, within the European Union, the bite of the Data Protection Authorities underscores the importance of compliance with the Data Directive. Indeed, article 25 of the Data Directive may allow the EU to sanction against data exchange with a company (EU-based or foreign) that does not comply with the directive [10]. The law has considerable scope and bite in the enforcement of personal privacy protection. New technologies such as Agent-Based electronic commerce can complicate compliance with the law.

2.2. Agent-based e-commerce privacy compliance

For web-based applications, it has become a market imperative to support some sort of privacy policy. Typically, these policies consist of a written and audited policy disclosing [7]: what personal information is being gathered, how the information will be used, with whom the information will be shared, choices regarding how collected information is used, safeguards for protection of information from loss, misuse or alteration, and, how you can update or correct inaccuracies in your information. Compliance to a privacy seal program involves a privacy audit of the way in which the company interacts with users, and implements technologies to provide the data protection required under the policy. Even for the client-server situation, there are very few tools to automatically implement privacy seal policy throughout an organization.

With respect to intelligent agent-based electronic commerce, there has been little research in the development of privacy compliance. The security of the underlying technology supports the ability of the application to deliver privacy. An issue with agent-based systems is the security of their operation [11]. In the electronic commerce context, a software agent is an entity that works autonomously towards a goal. It is given the authority to operate on behalf of an individual or organization. While progressing towards its goal, the software agent may interact with other agents on different computers over various networks. Software agents may be either stationary or mobile.

Systems deploying mobile agents lead to increased security threats. These threats include: the agent platform against the agent, agents against other agents and other agents against the agent system. Various techniques have been developed to mitigate many of these threats. Techniques like sandboxing, signed code, state appraisal, obfuscated code, proof-carrying code, computing with encrypted functions among others are at various stages of development. These approaches have been developed practically to varying degrees. Challenges persist especially in the prevention of security breaches from untrusted hosts.

Security of the agent platform alone does not assure system privacy. Techniques and methodologies are required to assure confidential communication, secure audit of privacy related transactions, and secure storage and maintenance of private data. Overall, the agent system must comply with regulations or policies from government, organizations and individuals. Some of the types of the information that may be collected or exchanged during the course of agent-based electronic commerce interactions that should be kept private include:

1) Personal information and proprietary technical or business-related information. The electronic commerce application acts on behalf of an individual or organization. Often, the agent requires confidential information regarding the organization in order to interact with other agents or brokers. As well, confidential or private information related to the assigned tasks must be exchanged. Depending on the nature of the collaboration, this information may be quite detailed and sensitive. How do collaborators share information in a selective manner with other participants? For instance, different collaborators either through their roles, personal or corporate preferences, may sanction different levels of privacy related to information exchanged or collected during interactions depending on the origin or nature of the interacting parties or depending upon a cost-benefit or risk analysis of the interaction.

2) Itinerary information. The current, previous, and projected locations of a mobile agent or the position of a

stationary agent should be kept private. Information about the agent whereabouts could indicate ownership or current or intended activity. As well, location information could be used by an agent or human to attack the agent in order to extract private information or to prevent the agent from operating. The latter case would be a denial of service attack on the agent.

3) Communication connection. Communication between the agent and the resources it contacts must be kept confidential. Secure Sockets Layer v. 3 and VPN approaches offer established solutions for this issue. Irrespective of knowing what information is exchanged, the fact that an individual or organization is interacting with others in distributed electronic commerce environments gives an indication of the manner in which one interacts with others. Information such as: the speed with which a response is made, the number of interactions, the quantity of information exchanged with others, and the appropriateness and context and amount of the information exchanged all provide an important indication of the types of relationships the agent forms during its electronic commerce operations. This information may be collected by third parties. It may be mined from logs relating information exchange between users. This information should therefore be kept private.

To meet and to manage the challenges for distributed privacy with agent-based electronic commerce, we are developing a distributed policy-based approach for agent-based electronic commerce. The next section describes our approach and building blocks.

3. Distributed Privacy System

Our approach attempts to meet the following requirements for privacy implementation:

1) Policy-based privacy. Policy is considered to be information which can modify the behavior of a system [12]. When applied to the privacy domain, privacy policy contains statements and rules that indicate privacy preferences. The rules expressed in the policy offer a means for expressing preferences for both the information gatherer and the information provider [28]. For the gatherer, they indicate the way in which private information will be handled. For the provider, they indicate preferences for the way in which information may be handled. Considering agent-to-agent interaction, all gatherers and providers of services may specify policies indicating the type of information considered to be private and how it will or should be dealt with.

2) Accountability. The system audits activities of participants, keeping track of compliance with individual and agreed upon privacy policies. Participating entities may receive audit logs of activities pertaining to triggered, scheduled or negotiated privacy exceptions. This approach is intended to bring an element of enforced privacy compliance.

3) Accessibility/Flexibility. Participants may access and adapt policies to specify privacy requirements in detail.

4) Automated policy negotiation. To determine the classification, handling and disposition of information considered to be private, a policy negotiation engine reconciles differences between collaborating parties. This approach simplifies the process of setting joint privacy agreements between parties.

5) Consensual assignment. Participants may be notified in situations wherein their informed consent is required to release information requested by any party.

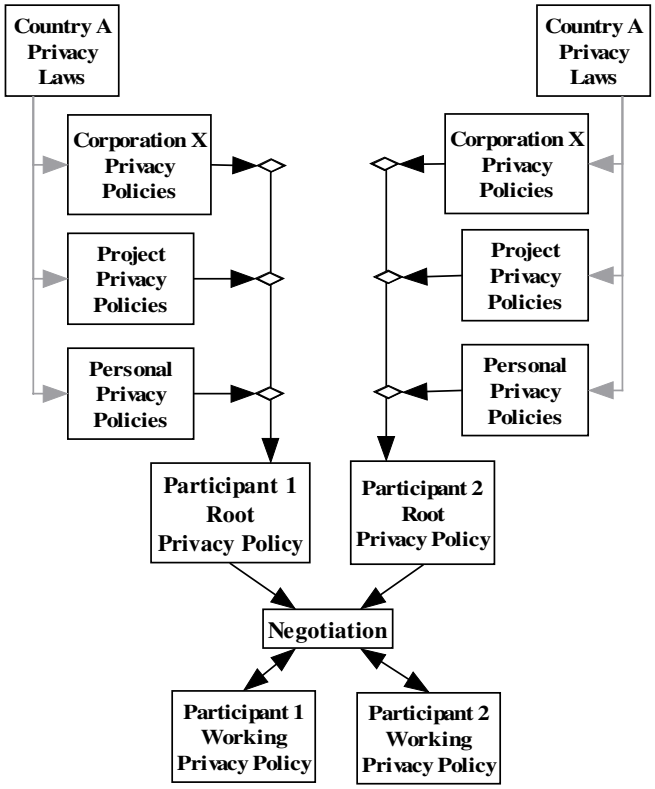

Figure 2. Dependencies between working privacy policies and government regulations, and company and personal privacy policies. The Root Privacy Policy is the combination of the country, corporation, project and personal privacy policies.

The "Root" Privacy Policy for the participant in an exchange of private information (**figure 2**) is considered to be the core policy used as the starting point for information exchange with others. It is comprised of a combination of several policies. For example, these policies may include

corporation, project as well as personal privacy policies. The laws of the country influence the privacy policies at all levels. The P3P preference exchange language, Appel [34], is the basis used to build privacy policies. As schematically illustrated in **figure 2**, many different policies may interact to generate the root policy. For instance, these policies may include:

- Aspects of a country's privacy laws or regulations influence the content of the privacy policies. Effectively, they create the framework within which the policies operate. The laws may place requirements upon the operation of an information gathering organization. For instance, the Directive 95/46/EC requires that information gatherers provide citizens with access to the information stored about them. Under these circumstances, the policy for the gatherer will indicate compliance with this regulation and procedural details.
- Privacy policies for the corporation indicating how the corporation may deal with private employee information as well as how the company wishes employees to deal with their own information when conducting business on behalf of the corporation.
- Privacy policies for a project. In the cases of corporate and project policies, there may be some requirements for confidentiality of corporate information. These policies are separate from privacy policies for individuals. Yet, some projects may require such secrecy that limitations upon the types of personal information exchange for project members may be restricted. This means that a somewhat lax individual privacy policy would be "overruled" by a demanding project policy.
- Personal privacy policy. This policy indicates the choices an individual may make concerning how he or she wishes to have others deal with personal information. For instance, there may be preferences regarding the options an information gatherer may provide concerning client recognition (the use of cookies), or how personal data is stored.

Thus the corporate and project policies will have a bearing upon the content of the root policy. The content of and the extent to which these policies may modulate root policy depend on the privacy legislation for the jurisdiction. Other policies may modulate the root policy. For instance, the security policy of an organization may limit or forbid the use of cookies, or scripting languages for browsers. Such organizational policies may override personal preferences for network activities performed with company resources.

Policy negotiation (see f**igure 2**) involves the exchange and analysis of the root policies of the participants to determine where there are conflicts. Conflicts are considered to be situations where there is a mismatch between the rule sets of the two parties. For instance, a conflict may arise when one root policy prohibits any information exchange with a third party while one of the other participators does. The negotiator follows a set of rules to deal with different conflict situations to produce the working privacy policies for the participants.

Figure 3 illustrates the overall framework in terms of the core services supplied for privacy management. While policies are specified for system operation, services may be attached to any operating agent of the system agents in the system, depending on policy requirements. Below is a description of each of the privacy and security services.

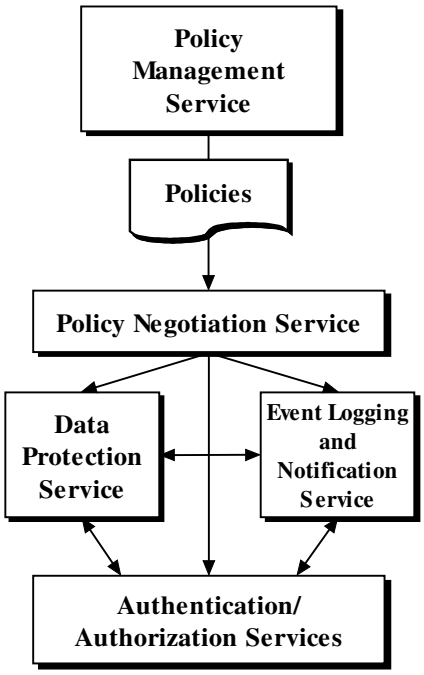

Figure 3. Policy-based Privacy and Security Services

3.1. Policy Management Service

This service manages the development and maintenance of policies for system privacy and security. Policies are embodied as XML documents. Users develop and maintain policies using a web-based interface. Authorized users may manage different policy options for handling the detailed privacy and security options for system operation. For instance, in the case of privacy

policies, a variety of options for user privacy are possible according to individual role (e.g. managers, employees, individuals, administrators). Typical options include:

- The level of protection required for potentially sensitive information.
- The types of events that will be logged (e.g. changes and access to profiles or student records, access to services, changes, etc.).
- Event filtering for user notification. For instance, a user may choose to be notified, when information about his or her transaction is accessed. The level of alarm indicated in this notification would be colored by the policy specified for the particular e-commerce interaction.

While the organization would have a general policy for privacy, options presented to e-commerce participants would be derived from the general policy. There may be different policies for different categories of participants. In these cases, some policies may be more flexible than others, allowing personal preferences to predominate in the negotiated privacy behavior of the system.

In a similar fashion, policies for system security are adjusted. In this case however, only the system administrator is authorized to change these policies.

3.2. Policy Negotiation Service

This service has three functions regarding policy: interpretation, negotiation and resolution. Policy actions are triggered by the occurrence of events in the execution for which, policy has been defined. Policy expressed in policy documents must be first interpreted. Where the event is triggered by interaction between two parties, the respective policy threads relating to the handling of the event must be negotiated. Negotiation involves assuring the expressed policies of both parties are upheld in the ensuing action. The resolution part of this service determines how an event is processed. In most cases negotiation will result in an automated resolution, based upon the degree of flexibility expressed by administration and between users. In cases where the user or institution has expressed inflexibility and there will likely be a conflict in resolution. In these cases, users are notified and allowed to select options as to how to proceed.

3.3. Data Protection Service

Depending on policy requirements, data relating to privacy and security (including policy documents themselves) may be stored and protected. Some institutions for instance may have a policy indicating that all student records must be stored encrypted in a particular manner (e.g. DES, triple DES, Rijndael, etc.), in a particular location (locally, or at a trusted hosted), as well as archiving requirements. This service handles the encryption and decryption process, and in concert with the authentication service for the generation, exchange and access to the encryption keys. Another function of this service is the protection of the distributed logs containing protected information about the interchanges of private data. In this case, the data protection service works with the event logging and notification service.

3.4. Event Logging and Notification Service

This service implements the logging and filtering of events for notification. The objective of this service is to provide users with an indication of compliance to expressed policy through a notification mechanism. Under the control of policy, the event logging service may invoke a process to monitor and filter privacy-related events in the system. These processes may be located at the user terminal within a user or terminal agent, or at one of the host servers for the system. Events may include changes to profiles, alterations or other accesses to student records etc. This service may also filter the logged events (based upon expressions in user policy) to determine when particular types of events occur.

3.5. Authentication/Authorization Services

These services assure the identities of and regulate the authorization of the users, agents and resources operating within the system. For the different types of users, there are different levels of authorization. Normally, authentication/authentication service acts as a trusted third party for determining access to services or other resources. In the situation where a user is operating remotely, without Internet access, the authentication service provides for local authentication and authorization.

3.6. General Issues

Our system is based upon a framework that provides some of the essential requirements for implementing secure agent-based applications in a variety of areas. In the development of our architecture, the main goals in the security and privacy area are:

- Secure channels for communications between agents or operators;
- Scalable design;
- Secure delivery of software agents,;
- Secure operation environment for the agents;
- Flexible security provisions;

Developments supporting these requirements have been reported previously [6]. An important issue is scalability. This is important especially when many hundreds of agents may interact with each other. The approach of having a central authority for managing policy would be a bottleneck. To help alleviate this bottleneck we use a distributed policy approach [13].

Figure 4 illustrates conceptually the central role the policy engine plays in agent operation. The various processes in **figure 4** may be distributed over different computers. The Policy Engine implements the policy negotiation service. Policy negotiation involves an exchange of policy entities between negotiating agents. Depending on the resolution of policy negotiation, the engine mediates privacy exception-based actions. The policy engine modulates what an authenticated task or individual is allowed to do. Privacy exceptions may trigger an event and transaction-logging mechanism to provide a means for recording the occurrence of specific policy-triggered activities. This approach offers a means for tracking and monitoring that the implemented policies are appropriately carried out for all privacy exception initiated actions.

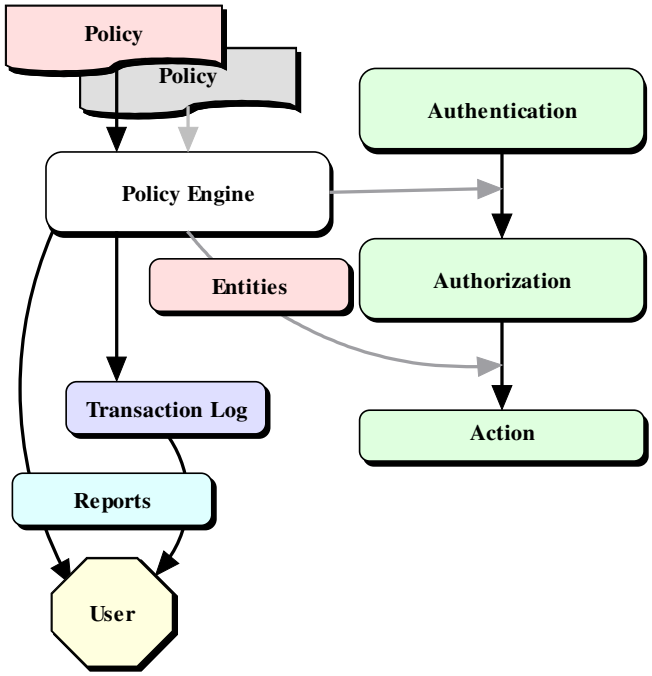

Figure 4. The policy engine plays a central role for managing privacy during agent interactions.

4. Related Work

With the development of the wired society it has become clear that technology is not privacy neutral. Garfinkel [14] suggests that current developments leave us with only two choices: 1) allow our personal data to rest in the public domain or 2) become hermits (no network/telephone use, no credit cards, no web surfing, etc.). The latter option is not an option considering the advantages Internet technologies, and, more importantly, the commercial drive to deploy electronic commerce solutions everywhere using every possible type of communication device.

Security for agent-based electronic commerce systems has been examined more from the point of view of security for the agent system [15] rather than focussing on the security and protection of information garnered or exchanged during a transaction. While access controls and fine-grained security control are important for secure agent operation, protection of the privacy of information is also vital. In the CSCW and e-learning area, for instance, Foley and Jacob describe a technique for specifying security in the development of secure electronic examinations for courseware [16]. Based upon activity analysis this approach provides some preliminary techniques for assessing the requirements for confidentiality in dealing with the courseware development application domain. While the authors do not describe a system for implementing a policy-based approach for dealing with confidentiality requirements in electronic collaboration in general, it does offer promise for analysis for the purpose of policy generation.

Security and privacy are considered to be a basic requirement in multi-agent applications. Considering the development and general acceptance of multi-agent systems for electronic commerce as well as computer supported cooperative work, it is clear that agent systems must have a certification process [17]. There are several multi-agent environments that provide different levels of security [18], [19]. The approach for most of these is to secure communication channels [6], [20] with protocols like Secure Sockets Layer (SSL) version 3. This approach does not address the need for flexibility in specifying application issues for privacy. For instance, it is often important to specify which communications should be protected and what information may be exchanged with third parties not only for privacy purposes but also to reduce computational overhead.

Prevelakis et al. [21] describe an agent-based framework for the exchange of electronic documents over open networks. This approach builds upon the low level security functionality offered in many agent platforms to offer some security regarding data exchange over networks. The authors state that the system eliminates unauthorized copying, redistribution or modification of the documents. The system provides authentication of the sender, recipient,

and the document. It implements a uniform policy and a trusted third party approach for authentication.

Agent-based applications have been developed for electronic commerce [22], [23], [24], supply chain management [25] and for CSCW [3], [26], [27]. The agent model provides system characteristics of cooperation, distribution, interaction, concurrence and autonomy. There has been relatively little attention paid to managing distributed electronic commerce privacy for the purpose of compliance with legal and/or corporate policy requirements. The impact of a lack of a well-defined structure for privacy and security of interactions can be broad on both the acceptance and the use of any technology. User perceptions of privacy provide an example of how policies can differ across organizational boundaries [1]. Different organizations have different values regarding the interactions and actions of their employees. For instance, in universities freedom of speech is considered of paramount importance, whereas in military establishments controls may be in place to ensure the protection of a nation's security, usurping individual privacy. Depending on the organizational setting, there can be a marked contrast as to how much personal and sensitive information individuals are willing to share through computer mediated communications. In effect, the privacy offered by a technology affects how individuals use that technology. User trust can be enhanced when organizations recognize the expectations of employees, provide policies expressing the guidelines and implement processes to carry out those policies.

Enormous amounts of information about web site visitors are being collected by thousands of web sites. The information collected may be aggregated, filtered and used for a variety of purposes. This may be done with or without the permission of the web site visitors. In a movement toward developing in the World Wide Web consortium (W3C) has developed the platform for privacy preferences (P3P) [28], [29]. P3P offers a way for users to reach an agreement with services such as web sites or applications that request data and offer a privacy practice. P3P offers a machine-readable means for specifying the privacy practice for a service. A user defines his or her privacy options in a user agent (potentially a plug-in for a web browser) and may be alerted when there is disagreement between a service proposal and the selected privacy options. Issues not covered by P3P are: 1) a means for negotiating a contract especially in a peer-to-peer exchange, 2) a means for proving privacy policies of all parties have been upheld, 3) a specification of how private information is protected 4) a non-web specific approach providing interactions beyond the simple exchanges, 5) more detailed specification of the requirement for the private information [30]. Our work offers an approach for addressing these issues.

6. Discussion and Conclusions

In this paper we describe the impetus for privacy-enhanced services to enable agent-based electronic commerce. In our discussion, we have drawn upon the legal, sociological and technical developments of electronic commerce and agent-based systems. We also describe early work in the development of an approach for managing and negotiating privacy for agent-based applications in electronic commerce.

An issue not addressed in this paper is the one associated with creating and operating electronic commerce applications on open computing platforms and open networks. It is difficult, or impossible to build applications that would protect information from unauthorized access on open computing platforms. Techniques such as software and hardware in-circuit emulation and reverse engineering may be used to launch an attack on private information. Reverse engineering an application to determine secrets though illegal in some jurisdictions can be trivial with applications that are not designed to safeguard against this intrusion. For these reasons, designing systems to operate with a high degree of security in open networking and computing environments is a challenging area for research. . Regarding open networks, while secure communication channels and encryption technologies may be used to assure privacy of information exchange, safeguarding against denial of service attacks is very difficult.

Our work is developing on several fronts. We are currently collaborating in the development of related privacy enhancing technologies for agent-based electronic commerce systems in the Privacy Incorporated Software Agent (PISA) project. PISA is a European Union 5th framework project. Commencing in January, 2001, this project involves researchers from the Netherlands, Belgium, France, Italy and Canada [31]. Our objective is the development of technologies to enable privacy protection for agent-based electronic commerce applications. The results of this project will be an approach for making detailed privacy threat analysis of intelligent agent electronic commerce applications and demonstration applications of specific privacy enhancing technology for intelligent agents.

At the same time, we are also examining the application of privacy technologies in other domains. We are investigating approaches and technologies for privacy enhancement is distributed manufacturing [32]. In this case, the objective is to develop approaches that would offer privacy and security controls for Internet-based manufacturing. In the e-manufacturing domain, different organizations may have different policies regarding the type and the amount of information that may be shared with

other organizations. A flexible approach for managing and for negotiating privacy and security policies automatically would be a vital enabling technology in this area.

We are investigating the applicability of distributed privacy policy approach in the area of electronic education. Within the constant learning environment promoted by most companies, employees are encouraged to take continuing education courses. Many of these courses are on-line. Information about the identity, personal preferences and progression of students in their courses should be held private. Indeed other security and privacy issues arise considering that the students may be taking online courses using employer-provided Internet access. A particular challenge in this work is assuring that the distributed privacy transaction logs are secure and original, i.e. unaltered. While there have been some developments in this area [33] they have yet to be successfully applied in distributed applications.

7. References

[1] S.P. Weisband, B.A. Reinig, "Managing user perceptions of email privacy, Communications of the ACM", vol. 38, no. 12, 1995, pp. 40-47.

[2] Information on the EU Directive on Data Protection http://www.privacy.org/pi/intl_orgs/ec/eudp.html

[3] P. Maes, R. Guttman, A. Moukas, "Agents that Buy and Sell", Communications of the ACM,Vol. 24, 1999, pp. 81-91.

[4] A.P. Kosoresow, G.E Kaiser, "Using agents to enable collaborative work", IEEE Internet Computing, Vol. 2, No. 4, July-Aug. 1998, pp. 85-87.

[5] M. Breugst, L. Hagen, and T. Magedanz, "Impacts of Mobile Agent Technology on Mobile Communications System Evolution", IEEE Personal Communications, vol. 5, no. 4, (1998), pp. 56-69.

[6] Korba, L. Issues in Agent-Based Electronic Commerce. Proc. of the SSGRR 2000: International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet, l'Aquila, Rome, July 31-August 6, 2000.

[7] Truste seal web site, http://www.truste.org

[8] R. Oppliger, "Privacy Protection and Anonymity Services for the World Wide Web", Future Generation Computer Systems Journal, Vol. 16, Issue 4, February, 2000, pp. 379-391.

[9] American Express Private payments http://www.americanexpress.com/privatepayments/info_page.jsp

[10] J.A. Harvey, K.A. Verska, What the Euorpean Data Privacy Obligations mean for U.S. Businesses. Gigalaw.com, http://www.gigalaw.com/articles/2001/harvey-2001-02-p1.html

[11] W. Jansen, "Countermeasures for Mobile Agent Security", Computer Communications, Special Issue on Advances of Network Security, Elsevier Science BV, Summer, 2000, 14 p., http://www.itl.nist.gov/div893/staff/jansen/wjhome.html

[12] M. Sloman, "Policy driven management for distributed systems", J. Network and Systems Management, vol. 2, no. 4, pp. 333-360, Plenum Press, 1994.

[13] M. Blaze, J. Feigenbaum, J. Lacy. Decentralized Trust Management, Proc. of the 17th Symposium on Security and Privacy, pp. 164-173. IEEE Computer Society Press, Los Alamitos, 1996.

[14] S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilley & Associates, 2001.

[15] P.J. Marques, L.M. Silva, J.G. Silva, J.G. Silva, Security Mechanisms using Mobile Agents in Electronic Commerce, Proc. of the 18th IEEE Symposium on Reliable Distributed Systems, Oct 19-22, 1999, pp. 378-383.

[16] S.N. Foley, J. Jacob, Specifying security for CSCW systems, Proc. 8th IEEE Computer Security Foundations Workshop, June 13-15, 1995, pp. 136-145.

[17] H.S. Nwana, J. Rosenschein, T. Sandholm, C. Sierra, P. Maes, R. Guttman, Agent-mediated electronic commerce: issues, challenges and some viewpoints, Proc. of the 2nd Int. Conf. on Autonomous Agents, May 10-13, 1998, pp. 189-196.

[18] Links to other agent tools collected by AgentBuilder. http://www.agentbuilder.com/AgentTools/

[19] P. Bellavista, A. Corradi, C. Stefanelli, A secure and open mobile agent programming environment, Proc. 4th Int. Symp. On Autonomous Decentralized Systems, March 21-23, 1999, pp. 238-245.

[20] Mitsubishi Concordia Agents Information Page, http://www.meitca.com/HSL/Projects/Concordia/Welcome.html

[21] V. Prevelakis, J-H. Morin. And D. Konstantas, Controlling the dissemination of electronic documents, Proc. Tenth Int. Workshop on Database and Expert Systems Applications, Sept. 1-3, 1999, pp. 869-873.

[22] J.J. Jung, D.Y. Hwang, and S.B. Jeon, Agents-based framework for brokerage between buyers and sellers on electronic commerce, Proc. Int. Conf. on Electronic Commerce, 1998, pp. 17-22.

[23] H.S. Yoon and J.K. Lee, Intelligent agents based virtually-defaultless check system: safecheck system, Proc. Int. Conf. on Electronic Commerce, 1998, pp. 224-231.

[24] J.K. Lee, and W. Lee, Intelligent Agent Based Contract Process in Electronic Commerce: UNIK-AGENT Approach, Proc. 30th Hawaii Int. Conf. on System Science, 1997, pp. 230-241.

[25] M. Barbuceanu, M.S. Fox, Coordinating multiple agents in the supply chain, Proc. of the 5th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1996, June 19-21, 1996, pp. 134-141.

[26] J. Dong, J.C. Zheng, S.Y. Xiao, Software Models in CSCW, Proc. IEEE Int. Conf. on Intelligent Processing Systems, Oct. 28-31, 1997, pp. 881-885.

[27] L. Hongchen, S. Meilin, Application of agents in workflow management system, APCC/OECC '99 5th Asia-Pacific conference on Communications & 4th Optoelectronics and Communications Conf., Oct. 18-22, 1999, pp. 1068-1072.

[28] Platform for Privacy Preferences http://www.w3c.org/p3p

[29] J. Reagle and L. F. Cranor, "The platform for privacy preferences", Communications of the ACM, Vol. 42, No. 2, 1999, pp. 48-55 .

[30] Privacy Server Protocol http://yuan.ecom.cmu.edu/psp/

[31] Privacy Incorporated Software Agent (PISA) Project, http://pet-pisa.openspace.nl/

[32] Weiming Shen, Sherman Lang, Larry Korba, Lihui Wang and Brian Wong, Reference Architecture for Internet Based Intelligent Shop Floors, Network Intelligence: Internet-Based Manufacturing, Proceedings of SPIE Vol. 4208, pp. 63-71 (2000).

[33] B. Schneier, J. Kelsey, "Secure audit logs to support computer forensics", ACM Trans. on Information and System Security, Vol. 2, No. 2, 1999, pp. 159-176.

[34] P3P Preference Exchange Language (Appel) http://www.w3.org/TR/P3P-preferences.html