Knowl Inf Syst
DOI 10.1007/s10115-011-0415-3

REGULAR PAPER

Knowledge-empowered agent information system for privacy payoff in eCommerce

Abdulsalam Yassine · Ali Asghar Nazari Shirehjini · Shervin Shirmohammadi · Thomas T. Tran

Received: 9 September 2010 / Revised: 3 March 2011 / Accepted: 10 May 2011

Abstract Today, many online companies are gathering information and assembling sophisticated databases that know a great deal of information about many people, generally without the knowledge of those people. Such endeavor has resulted in the unprecedented attrition of individual's right to informational self-determination. On the one hand, Consumers are powerless to prevent the unauthorized dissemination of their personal information, and on the other, they are excluded from its profitable commercial exchange. This paper focuses on developing knowledge-empowered agent information system for privacy payoff as a means of rewarding consumers for sharing their personal information with online businesses. The design of this system is driven by the following argument: if consumers' personal information is a valuable asset, should they not be entitled to benefit from their asset as well? The proposed information system is a multi-agent system where several agents employ various knowledge and requirements for personal information valuation and interaction capabilities that most users cannot do on their own. The agents in the information system bear the responsibility of working on behalf of consumers to categorize their personal data objects, report to consumers on online businesses' trust and reputation, determine the value of their compensation using risk-based financial models, and finally negotiate for a payoff value in return for the dissemination of users' information. The details of the system as well as a proof-of-concept implementation using JADE (Java Agent Development Environment) are presented here.

Keywords Knowledge · Information system · Agents · Privacy · eCommerce

A. Yassine (✉) · A. A. N. Shirehjini · S. Shirmohammadi · T. T. Tran
Distributed and Collaborative Virtual Environments Research Laboratory, School of Information Technology and Engineering SITE, University of Ottawa, Ottawa, ON, Canada
e-mail: ayassine@discover.uottawa.ca

A. A. N. Shirehjini
e-mail: anazari@discover.uottawa.ca

S. Shirmohammadi
e-mail: shervin@discover.uottawa.ca

T. T. Tran
e-mail: ttran@site.uottawa.ca

Published online: 28 May 2011

1 Introduction

Today, many online companies are gathering information and assembling sophisticated databases that know a great deal of information about many people, generally without the knowledge of those people [6,34]. Such information then changes hands or ownership as part of normal e-commerce transactions or during a firm's strategic decisions, which often include selling consumers' personal information lists to other firms [34]. With the increasing economic importance of services based on the processing of personal data, it is clear that firms, especially online service providers,[1] have high incentives to acquire consumers' personal information [47]. A look at present-day practices reveals that consumers' profile data are now considered one of the most valuable assets owned by online businesses [6,47]. As a result, a flourishing market in the sale of personal information has been created [46,47]. Although private data are not traded separately, but when aggregated together, the tiniest nuggets of personal information have value [34,47,13]. This paper presents a knowledge-empowered agent information system architecture that helps tip the balance of power in favor of consumers.

The argument presented in this paper is as follows: if consumers' personal information is a valuable market asset, should they not be entitled to benefit from their asset as well? Given such argument, a natural question comes to mind is: will online businesses buy into it? From a pure economical perspective, online businesses are expected to benefit from such models as well. Since attention in the information market is one of the main reasons, if not the most important reason, behind the collection of personal information, it is essential for online businesses to find ways to economize on attention [47]. In other words, online businesses essentially incur excess costs (junk mail, junk phone calls, junk email etc.) to attract consumers' attention to their products and services. However, if they know precisely what the consumer wants, they could make a much better decision about whether or not to provide the consumer with information about their services.

The scope of this paper is on developing knowledge-empowered agent information system architecture for privacy payoff as a means of rewarding consumers for sharing their personal information. Software agents are becoming a choice technology for carrying out complex tasks that many users cannot do on their own [36]. The proposed system, described in Sect. 3, consists of several agents that incorporate necessary knowledge to maximize the consumers' benefit. The agents in the knowledge-empowered information system bear the responsibility of working on behalf of consumers to categorize their personal data objects, report to consumers on online businesses' trust and reputation, determine the value of their compensation using known financial models, and finally negotiate for a payoff value in return for the dissemination of users' information. The viability of the system is demonstrated through detailed analysis and a prototype implementation, which is based on the JADE multi-agent framework.

To the best of our knowledge, no other work has considered employing software agents in information system architecture for privacy payoff as a means of rewarding consumers for sharing their personal information in e-commerce similar to our work. Contributions made in this work are as follows:

- We propose a knowledge-empowered agent information system for privacy payoff. This is a rather significant and somewhat complex multi-agent information system that, in the end, makes the user's life easy when dealing with privacy payoff negotiation;

[1] Throughout the paper, online service provider and online business are used interchangeably.

- We propose a new technique to valuate private data based on privacy risks and use fuzzy logic in the agents for determining the trustworthiness of online businesses;
- We extend existing trust models by introducing a new layer of assessment based on privacy credentials, thus advancing the state of the art in this aspect as well;
- We extend an agent-based negotiation protocol presented by [45] for the goal of maximizing the consumers' benefit;

The remainder of this paper is organized as follows: in the next section, we discuss the related work. In Sect. 3, the proposed system architecture is presented followed by proof-of-concept implementation in Sect. 4. In Sect. 5, we discuss our work. Finally, in Sect. 6, we conclude the paper and present plans for future work.

2 Related works

This section presents work related to agent-based eCommerce information systems and privacy systems in eCommerce. In particular, we examine a sample of such studies that we believe to be representative and specifically related to the work in our topic. Although far from being exhaustive, this section gives a rather complete idea of the current state of the art.

2.1 Agent-based eCommerce information systems

The rich content and the dynamic nature of eCommerce have made shopping activity a process that requires large effort. A human buyer, for example, requires collecting and interpreting information on merchants, products, and services reviews, making optimal decisions, and finally entering appropriate purchase and payment information. The large amount of available information is overwhelming for individual consumers [58]. Developing actionable trading agents help automate a variety of activities, mostly time-consuming ones, and thus lower the transaction costs. An example of such work is presented by [5]. The study uses agents that can produce optimal trading strategies to be directly used by users to take decision-making actions in eCommerce situations. Other examples of agent-based systems that are extensively studied in eCommerce are negotiation systems. [59] propose a knowledge-based system for automated negotiation in eCommerce. In such a system, the authors emphasize the utilization of knowledge originated from historical negotiation data in estimating and fine-tuning the negotiation parameters, for improving the performance of automated negotiation.

Other forms of agent-based information systems apply the concept of consumer-driven eCommerce societies, such as the work of [42], which proposes a multi-agent system of consumers that represent their service needs semantically using ontologies. The aim of the system is to allow consumer agents to create new service descriptions and share them with other consumer agents thus creating an eCommerce society of consumers. According to the authors, such a system leads to better offerings from service providers as they compete among each other to provide attractive promotions and target service consumers more effectively.

While our system employs agents to automate activities similar to the above-mentioned work, it tackles a rather unique problem in eCommerce (privacy payoff), which is novel and has not been addressed by any previous work. Each agent in our system autonomously assumes a specific activity such as consumers' personal data categorization, trust and reputation, payoff computation, and negotiation. Furthermore, our study, like [42] study, uses agents that utilize attribute ontologies to aggregate consumers' information records

according to a specific interest thus forming a community of eCommerce consumers. The formation of such a community is beneficial for an individual consumer, because the agent negotiating on behalf of a consumers' community would be in a better position to bargain over the revelation of their personal information and get something of value in return.

To give a better understanding of our work, we also need to describe some of the existing work in privacy systems for eCommerce, although they are not agent based. This is shown next.

2.2 Privacy systems in eCommerce

Since the release of the Platform for Privacy Preferences (P3P) by the World Wide Web Consortium (W3C), several studies were conducted to integrate legal requirements into the mechanism of data revelation such as the work in [12] and [27]. Both studies focus on the definition of privacy policies and their enforcement on user's private data in eCommerce.

Other studies such as the work of [29] propose Privacy Integration Queries (PIQ), which claims to have the strongest unconditional privacy guarantees: differential privacy. The privacy guarantees require no privacy sophistication on the part of the platform's users. The aim of PIQ is to increase trust even for analyst and providers with no privacy expertise.

In terms of personal information valuation as a topic, [24] explored the economics of privacy in eCommerce personalization systems, where people can opt to share personal information in return for enhancements in the quality of an online service. Before [24], many other studies in the literature discuss similar systems [1,44]: from incomplete information about privacy threats and defenses to bounded ability to deal with their complex trade-offs and from low (and decreasing) privacy sensitivities to behavioral phenomena, such as immediate gratification.

The work of [26] and [33] is somehow close to ours. They present mechanisms that allow users to potentially benefit from sharing private data. [33] presents a system based on negotiating privacy versus rewards. The system does not, however, consider the value of private data in question, and therefore, the online business has the upper hand in the negotiation process. [26] proposes the National Information Accounts, a market-based negotiation system, in which information about individuals is traded at a market-clearing price to the level where supply satisfies demand. This model, although interesting and ingenious, does not suit the multiple possibilities to collect, store, and process information in a networked society, centered around the Internet, as a global, unregulated communication channel.

3 System architecture

In this section, the proposed information system architecture is presented. A high-level view is described in the next Sect. 3.1, followed by detailed descriptions of each agent in the system; specifically, information agent in 3.2, trust and reputation agent in 3.3, payoff agent in 3.4, and negotiation agent in 3.5.

In our previous study [50–53], we introduced analysis related to the information agent (3.2) and the payoff agent (3.4); however, to present a self-contained article, we are re-presenting them here as well with extensions that are related to the information system design as we are going to see in the next few subsections.

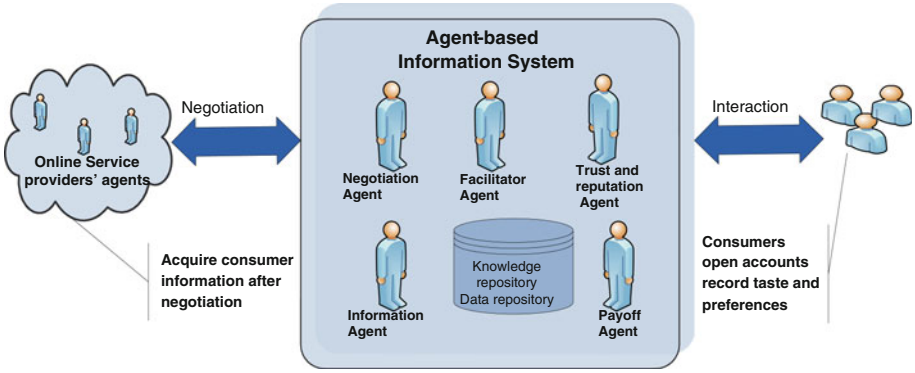

Fig. 1 High-level architecture of the proposed system

3.1 High-level view

Figure 1 depicts the high-level architecture of the proposed system. Consumers open their accounts in the system and record their taste and preferences, while online service providers negotiate, through their engaged agents, with the system to acquire the data.

The agents in the system take on the responsibility of helping consumers valuate their personal data objects that are perceived to be valuable, to capitalize on them for the goal of maximizing their market value once the consumer decides to reveal them. To explain how the system works, consider the following scenario: Alice is a privacy pragmatic person. According to [43], privacy pragmatic person is defined as a person who is sensitive to data profiling but generally is willing to provide data. Alice is willing to share her personal data preferences with certain online service providers for a discount value or a reward fee. But Alice has certain requirements before she consents to complete the transaction:

(1) She wants complete information about the service provider's privacy practices and its trustworthiness
(2) She wants to determine the level of risk involved in the transaction based on information from (1)
(3) She wants the system to valuate her data combination risk based on her perceived risk of each private data object
(4) She wants her reward or discount value to be valuated based on the involved risk from (3)
(5) She wants the party that negotiates on her behalf to be strategic during the negotiation process so she can get the maximum benefit
(6) She wants to have the privilege of accepting or denying the final offer

To satisfy Alice's requirements, the system employs several agents where each one performs a specific task. The order of task execution is captured in the interaction diagram shown in Fig. 2.

(1) Alice opens her account that records her taste, preferences, and personal data (essentially a detailed subscription form that needs to be filled once, but can be updated as desired, an example of such a form is provided in Sect. 4). Her information is stored in the data repository. The information agent automatically classifies the data into different categories, such as contact data, personal ID data, and hobby data (explained later in

Sect. 3.2). The decision about data categorization is performed based on ontological formulation.

(2) When the service provider submits a request to obtain personal data (for example, data about consumers who like sports), the trust and reputation agent assesses the trustworthiness of the service provider. The trust and reputation agent employs fuzzy logic techniques (details of this technique are discussed in Sect. 3.3) to rate the privacy credentials of the online business. Privacy credentials (such as privacy seal, membership to privacy auditing services, security seals, authentication mechanisms, and contents of privacy statement) are attributes that can be thought of as the means by which one can judge the competency of the online business with respect to privacy and private data protection (thus satisfying Alice's requirement 1)

(3) The trustworthiness rating is communicated back to Alice so she can make an informed decision when assigning the level of privacy risk to the categories of her private data objects (thus satisfying Alice's requirement 2).

(4) After Alice assigns her privacy risk weights to her private data objects, the information agent computes the total privacy risk value for each consumer as well as the combination risk (thus satisfying Alice's requirement 3).

(5) The payoff agent uses the quantified privacy risk value to compute the payoff that Alice should receive. The payoff or the compensation is seen as a risk premium valuated in response to the amount of potential damages that might occur (cost of risk) with respect to the risk exposure (thus satisfying Alice's requirement 4). The payoff agent uses a computational model similar to the models used by the financial and insurance institutions (explained in Sect. 3.4).

(6) Once the payoff is determined, the negotiation agent negotiates with the online business on Alice's behalf. The intelligence of the negotiation agent is realized by the negotiation strategy, i.e., the strategy of making concessions and evaluating the incoming offers and making decisions to interact with the negotiation opponent (thus satisfying Alice's requirements 5). The outcome of the negotiation is communicated with Alice. Alice either accepts the offer if it is equal or greater than the expected payoff and in this case shares her data with the online business or denies the offer and in this case her personal data will not be shared with the online business (thus satisfying Alice's requirements 6).

The order of task execution described above is coordinated by the facilitator agent as seen in Fig. 2. The facilitator agent is equipped with knowledge management capabilities. The workspace of the facilitator agent consists of a knowledge repository that keeps the general knowledge of interaction between the agents.

In the proposed system, we assume that there is some forms of enforcement mechanisms that make consumers feel safe when using the system. In reality, there are multiple security solutions that can be easily integrated within the proposed system although this is beyond the scope of our work. Examples of such mechanisms are: the use of digital certifications where data stored in the system are encrypted with private and public keys. The entity that runs the system would not be able to use the data unless a certification of authentication is provided by a Trusted Third Party such as Comodo's Certification Authority (CA). The reader may refer to [32] for more details on such mechanisms. Another possible way is the use of k-means clustering where data can be retrieved with a cryptographic protocol while preserving privacy [38]. Mechanisms of hiding sensitive information in large databases such as the work proposed by [15] and [22] are also another ways of privacy preservation and hacking prevention.

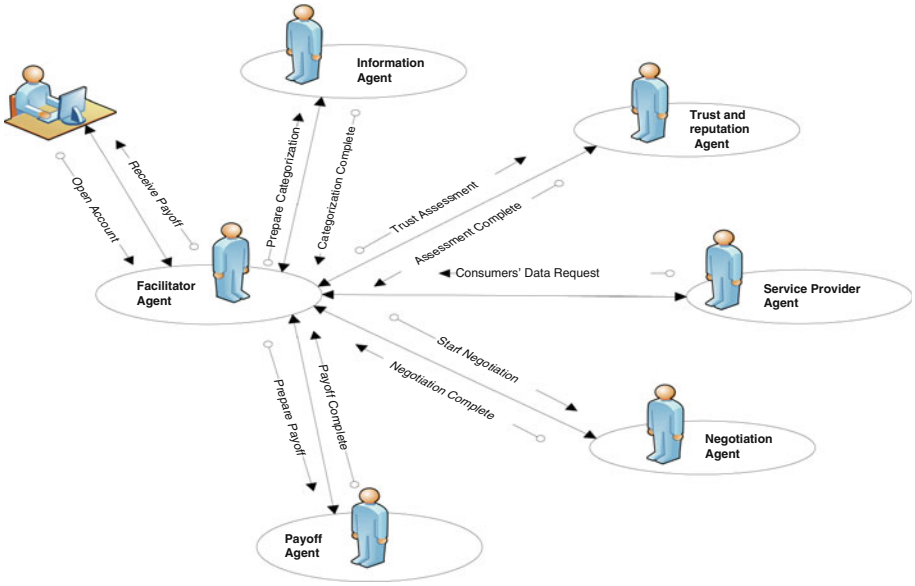

Fig. 2 Interaction diagram of the proposed system

3.2 Information agent

This subsection describes the components of the information agent and their details. In particular, we discuss the attribute ontology used in the process of personal data categorization and the computational process of privacy risk quantification.

3.2.1 Attribute ontology

Any operation that involves private data may be viewed as a process that may potentially result in privacy risk depending on the sensitivity level of the private attributes involved in the operation. The information agent categorizes the private data in a way that captures two important characteristics, namely, semantic equivalency and substitution rate given in the following definitions:

Semantic equivalency: Consider two transactions that expect as their input a person's home phone number and the same person's family name. One transaction describes the parameters: PhoneNumber and FamilyName, while the second transaction describes the parameters: PhoneNumber and LastName. From a privacy perspective, both transactions are equivalent. This is due to the semantic equivalence of FamilyName and LastName. To capture this equivalency among attributes, the agent uses ontology sets of semantically defined attributes. The following are examples of such sets:

Set 1 = {FamilyName, LastName, Surname}
Set 2 = {Address, HomeAddress, Location}

Substitution rate: The substitution rate of private data captures the level of risk in relation to private data revelation. Private data attributes that are considered substitutable have a constant substitution rate, i.e., the level of exposure risk stays the same. On the other hand,

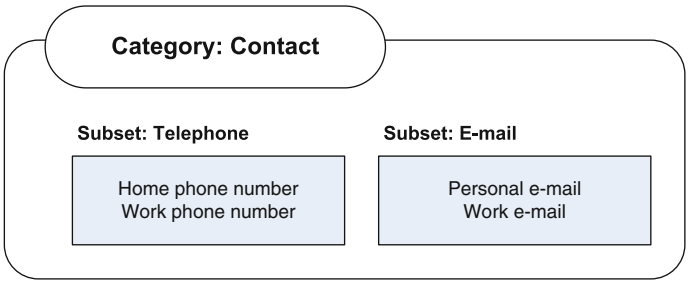

Fig. 3 Example of private data categorization

private data attributes that are not substitutable may result in an increase in the privacy risk. Substitution rate is explained next when we describe data classification.

3.2.2 Data classification

The agent receives data specification from consumers, which reflects their true personal information and then classifies them into M different categories $(C_1, C_2, \ldots, C_M)$, such as personal identification, contact information, address, hobbies, and tastes. In every category C_i, private data are further divided into subsets, that is $C_i = \{S_{ik} \text{ for } k = 1, 2, \ldots\}$ based on the attribute ontology that applies to the data set, an example is shown in Fig. 3.

In Fig. 3, we consider category Contact, which is divided into two subsets, Telephone and E-mail. The information agent uses the attribute ontology to reason about the classification of the data as follows: first, data in different categories may have different context-dependent weights. The value of the private data may differ from one context to another (personal data value in context sports and personal data value in context health); therefore, its composition may have different implications on the level of revelation.

Second, the substitution rate of private data in the same subset is constant and independent from the current level of revealed data, i.e., assuming that one of the private data has been revealed, revealing the rest of the data in the same subset will not increase the privacy disclosure risk. For instance, a consumer's contact information can be expressed by work phone number or home phone number. Knowing both of them at the same time allows only marginal improvements. This will allow considering each private data subset as one unit.

Third, data in different subsets are not substitutable, revealing any one of them will increase the privacy risk. For example, the consumer's telephone number and her email address constitute two possible ways to contact the consumer but they are not completely interchangeable.

3.2.3 Risk quantification

After the agent classifies the personal data into different categories, as explained in the previous subsection, the agent now computes the disclosure privacy risk of private data. But first, it needs to capture the consumers' preferences about revealing different attributes of personal data for each category i under context j. The context here refers to the situation and the nature of the private data involved in the situation. Individual's privacy cost valuation (cost resulting from privacy risk) differs from one type of information to another. We use the parameter $\beta_{ij} \in [0, 1]$ to capture the privacy risk of each private data in category i under context j. β_{ij} represents the consumer's valuation of her private data under each context

(we will explain how the consumer will specify this value in Sect. 4). Each consumer is assumed to be stochastically equivalent and has independent distributed valuation for each context. According to [33] and [54], individuals have various global valuation levels for each transaction that involves private data. Also users' potential privacy risk depends on their information disclosure behavior [28].

Let us consider a consumer with identity I and several private data attributes $\Lambda = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_n\}$. We let the privacy risk to vary with Λ and β according to the functional form $\Psi(\Lambda, \beta)$, where $\Psi(\Lambda, \beta)$ characterizes the magnitude of privacy risk resulting from the composition of different private data attributes Λ and the cost β (privacy risk cost) of revealing them. The calculation of $\Psi(\Lambda, \beta)$ is as follows (from now on, and for the sake of clarity, we will drop the symbols Λ and β):

Let Xi be the cardinality of Ci (i.e., $Xi = |Ci|$). We perform normalization over the whole private data set. The normalized data size NXi reflects the ratio of each category in a consumer's privacy.

$$NX_i = \frac{X_i}{\sum_{k=1}^{M} X_k} \tag{1}$$

where M is the number of the private data categories.

After the consumer assigns the value β_{ij} for each category i under context j, the agent computes the weighted privacy risk, as in (2), and then normalizes it, as in (3). The value $N\Psi_{ij}$ in (3) reflects the risk of revealing all data in category i under context j. The purpose of this normalization is to put the privacy risk of each category into the range of [0,1].

$$\Psi_{ij} = NX_i * \beta_{ij} \tag{2}$$

$$N\Psi_{ij} = \frac{\Psi_{ij}}{\sum_{n=1}^{i} \Psi_{nj}} \tag{3}$$

The privacy risk weight of revealing α_i subsets from category i is calculated as in (4).

$$\Psi_i = \frac{\alpha_i}{X_i} * N\Psi_{ij} \tag{4}$$

Next, we present the details of the trust and reputation agent.

3.3 Trust and reputation agent

As mentioned earlier in Sect. 3, in order for Alice to assign privacy risk weights to her private data objects, she wants to know the reputation and the competency of the online business with respect to privacy and private data handling. To understand how the service provider is going to handle the personal information, it is essential to assess its trustworthiness based on privacy credential attributes, which the online provider has obtained (e.g., trustmark seals, privacy certificates, contents of the privacy statement, encryption mechanisms). Empirical research on the impact of such attributes on individuals' perceived trust, e.g., that of [35,39], to name few, report that the impact varies depending on the type of the attribute. Examples of such attributes are shown in Table 1.

In this paper, the rating of each attribute as shown in Table 1 under column "Significance" is based on studies on consumer research analysis such as those of [8,16,25,39] and industry studies such as those of [10,21]. These studies analyze the impact of different trusting attributes on consumers' online purchasing behavior and their perceived trust. For example, in [39,16], the "use of encryption mechanism" and "periodic reporting on privacy matters" have low impact on the perceived trust according to consumer research analysis.

Table 1 Examples of trusting attributes and their significance

Credential	Type	Significance
Trustmark seals	e.g., Reliability Seals, Security Seals, Vulnerability Seals, Privacy Seals	Varies depending on the type of the seal and the issuing party [39,57]
Dispute resolution	Independent resolution mechanisms, e.g., American Arbitration Association	Medium [8]
Membership to privacy compliance auditing service	e.g., Pricewaterhousecooper, PrivaTech	High [10,31]
Privacy statement	Privacy policy generator, e.g., Organization for Economics Cooperation and Development OECD	Varies depending on the contents [30]
Authentication-based disclosure of information	e.g., Kerberos-based vs. username/password authentication	Low [39]
Periodic reporting on privacy matters	e.g., reports on privacy training, reports on privacy compliances	Low [39]
Allows consumers to opt out	Opt out of data-sharing and marketing solicitations	High [16]
Use of encryption mechanisms	e.g., 128-bit is better than 64-bit encryption scheme	Low [39,16]

The attributes and their classifications are stored in a database dedicated for the privacy credential ratings. The trust and reputation agent uses a fuzzy logic mechanism (discussed in the next subsection) to determine the privacy credential score and the privacy report for each service provider (implementation of such report is shown in Sect. 4).

3.3.1 Fuzzy logic-based rating

Privacy attributes can be thought of as the means by which one can judge if the online business is trustworthy to handle the consumers' private data. As shown in Table 1, attributes differ in their impact according to their significance (low, medium, and high).

Let us assume that ζ_k is the set of K attributes, written as follows:$\zeta_k = \{\zeta_1, \zeta_2, \zeta_3, \ldots, \zeta_K\}$; k = 1, . . ., K. As mentioned earlier, each attribute has its own impact on the perceived trust as shown in Table 1. The set ζ_k is classified into three subsetsζ_f^h, ζ_g^m, and ζ_w^l of high, medium, and low credentials, respectively, such that $\zeta_f^h \cup \zeta_g^h \cup \zeta_w^l = \zeta_k$. Subsets ζ_f^h, ζ_g^m, and ζ_w^l will be used as reference sets against which the online business will be measured. In reality, the service provider may have obtained different types of attributes, each of which has a different impact on the perceived trust. We introduce here a factor, called Online Provider Reliability Φ, which helps determine the competency of the online business with respect to privacy and private data handling. The competency is an indication to what extent the service provider can be trustworthy to respect consumer's private data and adhere to the best practices of respecting consumers' privacy. Let φ be the set of credential attributes that the online business has. In reality, φ would include attributes of different types, i.e., high, medium, and low (e.g., [39,8,57]). According to [39,23,18], and [25], the higher the number of credential attributes, the more reliable is the online provider to protect consumers' personal data. However, as mentioned earlier, the service provider may have obtained different types of attributes. Therefore, its reliability Φ is based on such combination. We denote by Θ to represent the combination of X, Y, and Z, then we determine the online service provider's reliability Φ as follows:

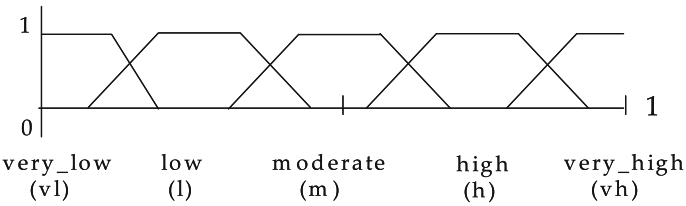

Fig. 4 Fuzzy sets for variable Φ

$\Phi = \mathrm{X}\Theta\mathrm{Y}\Theta\mathrm{Z}$, such that $X \leq \left|\zeta_f^h\right|$, $Y \leq \left|\zeta_g^m\right|$, and $Z \leq \left|\zeta_w^l\right|$, where $\left|\zeta_f^h\right|$, $\left|\zeta_g^m\right|$, and $\left|\zeta_w^l\right|$ are the cardinalities of sets ζ_f^h, ζ_g^m, and ζ_w^l, respectively.

An important facet of the above combination is the rules that determine how the value of Φ will be determined. This is because the weights of the attributes in the combination are often set by using linguistic variables [39,40,8], such as "I believe that if the service provider provides a readable, easy-to-understand privacy statement, then my trust in his intentions is high." Setting a label of HIGH may be interpreted to represent more than one numerical value. The reason for that is the vagueness of human perception. To avoid assigning a specific numeric value to this rather subjective concept, we follow the work of [56,40] and use fuzzy rules where we can subdivide a range [0,1] into a number of linguistic labels such as VeryLow, Low, Moderate, High, and VeryHigh. Not to mention that the valuation of the acceptance of the service provider's reliability value (from human perspective) is too complicated by using conventional mathematical methodologies [40]. Fuzzy logic helps us determine the final linguistic label that is translated into a single crisp value, which could be a numeric scale if needed. In our case, the final linguistic label is translated into a scale composed of five "Stars" such that one star is VeryLow, two stars is Low, and so on and so forth. Using fuzzy logic, the reliability of the online business is determined as shown in Fig. 4.

Figure 4 shows the fuzzy sets for the variable Φ. The complete set of inference rules that map the inputs to the output is as follows:

IF Φ is very high, THEN privacy risk is low,
IF Φ is high, THEN privacy risk is low
IF Φ is moderate, THEN privacy risk is moderate
IF Φ is low, THEN privacy risk is high
IF Φ is very low, THEN privacy risk is very high

The heuristic behind the above rules is that online businesses that show a high degree of competency to protect consumers' data are assumed to honor their promises and can be trusted. Table 2 shows a possible set of rules, which the mechanism uses to determine the reliability Φ. In Table 2, *vh, h, m, l,* and *vl* stands for *very high, high, medium, low* and *very low*, respectively. Note that the rules presented in Table 2 tend to ensure the minimum credentials to determine the value of the variable Φ.

3.4 Payoff agent

In this section, we present the details of the payoff agent. The payoff agent computes the reward value that the consumer should receive as a result of revealing their personal information. The payoff is computed in response to the amount of potential damages that might occur (cost of risk) with respect to the risk exposure. The payoff, which can be seen as a risk-base premium or compensation, is the worldwide practice of the financial institutions

Table 2 Example of reliability rules

Rules
$\text{IF}\left(X \geq \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \geq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \geq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ vh$
$\text{IF}\left(X \geq \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \geq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \leq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ vh$
$\text{IF}\left(X \geq \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \leq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \geq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ h$
$\text{IF}\left(X \geq \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \leq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \leq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ h$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \geq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \geq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ m$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \geq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \leq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ m$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \leq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \geq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ m$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y \leq \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \leq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ l$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y < \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \geq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ l$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y < \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z \leq \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ \ is\ vl$
$\text{IF}\left(X < \frac{\left\lvert\zeta_f^h\right\rvert}{2}, Y < \frac{\left\lvert\zeta_g^m\right\rvert}{2}, Z < \frac{\left\lvert\zeta_w^l\right\rvert}{2}\right)\text{THEN}\Phi\ is\ vl$

and the insurance industry and is implied in many other industries [2]. The basic idea is that those who are considered more risky should pay more interest. This means that risk-based premium is a quantified value applied to compensate for unwanted events that might lead to revenue loss or increased cost. Privacy risk is the business risk resulting from the use and mishandling of personal information. Like all business risk, privacy risk could result in financial hardship [6,26].

Previously, in Sect. 3.2.3, we showed how the information agent determines the privacy risk value $\Psi(\Lambda, \beta)$ that the consumer expects when revealing his or her personal information. The payoff agent's responsibility is to determine the payoff value that the consumer should receive given the privacy risks that are involved. Intuitively, we want to associate high benefit/compensation with $\Psi(\Lambda, \beta)$ that allow high identification of I (the identity of the consumer) given Λ and high risk β. One approach for determining this value is to construct a risk premium that is valuated in response to the amount of potential damages that might occur (cost of risk) with respect to the risk exposure. In this manner, the compensation paid to the consumer is justified, at least in part, from the damages that might occur. This approach will help make service providers more conservative when handling users' personal information. This is because privacy risk penalties and reputation consequences on the violators of users' presumed privacy rights are more likely to be costly. This approach is widely used in the financial and auto insurance industry [11].

Theoretically, the expected payoff of a risky asset in conjunction with expectations of the risk-free return should be used to construct the risk premium [11]. The basic idea is that those who are considered more risky should pay more interest. The standard model [11] is:

$$\text{Expected return} = \text{RiskfreeRate} + \text{AssetRisk} \cdot \text{Market Risk premium} \tag{5}$$

where:
Expected return is the payoff given to the consumer against revealing their private data (i.e., their asset);
RiskfreeRate is the expected return value at zero risk;
Market Risk premium is the expected market risk and it is positive; and
AssetRisk is the calculated risk of the private data (i.e., Ψ calculated from Sect. 4.3).

Assuming that the RiskfreeRate is zero (this assumption is valid since consumers do not expect to be compensated for private data if the level of risk is zero), this model requires two inputs. The first is the risk value of the private data asset being analyzed, and the second is the appropriate market risk premium(s). Equation (5) is now formally written as follows:

$$E\left(U_q\right) = \Psi_q \cdot E\left(\Re\right) \tag{6}$$

where:
E (Uq) is the expected return U of revealing private data q;
$E(\Re)$ is the expected market risk premium; and
Ψ_q is the calculated privacy risk of revealing private data q.

Equation (6) is simply saying that consumers' demand for revealing their personal information is measured based on the perceived risk and the market risk premium. The market risk premium is a monetary value estimated by looking at historical premiums over long time periods [11]. According to [9] and [2], the general behavior of market risk premiums follows a random variable, random walk, or autoregressive process over time. Here, we assume that the risk premium follows a random process and fluctuates over time following a geometric Brownian motion, where the expected risk-premium value will be the underlying mean. The geometric Brownian motion assumption has the advantage that the process depends only on two variables, the drift and the standard deviation. The distribution function of a geometric Brownian motion is lognormal, which has the favorable property that negative future values have zero probability. A stochastic (random) process $\Re$ is said to follow a geometric Brownian motion if it satisfies the following stochastic differential equation [37]:

$$\mathrm{d}\Re_t = \mu\Re_t \mathrm{d}t + \sigma\Re_t \mathrm{d}W_t \tag{7}$$

Where $\{W_t\}$ is a Wiener process or Brownian motion, μ is the drift, and σ is the standard deviation. Using Ito's lemma [37], we can derive the analytical solution of equation (7) as follows:

$$\mathrm{d}\ \ln\ \Re\left(t\right) = \frac{1}{\Re\left(t\right)}\mathrm{d}\Re\left(t\right) - \frac{1}{2}\frac{1}{\Re\left(t\right)^2}\mathrm{d}\Re\left(t\right)^2 \tag{8}$$

$$= \frac{1}{\Re\left(t\right)}\Re\left(t\right)\left[\mu\mathrm{d}t + \sigma\mathrm{d}W\left(t\right)\right] - \frac{1}{2}\frac{1}{\Re\left(t\right)^2}\Re\left(t\right)^2\left[\sigma^2\mathrm{d}W\left(t\right)^2\right] \tag{9}$$

$$= \mu\mathrm{d}t + \sigma\mathrm{d}W\left(t\right) - \frac{1}{2}\sigma^2\mathrm{d}t \tag{10}$$

The integral of (10) from 0 to t is:

$$\int_0^t \mathrm{d} \ln \Re(t) = \int_0^t \left(\mu \mathrm{d}t + \sigma \mathrm{d}W(t) - \frac{1}{2}\sigma^2 \mathrm{d}t \right) \tag{11}$$

$$\ln \Re(t) - \ln \Re(0) = \left(\mu - \frac{1}{2}\sigma^2 \right) t + \sigma W(t) \tag{12}$$

Basic calculus gives us:

$$\Re(t) = \Re_o e^{\left((\mu - \sigma^2/2)t + \sigma W t\right)} \tag{13}$$

where $\Re_o$ is the risk-premium value at time t = 0, i.e., it is the initial risk-premium value.

We now take the expectation $E[\Re_t]$ for (13):

$$E[\Re_t] = E\left[\Re_o e^{\left((\mu - \sigma^2/2)t + \sigma W_t\right)} \right] \tag{14}$$

Applying the law of normal variables with mean μ and variance σ^2 knowing that the Brownian motion, we get:

$$E[\Re_t] = \Re_o e^{\mu t} \tag{15}$$

The risk premium is assumed to be known at time 0. Some studies such as [17] estimate the market privacy risk premium to be between $45 and $57 per personal data record. Equation (15) estimates the value of the payoff as it varies over time.

Next, we provide the details of the negotiation agent.

3.5 Negotiation agent

It is a daunting prospect for an individual consumer to bargain with a huge service provider about a desired payoff against revealing personal information. Therefore, having an agent working on behalf of a group of consumers would be in a better position to bargain over the revelation of their personal information and get something of value in return. To set the stage for specifying the negotiation model, some rules and assumptions are given as follows:

- Since a bargaining negotiation is fundamentally time-dependent [4], we assume that both the agent representing consumers and the service provider agent utilize a time-dependent strategy while making a concession. This assumption is an appealing one since human traders easily understand deadlines, and it is trivially simple to specify a deadline to a software agent. Thus, the consumers' agent has a deadline T^{CA}_{deadline}, and the service provider agent has a deadline T^{SP}_{deadline}.
- The negotiation is non-cooperative with incomplete information, and competition among consumers is not considered
- The agents are negotiating over a single issue, i.e., the payoff that the consumers should receive against the revelation of their personal information

Having studied the rules of the negotiation, we can now present the negotiation strategy.

3.5.1 Negotiation strategy

In our setting of incomplete information, the intelligence of the negotiation agent is realized by the negotiation strategy. In particular, the strategy of making concessions and evaluating

the incoming offers and of making decisions to interact with the negotiation opponent. This paper adopts the work of [4] in defining a concession strategy. Each agent is assumed to have a different time preference, i.e., its time deadline. In round $0 < t < \min(T^{CA}_{\text{deadline}}, T^{SP}_{\text{deadline}})$if the proposal $P^{SP\to CA}_{t-1}$ at round $t-1$ is not acceptable to the consumers' agent, the agent may make a concession to service provider's agent at round t as reaching an agreement is always better than failing to reach an agreement.

In general, the proposal of agent A to its trading partner at round t ($0 \le t \le T^{A}_{\text{deadline}}$) is modeled as a time-dependent function as follows [4]:

$$P^{A}_{t} = IP^{A} - \phi^{A}(t) \times \left(IP^{A} - RP^{A}\right) \tag{16}$$

where t is the current trading time, IP is the initial price, RP is the reservation price, and $\phi^{A}(t)$ is a time-dependent function based on the time deadline preference.

The time-dependent concession strategy is used to decide the amount of concession in each round of the negotiation process. The time-dependent function $\phi^{A}(t)$ is determined with respect to time preference η^{A} and deadline T^{A}_{deadline} (where $\eta^{A} \ge 0$ and $T^{A}_{\text{deadline}} > 0$ is finite) and is given as:

$$\phi^{A}(t) = \left(\frac{t}{T^{A}_{\text{deadline}}}\right)^{\eta^{A}} \tag{17}$$

The open literature has described a large number of negotiation strategies with respect to the remaining trading time (one for each value of η^{A}). In this paper, we adopt the "sit-and-wait" strategy proposed by [4]. The "sit-and-wait" strategy is used in the case when the negotiation issue does not devaluate over time and has been proven by [4] that this strategy is the dominant strategy for an agent using time-dependent negotiation process, regardless of the strategy that its trading partner adopts. This strategy is very practical for two reasons:

First, unlike commodities or other services that might be devaluated over time, personal information as a trading object does not have such problem. The "sit-and-wait" strategy is best suited for this scenario since consumers' compensation is guaranteed after negotiation. The "sit-and-wait" strategy is only during the negotiation process, which usually does not take long time.

Second, for the consumers, even if the offer happens at some future stage of negotiation, as long as it is anticipated, the consumers' agent who makes this offer has bargaining power. The bargaining power arises from impatience. To achieve certain competitive advantages, online businesses have particular service delivery threshold that makes them more impatient. Therefore, they are more likely to make bigger concessions to seal the deal as soon as possible.

The "sit-and-wait" strategy for the consumer agent is as follows: At the time when $t < T^{CA}_{\text{deadline}}$, it follows that $(t/T^{CA}_{\text{deadline}})^{\infty} = 0$ and $P^{CA}_{t} = IP^{CA}$. When $t = T^{CA}_{\text{deadline}}$, it follows that $(T^{CA}_{\text{deadline}}/T^{CA}_{\text{deadline}})^{\infty} = 1$ and $P^{CA}_{t} = RP^{CA}$. Let Q^{CA}_{t} and $Q^{CA}_{T^{CA}_{\text{deadline}}}$ be the amounts of concession at $t < T^{CA}_{\text{deadline}}$ and T^{CA}_{deadline}, respectively. Before the deadline, the agent does not make any concession but "waits" for the service provider agent to concede, since $Q^{CA}_{t} = P^{CA}_{t-1} - P^{CA}_{t} = 0\left(0 \le t < T^{CA}_{\text{deadline}}\right)$. It only concedes at its deadline $Q^{CA}_{T^{CA}_{\text{deadline}}} = P^{CA}_{T^{CA}_{\text{deadline}}-1} - P^{CA}_{T^{CA}_{\text{deadline}}} = IP^{CA} - RP^{CA}$. The service provider agent, on the other hand, concedes to its reservation price at T^{SP}_{deadline}. In reality, the time deadline for the consumer agent is set to be a large value so the consumer agent can benefit from the impatient of the online business.

3.5.2 *Offer construction*

Consider that the negotiation is to acquire consumers' information records that are aggregated together according to a specific interest (e.g., a list of consumers who like soccer or like to travel to England). As mentioned earlier in Sect. 3.5, it is a daunting prospect for an individual consumer to bargain with a huge service provider about a desired payoff against revealing personal information. Therefore, consumers are grouped together based on their interest and have one agent bargain on their behalf. The consumers' agent and the service provider's agent therefore will have the following objectives in their offers.

Consumers' agent offer: The consumer agent's objective is to maximize the consumers' payoff as a community, that is, maximizing their social welfare SW. Consider that N is the number of records in the list, then (for simplicity, we consider that each consumer is represented by one record) at each round of the negotiation, the consumers' agent construct an offer as follows:

$$N' = \arg\max_{N' \subseteq N} \sum_{i \in N'} SW_i \,|Uq \tag{18}$$

Such that $N' \subseteq N$ and U_q is the payoff per personal data record q (personal data record refers to the vector of information fields that will be revealed). When the consumers' agent receives an offer from the service provider's agent, it calculates the number of records N' that satisfy this offer. The decision about the number of consumers is taken based on an offer/demand curve according to the consumer's valuation of his or her personal information record. Equation (18) simply aggregates all the records that are within the range of the offered price. Any record that belongs to an individual whose valuation is higher than the offered price will not be included in the aggregated records. The main reason behind constructing the offer in such a way is the difference in the individual's valuation of privacy concerns and risks.

Service provider's agent offer: Assume that the service provider's agent has a utility value V_r, where r refers to the consumer's record in the list. Let C_r be the cost of acquiring record r (that is, the payoff offer given to the consumers' agent per record), then the agent's goal is to maximize the function $(V_r - C_r)$. The service provider's agent constructs its offer so that the value C_r is minimized. The optimal value that maximizes the utility is when $C_r = 0$, but such an offer will end the negotiation process in the first round, and the service provider will walk away with nothing. The strategy of the service provider's agent is to start with a small value C_r (for example a predefined percentage of the utility V_r) and then in each round of the negotiation gradually increases the offer at a step rate equal to θ (an arbitrary bid increment value determined by the provider and can be adapted during the negotiation if required) until it reaches its *RP*(reservation price). When the deadline expires, the best response strategy for the service provide is to concede to its reservation price *RP*. This is given in the following proof:

Let $Z = D(RP).(V_r - RP)$ represent the payoff of the service provider for the offered price *RP* and *D(RP)* is the number of record demand corresponds to the *RP* value. If *RP* is not the best response action, then there exists a utility $\dot{Z} > Z$ such that $\dot{Z} = D(RP^*).(V_r - RP^*)$ and $RP^* < RP$ is the best response. Assume the service provider at the deadline decided to terminate at RP^*, the consumer agent will then reply with $D(RP^*) < D(RP)$, and since the service provider has no prior knowledge of $D(RP^*)$ value, the risk of loosing utility $Z > \dot{Z}$ is credible. Hence, the best response is RP, that is, the response that does not involve credible risks.

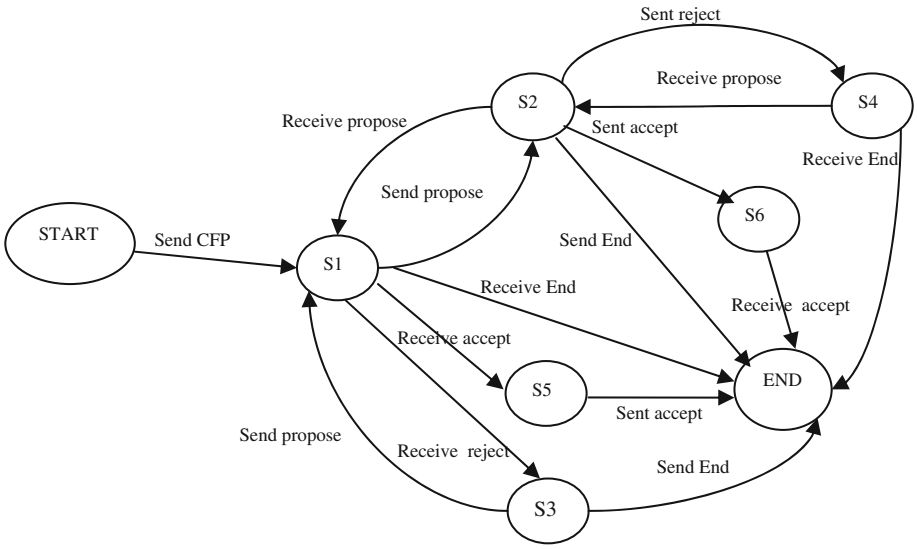

Fig. 5 State machine of 1:1 negotiation protocol

3.5.3 Negotiation protocol

A basic condition for the automation of the negotiation process among agents is the existence of a negotiation protocol, which encodes the allowed sequences of actions. Although FIPA (Foundation for Intelligent Physical Agents) provides a plethora of protocols [14], such as FIPA brokering, FIPA English auctions, FIPA Contract net protocol, we found that there is no agreed upon standard interaction protocol for 1-1 automated negotiation. As a result, we adopt the negotiation protocol proposed by [45] and implemented by [41]. This protocol is a finite state machine that must be hard-coded in all agents participating into negotiation. While we understand that hard-coded protocols in agents may lead to inflexibility, the focus of this paper is not on protocol design but rather a negotiation strategy that maximizes the consumers' benefit. Following [41], our protocol is a finite state machine with discrete states and transition, see Fig. 5.

In Fig. 5, the notations Start, S1, S2, S3, S4, S5, and S6 represent the different state of the negotiation and END is the final state in which there is an agreement or a failure of agreement between the participants. *Send* and *Receive* primitives specify the interactions between the two agents and cause state transitions. For example, the sequence of transition START->S1->S2->S6->END can be interpreted as follows: the consumer agent initially sends a call for proposal message (CFP) to the provider agent (START->S1), then it receives a propose message (S1->S2) and after the evaluation it decides to send an accept message (S2->S6). Lastly, it receives an accept message and the negotiation terminates successfully (S6->END). In the next section, we present a proof-of-concept implementation.

4 Proof-of-concept implementation

A prototype of the proposed system has been implemented using JADE (Java Agent Development Environment) platform. JADE provides a multi-agent environment, which is composed

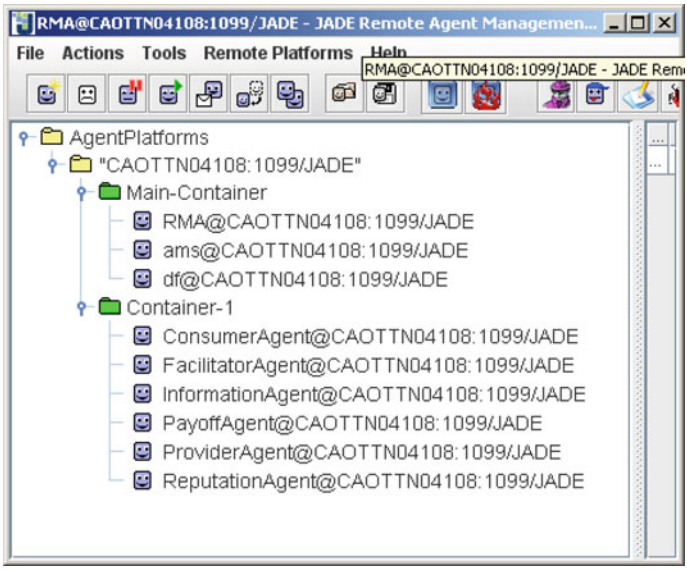

Fig. 6 Screen capture of the remote management agent GUI for JADE set-up

of the FIPA standard agents and of a set of application-dependent agents realized by the application developer. The communication component is implemented as a set of classes that inherit the jade.Core.Agent and jade.lang.acl.ACL message of existing classes of the JADE platform. These classes provide a means to construct, send, and receive messages via several FIPA communication performatives. Figure 6 shows a snapshot of the agents developed under container-1.

For the sake of convenience, the agents in our prototype reside on the same host, and all of them are under container-1. But this is not the only implementation choice. For example, we could have stored the database on another host and implemented the database agent to travel between the two hosts. Such setup would not make any difference with respect to the results of the system's validation. Similarly, if the trust and reputation agent is implemented and owned by another agency, their information can be communicated or migrated to the main host.

In our system, users open their accounts and record their preferences through a GUI interface as shown in Fig. 7. Once the user opens the account the facilitator agent sends a message to the information agent to categorize the personal information as explained in Sect. 3.2. The INFORM message sent by the facilitator agent contains the information "Prepare Categorization".

FacilitatorAgent: *Send message to Information Agent for data availability*
DatabaseAgent: *received the following message* :
(INFORM
:*sender (agent-identifier* : *name*
FacilitatorAgent@CAOTTN04108:1099/JADE :addresses (sequence http://CAOTTN04108.ad3.ad.alcatel.com:7778/acc))
:*receiver (set (agent-identifier* :*name*
InformationAgent@CAOTTN04108:1099/JADE))
:*content "Prepare Categorization")*

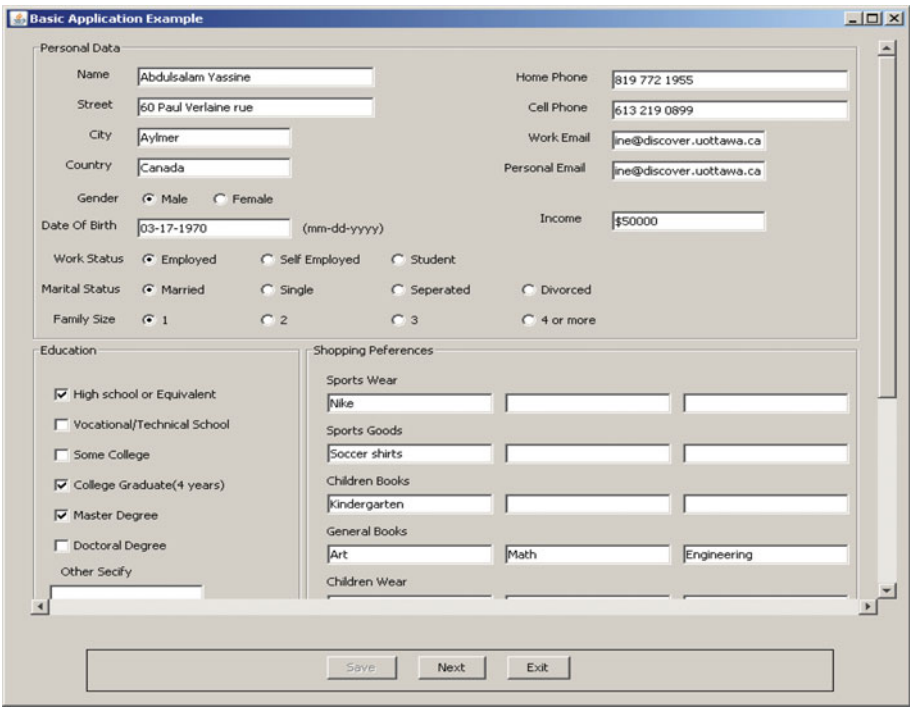

Fig. 7 User interface for consumers to open account and record their preferences

Figure 8 shows a snapshot of the user interface, which the consumers use to assign weights to their private data categories based on the service provider's privacy credentials and reputation score. In this example, the trust and reputation agent prepares the privacy credential ratings of a service provider called godaddy.com. The privacy credential report emphasizes key items of privacy concerns that are likely to be most interesting to users; for example, information about the provider' data-sharing practices and information about whether the provider allows opt out of data-sharing and marketing solicitations. For the reputation score, we collected reputation information from iVouch.com and Bizrate.com. These Web sites provide reputation services about online businesses based on customers' testimonials. The score provided in the report is the average of the reputation score provided by the commercial Web sites iVouch.com and Bizrate.com.

FacilitatorAgent: *Send message to Payoff Agent for payoff calculation*
PayoffAgent: *received the following message*:
(INFORM
:*sender (agent-identifier* : *name*
FacilitatorAgent@CAOTTN04108:1099/JADE :addresses (sequence http://CAOTTN04108.ad3.ad.alcatel.com:7778/acc))
:receiver (set (agent-identifier :name
PayoffAgent@CAOTTN04108:1099/JADE))
:*content "0.6428572")*

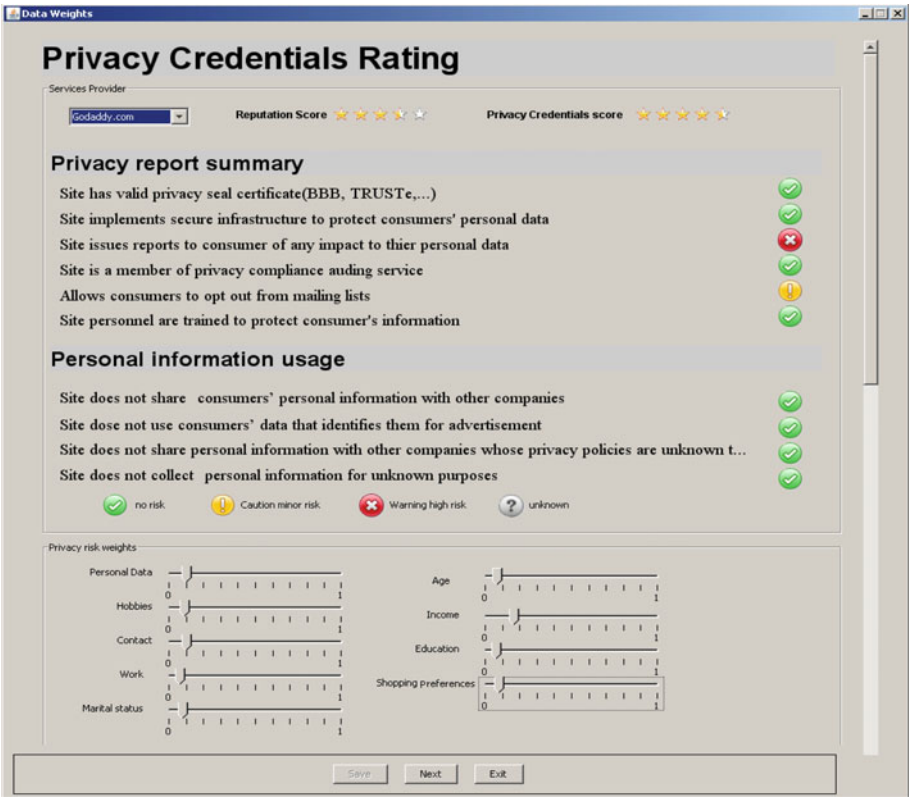

Fig. 8 User interface for consumers to assign their privacy risk weights

Table 3 Negotiation parameters for both the consumer agent and the provider agent

Consumer agent	Provider agent
Experiment 1- negotiation per record	
Reservation price = 45	Utility = 70
Time deadline = 10	Reservation price = 35
Number of consumer record = 2000	Time deadline = 6
	Bid Increment = 3
Experiment 2 – Risk-premium variation	
Reservation price set according to the Payoff valuation and risk premium	Utility = 70
Time deadline = 15	Reservation price = 35
Number of consumer record = 2,000	Time deadline = 10
	Bid increment = 3

Service providers are: Escapes.com, Expedia.com, Travelocity.com, Canadatravel.ca, Itravel2000.com

The user uses the credential report to learn about the service provider's privacy practices and then to assign the level of privacy risk to his personal data categories based on the perceived privacy risk. The system prompts (with an error exception) the user to revise his

selection if he/she makes an ill characterization such as exceeding the privcy risk sum of 1 for all categories. Once the user assigns the privacy risk weights, the information agent quantifies the total privacy risk of the user personal information. The payoff agent uses the quantified information to calculate the payoff value for the consumer. The message received by the payoff agent is shown below.

In the above message, the privacy risk value calculated by the information agent is 0.657143 for the user account shown in Fig. 7. The payoff agent uses this value to calculate the payoff that the consumer should receive. For this example, we assumed the risk-premium value to be $50, then the consumer should receive $32.142 as a payoff for revealing his personal information record.

After the payoff is calculated, the consumer agent (the agent that negotiates on behalf of consumers) receives a message to start the negotiation.

```
FacilitatorAgent: Send message to Consumer Agent to start negotiation...
ConsumerAgent: received the following message :
(INFORM
:sender (agent-identifier :name
FacilitatorAgent@CAOTTN04108:1099/JADE :addresses (sequence http://
CAOTTN04108.ad3.ad.alcatel.com:7778/acc))
:receiver (set (agent-identifier :name
ConsumerAgent@CAOTTN04108:1099/JADE))
:content “Start Negotiation”)
```

4.1 Negotiation results

For the setup of the negotiation process, we have created two agents namely the consumers' agent (working on behalf of consumers) and the service provider's agent (working on behalf of the online service provider). Table 3 shows the parameters we used to setup the negotiation process for the experiments. We have simulated 2000 user accounts stored in the database. We have randomly assigned values between 0 and 1 to simulate individual's differentiation of privacy concerns. As mentioned earlier in section “negotiation agent”, the negotiation process is time dependent and as such each agent has its own time deadline. Also each agent has its utility value, which represents its relative satisfaction.

Experiment 1: In the this experiment, the service provider's agent reaches its deadline and concedes to its reservation price. Each time the consumer agent receives an offer it calculates the number of records N' (as explained in Sect. 3.5.2) and sends it to the provider agent in a propose message. In the following paragraph, we show the exchange of offers in round 4 (a negotiation round corresponds to the process of sending a propose message and receiving a reply) as well as the final accept message. The propose message sent by the provider agent contains the provider's offer of $16 per record (shown in the content section of the message). The replied propose message sent by the consumer agent contains an offer equal to 371 consumers' records (shown in the content message). The exchange of message continues until the provider agent sends its final offer and the consumer agent accepts it. The content of the accept-proposal message include 1538 records of consumers that potentially will accept to share their personal information for the agreed upon payoff.

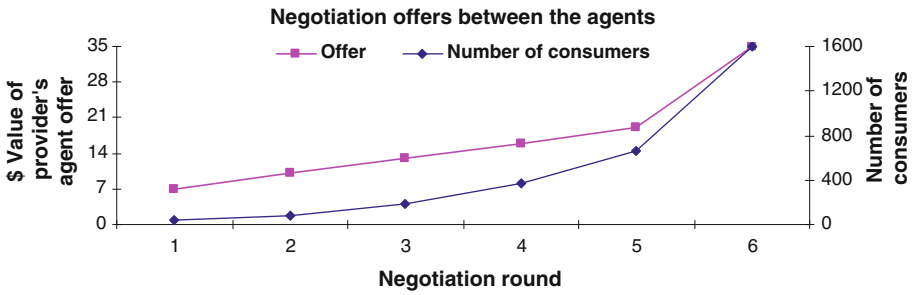

Fig. 9 Negotiation offers between the consumer agent and the provider agent

Exchange of messages in round 4:
(PROPOSE
:sender (agent-identifier :name ProviderAgent@CAOTTN04108:1099/JADE
:addresses (sequence http://CAOTTN04108.ad3.ad.alcatel.com:7778/acc))
:receiver (set (agent-identifier :name ConsumerAgent@CAOTTN04108:1099/JADE))
:content "inbidPR:16.0")

(PROPOSE
:sender (agent-identifier :name ConsumerAgent@CAOTTN04108:1099/JADE
:addresses (sequence http://CAOTTN04108.ad3.ad.alcatel.com:7778/acc))
:receiver (set (agent-identifier :name ProviderAgent@CAOTTN04108:1099/JADE))
:content "inbidCA:371")

ACCEPT-PROPOSAL message:
Provider Agent: received the following message:
(ACCEPT-PROPOSAL
:sender (agent-identifier :name ConsumerAgent@CAOTTN04108:1099/JADE
:addresses (sequence http://CAOTTN04108.ad3.ad.alcatel.com:7778/acc))
:receiver (set (agent-identifier :name ProviderAgent@CAOTTN04108:1099/JADE))
:content "inbidCA:1538")

Figure 9 depicts the values of the exchanged offers between the two agents. Each time the provider agent increases its offer, the number of consumers who are willing to share their personal information increases. This is because individuals valuate their perceived privacy risks differently. While some people are willing to accept lower offers to reveal their personal information (this type of individuals according to [43] are marginally not concerned), others expect offers that are worth the risk of exposure (e.g., privacy pragmatics and privacy fundamentalists).

In this scenario, the final payoff value is $35 for each record, which means that the total gain of the consumers' community is 1538*$35 = $53830.

Experiment 2: This experiment examines the effect of the risk-premium variation on the overall benefit of both the service provider and the consumers. The variation in the market risk premium is simulated by incrementing the drift value by 0.1, thus increasing the risk premium gradually. For this experiment, five service providers were chosen that represent different privacy practice regimes. The five service providers are travel agencies that offer similar services and similar prices. The service providers are Escapes.com, Expedia.com,

Travelocity.com, Canadatravel.ca, and Itravel2000.com and for convenience, we name them SP_1, SP_2, SP_3, SP_4, and SP_5, respectively. The privacy credential ratings of these service providers are as follows: Escapes.com PCR is 1 star, Expedia.com PCR is 1.5 stars, Travelocity.com PCR is 3 stars, Canadatravel.ca PCR is 4 stars, and Itravel2000.com PCR is 4.5 stars. Five different tests were performed, one for each service provider. Figure 10 shows the outcome of the experiments. It presents the service providers' benefit, the consumers' benefit, and the number of completed transactions. Results from the experiment show that service providers with high privacy credential rating achieve higher utility than service providers with lesser privacy credential rating; see Fig. 10a. In Fig. 10a, when the market risk premium is high (i.e., when the drift value is 2), service provider SP_5 acquired a benefit value equal to $18370 compared to $0, $0, $100, and $2860 for service providers SP_1, SP_2, SP_3, and SP_4, respectively. The reason behind this significant difference is that 334 consumers completed the transaction in the case of SP_5 (shown in Fig. 10f). The 334 consumers were expecting a payoff less than what offered by the service provider. This is based on the valuation of their private data given their perceived privacy risk of service provider SP_5. In case of service provider SP_4, 52 consumers completed the transaction, and in case of SP_3, only 2 consumers completed the transaction, as shown in Fig. 10d, e, respectively. In both cases, the consumers' perceived risk in SP_4 and SP_3 was low. At high market risk premium, service providers SP_1 and SP_2 could not secure any transactions. Figure 10b, c show that at high market risk premium, consumers did not complete any transactions with service providers SP_1 and SP_2. This puts more emphasis on the fact that service providers with higher trust values (i.e., respecting consumers' privacy) will be regarded by consumers despite how the market premiums behave.

Figure 10b–f record the performance of each service provider as well as the consumers' benefit. The influence of the market risk premium is significant in each case. When the drift value = (1, 1.1, and 1.2) representing low risk premium, all service providers were able to accumulate a benefit depending on their type, i.e., their privacy credential rating. However, as the risk premium increases to a moderate level (1.4, 1.5, and 1.6), service provider SP_1, for instance, accumulated $0 benefit (shown in Fig. 10b) because all consumers at that level were expecting higher payoff as the privacy risk increases. Such payoff is unaffordable by service provider SP_1. In Fig. 10c, the benefit of service provider SP_2 dropped to $0 at a 1.7 drift value suffering the same dilemma as SP_1 but at a later stage. SP_3 and SP_4 in Fig. 10d, e suffered from a sharp decline of benefit from $5,225 and $28,600 at moderate market risk premium to $1100 and $2,860 at a high market risk premium, respectively. Only SP_5 was able to keep a higher benefit at a high market risk premium. The outcome of the experiments reveals how the overall perception toward privacy impacts the benefit of both the service provider and the consumers. Consumers who are reluctant to complete transactions because they perceive high privacy risk impact the service providers' benefit as they ignore their services.

In sum, the experiments showed an interesting result about the effect of the overall perception of privacy risk. It showed that consumers and service providers are both better off if privacy risk is low.

5 Discussion

The goal of this paper is the development of a knowledge-empowered agent information system architecture that allows users to participate in the information market and benefit from sharing their personal information. One of the main contributions is the proposal of a

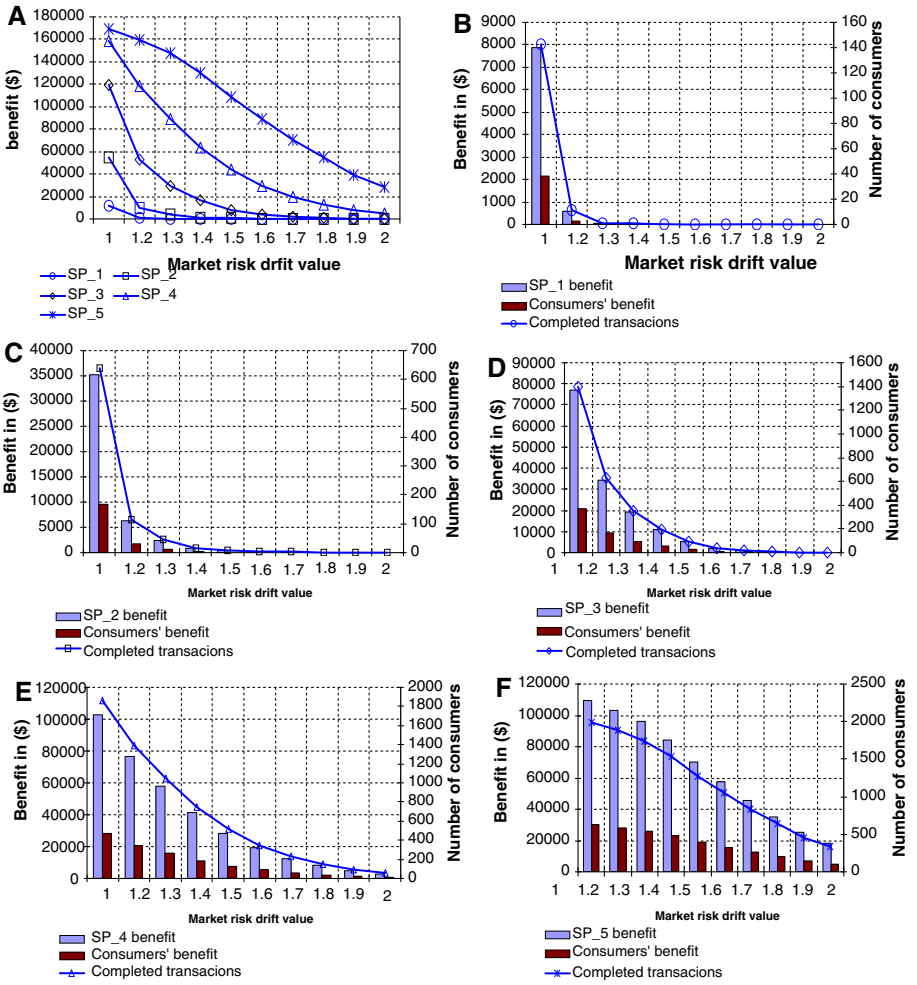

Fig. 10 Benefit of service providers and consumers. **a** Performance of service providers with respect to the market risk premium. **b**, **c**, **d**, **e**, and **f** detail the corresponding consumers' benefit and the completed transactions with respect to the market risk

new technique to categorize and valuate privacy risks derived from users' private data set based on attribute ontology. This new technique takes into account the granularity of private data, which is achieved by associating the contextual usage risk to the personal data objects. Our system allows users to assign credit values based on the users' perceived risk, trust, and the level of protection. As such, this paper contributed to the process of making privacy risk a measuring principle for the quantification of the privacy payoff value.

One of the challenges that users face in the online world is how service providers use their personal information. The paper advances the state of the art by proposing a new assessment scheme to determine the trustworthiness of service providers based on privacy credentials. This is achieved through the design and development of a new mechanism that allows consumers to see "good" signs and "bad" signs when visiting online stores. The trust and reputation agent, who is responsible of making such knowledge available to consumers,

provides a privacy credential score and a report detailing the competency of the service provider with respect to privacy and private data handling. The importance of such assessment is that it serves as a source of knowledge that allows consumers to learn how their personal information will be handled by a potential service provider.

Yet another contribution is the development of a model by which we can valuate the payoff for the consumers against the revelation of their personal information. In this paper, we were the first to use a financial model to construct the amount of the payoff based on the risk exposure. This model is well known in the financial and insurance industry. Financial models (such as the one we used) are designed so that those who are considered more risky should pay more interest. By so doing, we were able to valuate the payoff value that the consumers should receive against the revelation of personal information.

Concerning the negotiation with online service providers, this process is proven to be a daunting prospect for an individual consumer as explained in Sect 3.5. The extension of the "sit-and-wait" strategy allows us to empower the negotiation agent with a dominant strategy for an agent using time-dependent negotiation process.

In the proof-of-concept implementation that inspired by the scenario presented in Sect. 3.1, the validity of the system made clear that the proposed system is feasible. Furthermore, we have shown through experiments that a strategically placed agent can help consumers attain the maximum gain during the negotiation process. The most important conclusion of the experiments is that consumers and service providers are both better off if privacy risk is low.

While some people would argue that such system could lead to an intensified disclosure of personal data, it is unlikely to happen for the following reasons: first, the payoff or the compensation given to the consumers is for personal information that they usually provide for free anyway, while online businesses rack up lucrative amounts of money from personal information profiling. At best, consumers sometimes exchange a certain degree of privacy (i.e., providing some of their personal information) for small deals such as price discounts, customized offers, specials (Acquisti 2004) [7,17,19].

Second, the payoffs are risk-base premiums. Therefore, online businesses are expected to be more conservative when handling consumers' personal information as privacy risk penalties (risk-base premiums), and reputation consequences on violators of consumers presumed privacy rights are more likely to be costly.

Third, since attention in the information market within eCommerce is one of the main reasons, if not the most important reason, behind the collection of personal information, service providers have a financial stake in seeking ways for accurate information. In other words, service providers essentially incur excess costs (junk e-mails, junk advertisements, etc.) to attract consumers' attention to their products and services. However, if they knew precisely what the consumer wanted, they could make a much better decision about whether or not to provide the consumer with information about their services.

6 Conclusion and future work

This paper reports on a knowledge-empowered agent information system for consumers' privacy payoff in eCommerce. The key ideas and the overall system architecture are described, and a proof-of-concept implementation is presented. We plan to extend our work in various ways:

The first direction is to consider the effect of future learning in the collected personal information. The model presented in this paper assumes that the possession of information today does not influence the possession of information in the future or the possible reselling

of the information by the service provider, and therefore, it assumes a linear view of the information valuation with respect to the risk at the time of revealing the personal information. However, in reality, a future learning effect such as discovering patterns in sensitive data [3] might impose different usage of personal information at different time intervals. Another possibility of learning effect could result from different parties colluding with each other and share records to deduce the private information [49]. In such cases, different level of privacy risk assessment must be considered. This means that when the agent computes compensation prices should consider a learning premium in the belief that what personal information the consumer reveal today will allow online businesses to learn more about this same consumer in the future. In this case, when we generalized the concept of compensation prices of risk to private data, the linear correlation assumption becomes inadequate as the distribution of risk becomes non-normal.

The second direction is to engage real scenarios with actual users, this is because empirical studies, such as those of [48] and [20], to name few, of the value consumers assign to privacy risk have highlighted a dichotomy between professed attitudes and actual behavior, raising questions about individuals' awareness of privacy trade-offs and their true valuation of privacy.

References

1. Acquisti A, Grossklags J (2005) Privacy and rationality in individual decision making. IEEE Secur Priv 3:26–33
2. Bakshi G, Carr P, Wu L (2006) Stochastic risk premiums, stochastic skewness in currency options, and stochastic discount factors in international economies. J Financial Econ 87(1):132–156
3. Bhaskar R, Laxman S, Smith A, Thakurat A (2010) Discovering frequent patterns in sensitive data KDD'10, July 25–28, 2010, Washington, DC, USA
4. Bo An, Sim KS, Tang LG, Mia CY, Shen ZQ, Cheng DJ (2008) Negotiation agents' decision making using Markov chains. Stud Comput Intell 89:3–23
5. Cao L, He T (2009) Developing actionable trading agents. Knowl Inf Syst 18:183–198
6. Cavoukian A, (2009) Privacy as a negative externality: the solution privacy by design. WEIS Workshop on the Economics of Information Security in London, UK
7. Chellappa R, Sin RG (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inf Technol Manag 6:2–3
8. Chouk I, Perrien J, Nantel J (2007) Consumer trust towards an unfamiliar web merchant: role of third parties. EMAC 2007 (European Marketing Academy). Available at http://www.chairerbc.com/chairerbc/fr/confscig.asp
9. Clinebell JM, Kahl DR, Stevens J (1994) Time series properties of the equity risk premium. J Financial Res XVII(1)
10. Cline J (2003) Website privacy seal: are they worth it? Available at http://www.computerworld.com/s/article/81041/Web_site_privacy_seals_Are_they_worth_it_
11. Danthine JP, Donalaon IB (2002) Intermediate financial theory, 1st edn. Pearson Education, New Jersey
12. Desmarais C, Shen X, Shirmohammadi S, Cameron A, Goerganas ND, Kerr I (2007) PLUTO—a privacy control protocol for e-commerce communities. In: Proceeding IEEE conference on enterprise computing, e-commerce and e-services, Tokyo, Japan
13. Dighton JA (2003). Market solutions to privacy problems? Chapter 6 in digital anonymity and the law—tensions and dimensions. T.M.C. Asser Press, Harvard Business School, The Hague
14. FIPA specification http://www.fipa.org/
15. Gkoulalas-Divanis A, Verykios VS (2009) Hiding sensitive knowledge without side effects. Knowl Inf Syst 20:263–299
16. Gideon J, Egelman S, Cranor L, Acquisti A (2006) Power strips, prophylactics, and privacy, oh my! Symposium on usable privacy and security SOUPS, PA, USA
17. Hann I-H, Hui KL, Lee TS, Png IPL (2003)The value of online information privacy: an empirical investigation. AEI-Brookings joint center for regulatory studies

18. Holger B, Ram/on H, Sascha O, Roberto C (2007) Trust-based Service Provider Selection in Open Environments SAC'07 March 1115, 2007, Seoul, Korea
19. Hui KL, Tan BCY, Goh CY (2006) Online information disclosure: motivators and measurements. ACM Trans Intern Technol 6(4):415–441
20. Huberman AB, Ader E, Fine LR (2005) Valuating privacy. IEEE Secur Priv 3(5):22–25
21. Hussin AR, Macaulay L, Keeling K (2007) The importance ranking of trust attributes in e-commerce website. 11th Pacific-Asia conference on information systems
22. Keke C, Ling L (2010) Geometric data perturbation for privacy preserving outsource data mining knowledge and Information systems Published Online 23, November 2010 http://www.springerlink.com/content/e2132015k666x24k/
23. Kim DJ, Ferin DL, Rao HR (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decis Support Syst 44:544–564
24. Krause A, Horvitz E (2008) A utility-theoretic approach to privacy and personalization. In: Proceedings of the twenty-third AAAI conference on artificial intelligence
25. Larose R (2004) Promoting I-safety: the effects of consumer information and privacy seals on risk assessment and online privacy behavior. International Communication Association, New Orleans Sheraton, New Orleans. Available at http://www.allacademic.com/meta/p113099_index.html
26. Laudon KC (1996) Markets and privacy. Commun ACM 39(9): 92–104
27. Lioudakis GL, Koutsoloukas EA, Delaas Nl, Tselikas N, Kapellaki S, Preaerakos GN, Kaklamani DI, Venieris IS (2007) A middleware architecture for privacy protection. Comput Netw 51:4679–4696
28. Liu K, Terzi E (2009) A framework for computing the privacy scores of users in online social networks. Ninth IEEE international conference on data mining, ICDM.2009.21
29. Mcsherry F (2010) Privacy integrated queries: an extensible platform for preserving data analysis. Commun ACM 53(9) 89–97
30. Meinert DB, Peterson D, Criswell J, Crossland MD (2003) Would regulation of web site privacy policy statements increase consumer trust? Inf Sci 9:123–142. URL: http://inform.nu/Articles/Vol9/v9p123-142Meinert82.pdf
31. Pennington R, Wilcox HD, Grover V (2003) The role of system trust in business-to consumer transactions. J Manag Inf Syst 20(3):197–226
32. Piolle G, Demazeau Y, Caelen J (2007) Privacy management in user-centred multi-agent systems. ESAW 2006, Springer LNAI 4457, pp 354–367
33. Preibush S (2005) Implementing privacy negotiation techniques in e-commerce. In: Proceedings of the seventh IEEE international conference on e-commerce technology
34. Prins C (2006) When personal data, behavior and virtual identities become a commodity: would a property rights approach matter? SCRIPT-ed 3(4)
35. Ratnasingam P, Pavlou PA (2003) Technology trust in Internet based inter organizational electronic commerce. J Electron Comm Organ 1(1):17–41
36. Ribaric S, Hrkac T (2008) TeMS-a multi-agent system for temporally rich domains. Knowl Inform Syst 15:1–30
37. Ross S (2004) Stochastic processes. Wiley, New York, chap 8, (2nd edn, pp 366–381, 1995)
38. Sakuma J, Kobayashi S (2010) Large-scale k-means clustering with user-centric privacy-preservation. Knowl Inf Syst 25:253–279
39. Sha W (2009) Types of structural assurance and their relationships with trusting intentions in business-to-consumer e-commerce. Electron Markets 19:43–54
40. Schlager C, Pernul G (2008) Trust modeling in e-commerce through fuzzy cognitive maps. The third international conference on availability, reliability and security ARES 2008
41. Skylogiannis T, Anotniou G, Bassiliades N, Governatori G, Bikakis A (2007) DR-NEGOTIATE—a system for automated agent negotiation with defeasible logic-based strategies. Data Knowl Eng 63(2):362–380
42. Sensoy M, Yulom P (2009) Evolving service semantics cooperatively: a consumer-driven approach. Auton Agents Multi-Agent Syst 18:526–555
43. Spiekermann S (2001) Online information search with electronic agents: drivers, impediments, and privacy issues. http://edoc.hu-berlin.de/dissertationen/spiekermann-sarah-2001-11-22/PDF/Spiekermann.pdf
44. Syverson P (2003) The paradoxical value of privacy. 2nd Annual workshop on economics and information security (WEIS 2003)
45. Su SYW, Huang C, Hammer J (2000) A replicable web-based negotiation server for e-commerce. In: Proceedings 33rd Hawaii international conference on system sciences
46. Tang Z, Hu J, Smith MD (2008) Protecting online privacy: self-regulation, mandatory standards, or caveat emptor. J Manag Inf Syst 24(4):153–173

47. Taylor CR (2004) Consumer privacy and the market for customer information. RAND J Econ 35(4):631–650
48. Taylor H (2003) Most people are privacy pragmatists, who, while concerned about privacy, will sometimes trade it off for other benefits. The Harris Poll, 17
49. Yang B, Nakagawa H, Sato I, Sakuma J (2010) Collusion resistant privacy-preserving data Mining KDD'10, July 25–28, 2010, Washington, DC, USA
50. Yassine A, Shirmohammadi S (2009) An intelligent agent-based framework for privacy payoff negotiation in virtual environments. In: Proceedings of IEEE workshop on computational intelligence in virtual environments. Proceedings of IEEE symposium series on computational intelligence, Nashville, TN, USA
51. Yassine A, Shirmohammadi S (2008) A business privacy model for virtual communities. Int J Web Based Commun 5(2)
52. Yassine A, Shirmohammadi S (2009) Measuring users' privacy payoff using intelligent agents *IEEE computational intelligence society, international conference on computational intelligence for measurements systems and applications*, CIMSA09
53. Yassine A, Shirmohammadi S (2008) Privacy and the market for private data: a negotiation model to capitalize on private data. In: Proceedings of ACS/IEEE international conference on computer systems and applications, Doha, Qatar, March 31–April 4 2008, pp 669–678
54. Yu T, Zhang Y, Lin KJ (2006). Modeling and measuring privacy risks in QoS web services. In: Proceeding of the 8th IEEE international conference on e-commerce technology and the 3rd IEEE international conference on enterprise computing, e-commerce, and e-services, 4 p
55. W3C (2005) The platform for privacy preferences 1.1 (P3P1.1) Specification. W3C working draft 4 http://www.w3.org/TR/2005/WD-P3P11-20050104/
56. Xin W, Xiaojun S, Nicolas DG (2006) A fuzzy logic based intelligent negotiation agent (FINA) in e-commerce. IEEE CCECE/CCGEI, Ottawa, May 2006
57. Zhang H (2005) Trust-promoting seals in electronic markets: impact of online shopping decisions. J Inf Technol Appl. Available at http://www.allbusiness.com/jitta/journal-information-technology-theory-application/11499500-1.html
58. Zhang R, Tran T (2011) An information gain-based approach for recommending useful product reviews. Knowl Inf Syst 26:419–434
59. Zhuang Y, Fong S, Shi M (2008) Knowledge-empowered automated negotiation system for e-commerce. Knowl Inf Syst 17:167–191

Author Biographies

Abdulsalam Yassine received his Ph.D. and M.Sc. in Electrical and Computer Engineering from University of Ottawa—Canada in 2010 and 2004, respectively, his B.Sc. in Electrical Engineering from Beirut Arab University–Lebanon in 1993. He is currently member of the technical staff in the Wireless Communication Division at Alcatel-Lucent, Ottawa, Canada. His current research interests are mostly focused on Artificial Intelligence (AI), Electronic Commerce, Intelligent Agents and Multi-Agent Systems, Game Theory, Ambient Intelligence and Smart Environments, Smart Grids, and Pricing Communication Networks.

Ali Asghar Nazari Shirehjini received his Ph.D. in Computer Science from the Technische Universität Darmstadt in 2008. He is currently a senior researcher and co-director of the Competence Center "Next Generation Services" at the "Distributed Artificial Intelligence Laboratory" (DAI-Labor), Technische Universität Berlin, Germany. In the years between December 2008 and April 2011, he was one of the four Vision 2010 postdoctoral fellows at the University of Ottawa. In the years between 2001 and 2008, he worked at the Fraunhofer Institute for Computer Graphics and GMD-IPSI in Darmstadt, Germany. His research interests include Ambient Intelligence, Human Factors, Intelligent Agents and Multi-Agent Systems, Pervasive and Mobile Games, Game-based Rehabilitation, Massively Multiplayer Online Gaming (MMOG), and Electronic Commerce.

Shervin Shirmohammadi is an Associate Professor at the School of Information Technology and Engineering, University of Ottawa, Canada. He is the Associate Director of the Distributed and Collaborative Virtual Environment Research Laboratory (DISCOVER Lab) and Co-director of the Multimedia Communications Research Laboratory (MCRLab). His research interests are in multimedia systems and networking, specifically in gaming and virtual environments, video systems, and their applications. The results of his research have lead to more than 170 publications, over a dozen technology transfers to the private sector, and a number of awards and prizes. He is Associate Editor of ACM Transactions on Multimedia Computing, Communications, and Applications, IEEE Transactions on Instrumentation and Measurement, and Springer's Journal of Multimedia Tools and Applications. Dr. Shirmohammadi is an IEEE Distinguished Lecturer, a University of Ottawa Gold Medalist, a licensed Professional Engineer in Ontario, a Senior Member of the IEEE, and a Professional Member of the ACM.

Thomas T. Tran received his Ph.D. in Computer Science from the University of Waterloo in 2004, and was the recipient of the Governor General's Gold Medal at the Convocation Ceremony. He is currently an Associate Professor at the School of Information Technology and Engineering, University of Ottawa, Canada. He is also a member of the Institute of Electrical and Electronic Engineers (IEEE), the Association for the Advancement of Artificial Intelligence (AAAI), and the Canadian Artificial Intelligence Association (CAIAC). His research interests include Artificial Intelligence (AI), Electronic Commerce, Intelligent Agents and Multi-Agent Systems, Trust and Reputation Modeling, Reinforcement Learning, Recommender Systems, Knowledge-Based Systems, Architecture for Mobile E-Business, and Vehicular Ad-hoc Networks.