16th Bled eCommerce Conference

eTransformation

Bled, Slovenia, June 9 - 11, 2003

A Client-Side Business Model for Electronic Privacy

Dawn Jutla

Faculty of Commerce, Saint Mary's University, Canada
Dawn.Jutla@smu.ca

Peter Bodorik

Faculty of Computer Science, Dalhousie University, Canada
Peter.Bodorik@cs.dal.ca

Abstract

Strengthening the user perception of privacy and trust on the Internet will require user-focused technological approaches, enforceable privacy laws, and business interventions. We propose a novel user-focused business model for privacy with a supporting client-side e-privacy architecture. The e-privacy business model is detailed in terms of target markets and stakeholders, value or revenue model, and privacy information and transaction flows. The target markets and stakeholder descriptions capture two key requirements of heightening user control, and placing privacy in a trust position. A value model stacked towards the user perspective is necessary for any e-privacy business model to succeed. Finally, a multi-agent architecture, based on the P3P platform, completes our proposed e-privacy business model.

1. Introduction

Writing privacy interfaces into business applications must address a juxtaposition of marketing needs. On the one hand, businesses recognize the need to build online trust to increase online purchasing, develop online markets, conduct successful online marketing and realize sales through Web channels. On the other, businesses view consumer data as an asset of value that provides competitive advantage. Indeed, businesses are currently struggling to reconcile the rise of electronic customer relationship management (e-CRM) as a business tool (Magourik 2001), and the rising concern regarding the privacy of personal data. One mediator in this conflict is the regulatory framework in which the business operates. For example, in the European Union (EU), data collection is parsimonious due to legal necessity to comply with the 1995 EU Data Directive. Whilst in the United States, and to some extent in Canada and Australia, business models exploiting the richness and availability of data/information on the Web are still plausible.

The political history of Europe naturally creates a user whose intolerance of human indignity and intrusion into trusted and/or private domains is high.

Another mediator in the user trust, privacy, and business needs equation is the user herself. She can be empowered with cookie crushers, anonymizers, P3P preference documents, and privacy management software. P3P extensions are being proposed using novel approaches involving other stakeholders, such as associations or communities, to create social norms for policy preferences (Kaufmann and Powers 2002). The idea is to use technology to speed up an associations view (e.g. a Parents-Teachers Association view) on policy preferences for its membership to business in general. IBM researchers, Kaufmann and Powers (2002) call this proposal the social core contract. Thus trust creating mechanisms also known as "interventions for trust" can be outlined from each stakeholder: user (customer, employee, citizen), community, industry association, and government.

Privacy must be intrinsic in trusted electronic transactions – one of the volatile issues cited as a contributing cause of the failure of business models for the B2B marketplaces (e.g., VerticalNet's first business model). Businesses do not sufficiently trust the third party with the storage of their transactional data. We can argue that the currently available Trusted Third Party-based (TTP) business models for privacy such as Lumeria's and ZeroKnowledge's will eventually suffer similar fates as users are still suspicious despite TTP reassurances.

It is the premise of this paper that an e-privacy business model should be created from the user perspective, incorporating critical user requirements for privacy, and which builds on the P3P platform. Our proposed e-privacy model's architecture moves beyond the W3C simple guidelines for P3P.

The paper is organized as follows. The second section describes the target markets and stakeholders in e-privacy. The third section provides a value model component. A supporting e-privacy architecture is described in the fourth section. The fifth section discusses related issues and relevant literature. The final section offers a summary and concluding remarks.

2. A Business Model for e-Privacy

A business model is generally defined as (1) a description of target markets and stakeholders (2) description of how revenue is obtained, and (3) a description of the architecture for information flows, product flows, and transaction flows. (Timmers, 2000, Craig and Jutla, 2001). We describe an e-privacy business model in the context of Timmers (2000) definition in this and subsequent sections.

2.1 ePrivacy Target Markets

Users (customers, citizens, employees), businesses (including those in electronic markets), communities, and governments are the major stakeholders in online privacy. We posit that the user will be the primary stakeholder in terms of widespread adoption of any e-privacy business model. That users demand complete control over their private data, implying limited trust in other parties, has been evidenced by a number of failed initiatives (e.g. Microsoft code-named HailStorm service). We argue in this paper that one primary reason these initiatives have failed is because they have been perceived as attempts to take control of user's private data. We can translate this to the user's fear that a third party can “know too much” about the user – what is generally perceived as an invasion of privacy. Other reasons include resistance to having personal data collected as a business asset.

The link between control, trust, and privacy is explored in Novak et al (1999) where results from large users’ surveys bolstered the authors arguments that lack of trust arises “from cyberconsumers’ perceived lack of control over the access others have to their personal information during the online navigation process,” and from “..concerns of control span secondary use of information” Novak et al (1999) conclude that “trust will be best achieved by allowing the balance of power to shift toward a more cooperative interaction between the online business and its customers. The premise is also supported in Wang et al (1998). An e-privacy business model should thus capture two fundamental aspects. (1) perception of heightened *user* control, and (2) a trust position.

2.1.1 User Control

The user’s perception of *control* is one of the fundamental properties in building the online user’s trust. Online trust is one of the required elements for increased adoption of web-based services and products (Sasse and Adams, 1999, Adams 2000). Privacy control should mean adding user control to data collection activities in terms of the user exercising choice to opt in/out, or provide data or not, having the rights to access and correct her personally identifiable information (PII) and to object to incorrect use, and place limits on who can access her PII, for what purposes, and know physical (where) and temporal (when) storage of her PII.

In a seminal paper, Hui and Bateson (1991) show how perceived control is a crucial variable in mediating a consumer’s emotional and behavioral response to a service encounter. Perceived control can make the encounter more pleasurable. These findings are very pertinent to Web service encounters. Indeed trust and privacy issues have been reported as barriers to widespread adoption of electronic commerce (EU 2002). Hui and Bateson conclude that their results are interesting to service providers and businesses because perceived control over a service interaction can lead to increased customer satisfaction. Ackerman et al (2001) also supports the importance of control to privacy by stating that “privacy is intrinsically bound up with control – who controls what information as well as the applications and systems that construct and disseminate that information.”

Privacy control is also applicable to data collected through sensor-based systems and services of which the user may not be aware. According to Ackerman et al (2001), “the major privacy effects come from no mechanisms to tell the user what context-gathering systems are present and what they intend to do with collected data.“

In a project detailing intelligent software agents’ compliance to the EU Data Directive, Patrick and Kenny (2002) identify four categories of human-computer interface requirements for adhering to privacy principles - the 4Cs: *comprehend*, *conscious*, *control*, and *consent*. Adams and Sasse (2001), Dey et al (2001), and Ackerman et al (2001) provide sufficient arguments about users’ *context* for us to recommend the adding of *context* as a fifth category – a fifth C. User privacy needs are distinct in multiple, different contexts. Situational context refers to the whereabouts of the user, social situation, or relation between people. A key problem in pervasive computer systems, embedded in the environment, is that there may be multiple simultaneous users, not one user at a time as is the norm in conventional computer systems. This departure complicates privacy issues. Dey et al (2001) and Ackerman et al (2001) further illustrate the problem of physical identity context, where technologists envision “perceptual interfaces which track users’ positions in a room, can recognize them when they return, and can detect pointing gestures and certain facial expressions" (Darrell et al 2000). With the advent of computer systems with the capability to be truly invisible (e.g. the European Disappearing Computer Initiative (Wejchert, 2000)), or transparent (e.g. a hand-tool), or subordinated (e.g. wearable computers, mobile phones), questions that arise include (1) how to protect privacy when we are trying to attract one users's attention without disturbing other colocated people (Dey et al, 2001), (2) who has access to the data if the environment records everything about you, and (3) how is privacy impacted in the case of a system malfunction?

Adams and Sasse (2001) also identify privacy context in terms of the context of the data (e.g. sensitivity of information) rather than situational context. Context has also been studied in Hui and Bateson (1991) for perceived control in terms of perceived control lessening the effects of crowding (a context) in offline service encounters.

Clearly the five Cs of privacy apply to trust-building. Users and business do not trust what they do not comprehend or what gives them a feeling of vulnerability/helplessness. Behaviours that hide or deceive do not foster trust. People trust what they understand, when they believe that other parties are up-front and have told them what they should know about a transaction, when events can be controlled, or when they have choice and explicit consent. Trust levels go up or down depending on users' context whether they are in online multimedia, aesthically pleasing, sensitive situations, or "crowded" environments.

2.1.2 Privacy in a Position of Trust: Stakeholder Interventions

In this section we build on the extensive work that has been published in the area of online trust. We propose an extension to these works and qualitatively justify online privacy's position relative to online trust. We start by examining the most recent trust models and scales for electronic business and discuss their strengths and weaknesses. The first, and as yet only, scientifically validated models and measurement scales for trust in e-business are in (1) Bhatacharjee (2002), published in the journal of management information systems (JMIS), and in (2) McKnight et al, (2002) published in the Information Systems Research journal (ISR) in summer 2002. Both works are based on intensive review of the past trust literature, citing and defining the various ways trust has been conceptualized: as an attitude, belief, intention and/or behavior, domain-specific psychological state, and/or process. Interestingly enough, both independent works converge on their syntheses of the three most common trusting beliefs: benevolence, integrity, and competence (ability). These three sub-constructs are first proposed and studied in Mayer et al, (1995), and Gefen, (1997). Based on a review of 32 trust articles and books, McKnight et al (2002) identify and use these three sub-constructs to decompose the antecedents to trusting intentions in their trust model. Bhattacharjee (2002) reviews 16 trust studies, many coinciding with McKnight et al's review, consisting of conceptual frameworks, models, and scales in the domain of inter-personal, inter-organizational, and inter-firm trust. He notes the non-transferability of several results from studies on trust between two persons or individual level trust, and trust within a group, to individual's trust on an online firm.

McKnight et al's 68-item trust scale is very comprehensive and is based on a model that marries sociological, psychological, and social-psychological trust factors with the framework of the Theory of Reasoned Action (Fishbein and Ajzen, 1975). McKnight et al (2002) identify "disposition to trust", "institution-based trust", and "trusting beliefs" as antecedents to trusting intentions to engage in trust-related Internet behaviors. The authors define disposition to trust as the "extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons."

Institution-based trust (substitute Internet-based trust) is defined as “the belief that the needed structural conditions are present to enhance the probability of achieving a successful outcome in an endeavor such as e-commerce.” Trusting beliefs means “the confident truster perception that the trustee (e.g. business, government) has attributes that are beneficial to the truster.” Trusting intentions is the outcome and the construct is defined as “the truster is securely willing to depend, or intends to depend, on the trustee.”

In contrast to McKnight et al’s (2002)’s trust scale, Bhattarcharjee (2002) proposes a 7-item scale whose number is determined in a range through use of the Spearman-Brown prophecy formula. Smaller scales are always more desirable. However, trust in the context of e-business is complex, and the parsimony of the scale raises concern of over-simplification. For example, the ranges of privacy invasion and fair practices are fairly broad and can hardly be captured in the one item as proposed in Bhattacharjee’s pilot scale: “ Amazon is fair in its use of private user data collected during a transaction”.

Bhattacharjee’s trust measurement scale, similarly to McKnight’s (2002) depends on the aforementioned trust bases of ability (competence), integrity, and benevolence. He succinctly situates the three dimensions in the context of e-commerce and justifies the addition of 5 new items to existing scale items, including that of privacy of personal data. When situating integrity in the e-commerce domain, Bhattacharjee (2002) states “ in e-commerce, the rules of integrity refer to (1) conduct of online transaction, (2) customer service policies following a transaction and (3) firms’ use of private user information.” Unfortunately, Bhattacharjee (2002) dropped the privacy-related item from his trust scale after a single pilot experiment with 147 graduate MBA students as responders and Amazon.com as subject. Bhattacharjee fairly points out that the respondees may not have had any means to evaluate Amazon’s fairness of use of customer data and may have underweighted those items. Additionally, Amazon is a well-known, branded online company with many reputation-sharing and structural assurance mechanisms in place. We have concerns as to whether Bhattacharjee’s scale could cover fundamental trust issues when an inexperienced Internet shopper is transacting online with, say, a small Canadian small-and-medium sized enterprise (SME) in Nova Scotia for the first time. Bhattacharjee’s confirmatory study with the online customers of the largest national bank in the United States situates his work in the area of trust in big online businesses.

It is intuitively clear that online trust is more of an issue for the unknown SME than for the web channels of big business, and that online trust can be sector related. Trust in terms of privacy of data is always high for your financial institution – you have a history of giving it your personal information. In fact, Bhattacharjee reports that trust only accounts for 13% of why his respondees were willing to transact online. Whereas the GVU 1997 survey showed that 53 percent of online users do not trust commercial web sites collecting data, 66 percent do not register on online sites in fear that their data may be used inappropriately, and 40 percent falsify data when registering online [GVU98]. According to many reports (e.g. Ivis 2001), building online trust is the major hurdle that business entrepreneurs climb when trying to create an online customer base. Some researchers (e.g. Chellappa and Pavlou 2002, McLeod 2002) consider privacy as a sub-construct of trust and indeed privacy is similarly complex and, like trust, the responsibility for its provision lies on business, user (customer, citizen, employee), community, and government intervention mechanisms.

2.2 Stakeholders and Their Interventions for Trust and Privacy

Figure 1 illustrates the result of our stakeholder approach to creating an online trust and privacy model for electronic business. The arrows on the diagram represent the relationship “is an antecedent of”. The left hand side (LHS) of the model, shown to the left of the slanted broken line, is new to McKnight et al's model and represents the stakeholders. The RHS of the model is most of McKnight et al's (2002) trust model. For describing the different sources of stakeholder (business, government, user) interventions for trust, we separate business interventions for trust out of the "trusting beliefs" construct in McKnight's (2002) trust model.

The following discussion illustrates how privacy is a common thread throughout all stakeholder interventions for trust. In the online environment, businesses raise user perceptions of security, privacy, and trust by using semantic cueing mechanisms such as trust and/or privacy seals, closed lock/open lock icon, and opt-in versus opt-out policies (Adams 2000). While scientists may objectively measure how much security or privacy may be present in an online transaction, it is the individual's subjective perception of the security of their transaction or personal information that is critical to online trust. Perceived information security is studied in Chepalla and Pavlou (2002), where they define the construct as "the subjective probability with which consumers believe that their personal information will not be viewed, stored, or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations".

Furthermore, Chellappa and Pavlou (2002) empirically verified that the control mechanisms of *encryption (e.g. SSL, PGP)*, *protection* (e.g. through firewalls, presence of privacy policy statements), *verification* (e.g. identity of online store through familiarity with domain names), and *authentication* (e.g. through digital certificates /third parties), employed in e-business, positively influence consumers' perception of security, and thus enhances e-commerce trust.

Government/association and community interventions for trust building include policy making around trust issues, legislation, collaboration in chamber of commerce trust seals, endorsement of TTP authorities, support for PKI infrastructure, adoption of e-government, outreach programs for online trust education, and management of trust content (Jutla 2002).

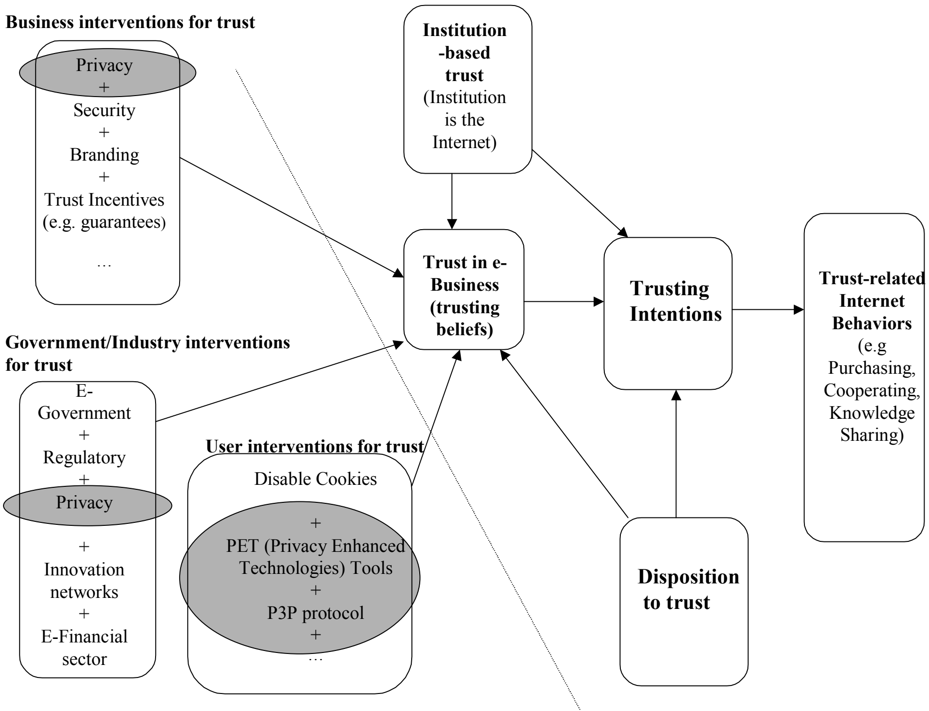
Business interventions for trust
Privacy
+
Security
+
Branding
+
Trust Incentives (e.g. guarantees)
…
Institution -based trust (Institution is the Internet)
Trust in e-Business (trusting beliefs)
Trusting Intentions
Trust-related Internet Behaviors (e.g Purchasing, Cooperating, Knowledge Sharing)
Government/Industry interventions for trust
E-Government
+
Regulatory
+
Privacy
+
Innovation networks
+
E-Financial sector
User interventions for trust
Disable Cookies
+
PET (Privacy Enhanced Technologies) Tools
+
P3P protocol
+
…
Disposition to trust

***Figure 1:** Stakeholder Model for Online Trust and Privacy*

Today, many uncomprehending users are unconsciously protected by the fragmentation among data/information collected by various businesses within a sector and among sectors. Preventing business from constructing complete user data profiles can be achieved by pseudonymity, non-collaborating businesses, cookie crushers, and anonymizers, to name a few.

3. Value Model vs Revenue Model

A revenue model forms part of the definition of a standard business model. Using approaches such as customer lifetime value, the value of personal data can be calculated and sold on the name list market. Magourik (2001) provides an insightful calculation that may value the customer share of his/her personal information asset at under three dollars at year's end if he/she made over $75000 annually, bought over $100.00 from the same catalog, and the name is sold a 100 times that year. However, users are not interested in such economic advantage when it comes to their private data (3 dollars is not worth the user's time spent managing his/her private data). An economic incentive is not unimaginable, however. For example, businesses may offer the user/customer coupons, discounts, points, free promotional offers, or other monetary rewards to electronically update customer or lead data. These rewards may add up to considerably more than $3.00 a year, especially if businesses provide user incentives to automatically fill-in electronic surveys. To prevent repetitive consumption of a user's time, we expect personal P3P-based software agents (agents that are more sophisticated than available now) may do update tasks transparently on a schedule that is pre-approved by the user.

Incentives with strategic value to the customer should also be considered. An example of one strategic benefit to the user or consumer is that if he/she has some control over the marketing of a name, then through contractual terms, companies may agree to trade the name only with other companies that will deliver information that is useful to the user.

Surveys show that the current user perspective towards giving up private data leans towards the strategic value of the customer directing his/her own personalization as opposed to the monetary incentives gained from direct sales of the customer's name and other information. From the Spring 1997 Nielsen Media Research/CommerceNet Internet Demographics Study and the 1997 GVU 7th WWW User Survey, Novak et al confirm that users in 1997 did not view their personal data in the context of an economic exchange of information. In addition Novak et al (1999) find more than two-thirds of respondents were uninterested in selling their data for monetary incentives or access privileges. Rather the web users wanted another type of exchange " one characterized by an explicit social contract executed in the context of a cooperative relationship built on trust." Kobsa (2001) reports that 31% (GVU 1998), 30% (Forrester 1999), and 51% (Personalization Consortium, 2000) of web users "are willing to give out personal data for getting something valuable in return." Thus, an e-privacy business model currently requires more emphasis on a value model definition rather than a revenue model definition.

The concept in adsertor marketing – "in which a consumer owns their name as a transferable asset as well as the marketing, financial, and demographic information attached to it Magourik (2001)" – may be significant in creating a value model for the user. Through electronically negotiated contracts, perhaps by a user's P3P-based agent, the user can agree to let a business use method-oriented personalization strategies, such as on-time tailoring, affirmative customization, individual-analysis, or pseudo-decision, for a value exchange. From the business perspective, self-reported customer information has a much higher strategic and quality value than data culled through databases' syntheses. Companies spend large amounts of money each year buying "fresh" user data and surveying their potential and existing customer base through expensive paper mail. Obtaining the ability to "go directly to source" electronically by negotiating with users and/or their agents may have benefits for business such as higher online survey response rates, compliance with privacy laws in the user's country, and eventually may have economic benefits with respect to data collection and legal costs. In turn, incentive mechanisms are extended to reward the customer for quality management of his/her data and also for solicitation of new data.

The next section examines the third descriptor of a privacy business model: the privacy architecture, containing the privacy information and transaction flows. We illustrate how agents are key to implementing an e-privacy business model.

4. ePrivacy Architecture with Enhanced User Control

Specifically, a value model for the user's e-privacy will be realized when easy-to-use and reliable privacy software become available to allow the customer, citizen, or patient to exert control over (1) how his/her data is used, (2) what length of time can his/her data be stored and used, (3) where the data is stored, (4) when the data is stored/updated/deleted, (5) who uses the data, and (6) why the data is being used.

At present, the consumer has no aggregated means of knowing whether a company is complying to privacy legislations in any of the 6 ways listed above. Many businesses bend rules such as those governing length of use of personal information. Even when the customer is given the option to delete personal data from a site, privacy groups such as the Denver-based Privacy Foundation have shown that several businesses delay the deletion, and thus maintain personal records for unspecified lengths of time afterwards (EPIC 2000). Companies using third party technologies to obtain personal data often store data on third party servers without the knowledge or permission of the customer.

Because of the potential for sifting large amounts of information, automated user agents will need to aggregate information and flag concerning items for the user's attention if detecting that the user's privacy preferences are not being met.

The agent-based P3P specification provides the base ideas/specifications for building an infrastructure upon which an architecture can be built. It specifies how resources, site policies, and user preferences can be expressed using XML, RDF (*R*esource *D*escription *F*ramework), and APPEL (*A P*3P *P*reference *E*xchange *L*anguage) but it does not specify a privacy architecture that would guide the development of agents which provide the desired functionalities. The P3P platform specifies general guidelines that should be followed when building such agents. Version 1.0 of the P3P specification was approved in April 2002 as a W3C and cross-industry recommendation for its widespread use as a platform for providing a measure of user control over privacy preferences.

Automated privacy critics, or iCritics, form one P3P-based mechanism that can add value to the user's privacy management tools. Noting the complexity of the privacy space, Ackerman and Cranor (1999b) propose semi-autonomous agents, iCritics, that can help users protect their privacy information. Privacy critics are agents that alert the user with warnings about potential privacy problems. A privacy critic could warn the user about what sensitive information is being revealed as the user surfs or fills out web forms, for example. Another example supported by Ackerman and Cranor is that a privacy critic could make a user aware that a site that they are visiting is on a warning list at reputable associations such as the BBBOnline.

Our proposed e-privacy architecture will thus consist of intelligent agents and their interaction and access to privacy repositories containing private data and privacy control information. The fundamental design approach that we use is to assign distinct agents to well-defined but distinct tasks. This approach facilitates security provision, by securing smaller and thus less complex components. It also leads to clear interfaces and protocols for agent interaction and thus support flexibility, expandability, and openness.

4.1 Privacy Information and Transaction Flows

To facilitate the perception of enhanced user-control and focus, and thus increase the user's trust in the privacy platform, we depend on familiarity and exploit the user's trust in her usual computing platform. This is likely to be a *personal computer* (PC) over which the user has complete control, or a workstation on a local network, for instance an office system she interacts with on a daily basis, that she trusts and with which she is comfortable. We shall refer to this "home" computing platform as a semi-secure but *trusted site* and it is used as the base platform for the privacy architecture described here. Thus, user agents (and not the external service agents) and repositories are based/located on this trusted platform. It should be noted that this trusted site is not to be confused with the trusted third parties (TTPs) of other approaches, for instance (Cingil 2002) that force the user to log onto a TTP solely for the purposes of storing and handling personal profile/personae information – a TTP that the user does not access or utilize for other purposes and thus is not familiar and comfortable with. In our approach, the user may delegate some of the private information and preferences to a TTP for the purposes of, for instance, access to web-services from remote sites or mobile devices, but this is strictly optional and distributing information among TTPs is under the user's control. As is done in other privacy architectures and/or models, it is assumed that the user utilizes one or more *anonymizers* when accessing web sites and her (the user's) identity should not be revealed through the use of the user system's URL. Indeed, ours is a hybrid, but heavily client-side, approach that depends on not one but multiple trusted third parties. We also assume the complementary use of security algorithms such as encryption and mix algorithms for specific security purposes.

The e-privacy architecture must support the following privacy-related transactions:

- interact with third party agents (e.g. service-site agents) or external Internet privacy agents (e.g. along the lines or iCritics)
- negotiate privacy contract by comparing the site's proposal to the user's preferences and possibly following the guidance from the user
- store and manage preferences and contracts, user private data and personae, service-site data, audit trails, historical data, and rewards
- negotiate with other entities for the sale or distribution of private and collected data

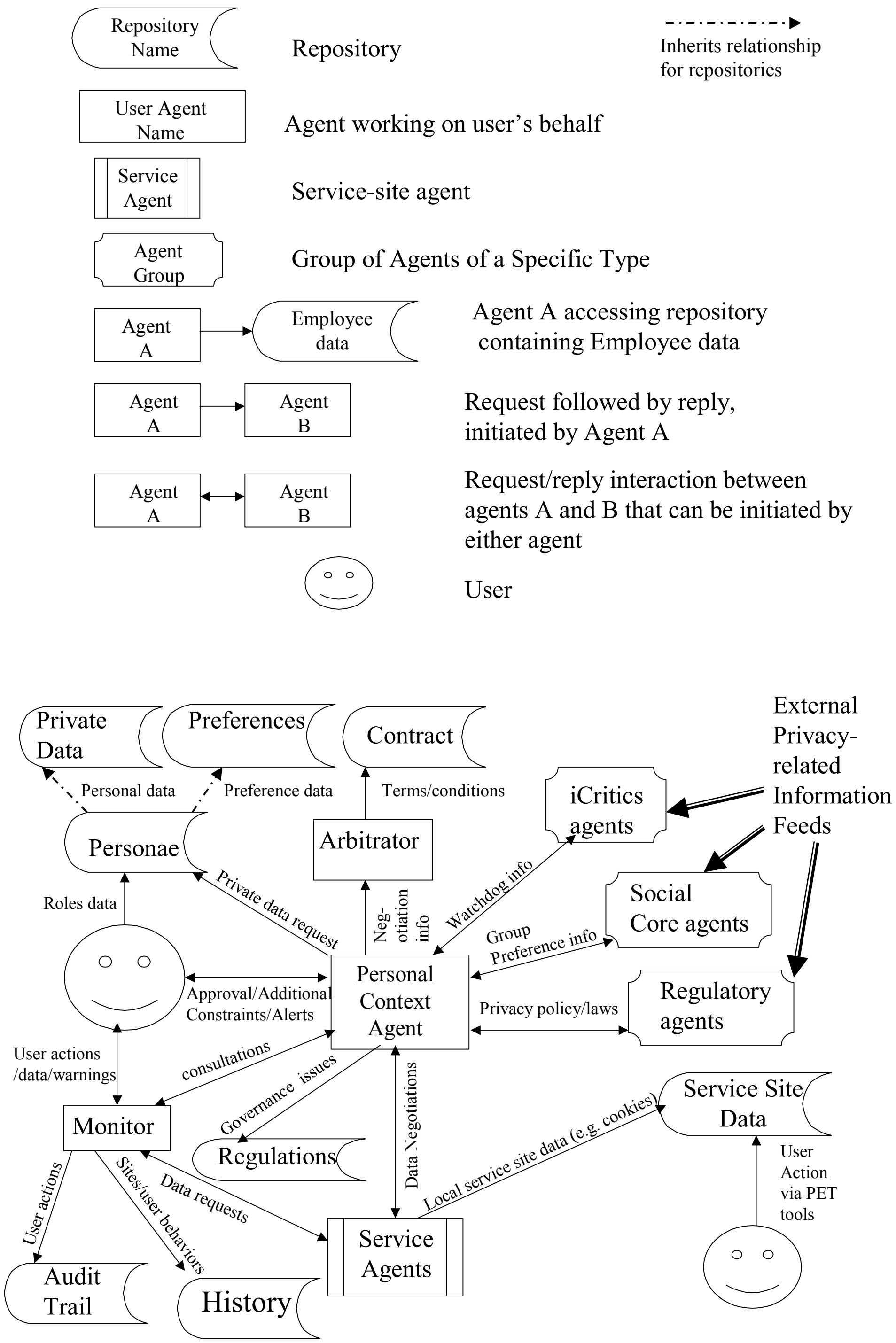

Figure 2: *Architecture for User Controlled e-Privacy*

The architecture of cooperating agents, shown in Figure 2, supports the transactions required in an e-privacy business model. The figure shows transactional and privacy information flows, interactions between the user and stakeholder agents, and access to repositories. Agents are either external or internal. As the name indicates, internal agents execute on the user's trusted system and some of them have access to the various repositories. There are two types of external agents. One type, *service-site agents,* located at the service sites, provide the user with services by interacting with the user or the user agents – it is this interaction that requires private information to be supplied by the user and for which the supporting privacy mechanisms are provided. The other type of agents effect trust intervention mechanism by the government. Community, association, and business stakeholders. Three representative agents are shown, iCritics (Ackerman and Cranor, 1999b), Social Core (Kaufmann and Powers, 2002), and Regulatory agents. It should be noted that in (Ackerman 1999b) the term iCritic agent refers to either internal or external agent that supports the user privacy. We use the term in a more restrictive sense to refer only to external agents that provide information on service sites that can be used by user privacy mechanisms. An already cited example is an iCritic agent monitoring reputable associations, such as the BBBOnline, providing information on a site in terms of complaints by customers. Social Core agents provide provide the user assistance with setting-up privacy preferences by providing preference recommendations for various activities. For instance, an agent representing PTAs may provide recommended privacy settings to be used by children. Of course, the Social Core agents have also other roles in terms of extending their influence on the service sites as described in (Kaufmann and Powers, 2002) but this is out of scope of this paper. Regulatory agents also provide assistance to the user in terms of regulations that apply in different privacy regions/countries so that the user agent(s) could adjust privacy preferences accordingly and the user could take appropriate actions in terms of managing her private data collected by service sites.

The *personal context* agent maintains context within which the user operates, controls the negotiation of the contracts with sites depending on the context, provides the user with information on the context and her action, and seeks guidance/instructions from her related to negotiations and context. The *arbitrator* agent has a straight-forward role. It takes a site's proposal(s) and user's preferences to determine whether or not privacy contract can or cannot be established with the accessed service site. The *monitor* agent guards the user from unintentionally revealing private data that she did not intend to reveal according to the negotiated contracts. The monitor observes the user's actions, what is input in forms and controls selected, and reports this to the *personal context* manager that actually determines whether or not to interrupt the user's activity and solicits guidance from the user. The revenue agent keeps track of rewards and with guidance from the personal context agent determines whether the incentive will be accepted. *Anonymous* (2003) detail the roles of the user agents.

We make distinctions among the terms persona, also known in the literature as a "face" (Lederer 2002), private data, and preferences. Private data includes information about the user, information that may be genuine or fictitious. For instance, the user may have three different addresses, two real, while one fictitious, and two pseudonyms containing information about two persons, one real, one fictitious. Furthermore, private data also includes meta-data that describes it. For instance, meta-data may describe properties such as whether data is genuine or fictitious, or whether it is health related or whether it is a personal preference such as liking motorcycles.

Preferences describe the user's privacy rules for access to the private data. The user may prepare different preferences to the same data for different personae.

Persona is a collection of private data, preferences that define privacy for that data, plus other information that is used for determining what private data may be used for the persona and which preferences may be used in accessing its data. For instance, a persona may have an attribute that specifies that only fictitious data may be present, while another attribute may place restrictions on what preferences may be used for access to the data.

Figure 2 shows several repositories, most with obvious contents: *private data, preferences, personae, contracts, service-site, history, regulations,* and *audit trail* repositories. Private data and preferences repositories are obvious in that the former stores the private data that are provided to service agents while the latter contains user preferences for negotiation of contracts. The personae repository contains information about composition of personae in terms of private data and privacy preferences. This is shown in diagram through inheritance relationship.

Contracts that were negotiated with sites are stored in the contracts repository while the regulation repository contains regulations that were used in forming privacy preferences. The history repository stands for a number of repositories storing historical information on user's behavior such as navigational history (click-stream) stored, perhaps, in an aggregated form(s). The audit-trail repository stores history of negotiations, usage of negotiated contracts and delivery of private data to service sites. The service-site repository contains information, for instance cookies, stored on the user's system by service sites' agents.

Service-site agents can access the service-site repository to store and retrieve information such as cookies. It is expected that in the (near?) future users will be not be willing to allow service-sites to store information on their systems without having control over what that information is, that is without having the ability to examine and potentially edit this information. Eventually, standards will be developed on how such information is stored, in a form of XML documents, so that a user will be able to examine, modify, or delete such information or portions there of. Safeguards must be in place to ensure that one service-site agent cannot access information stored by agents of other service sites.

The audit-trail repository is used to record all activities executed by agents on the user's behalf. It is explicitly included as part of the design. The user should have the ability to not only review contracts, but also her behavior, use of personae, data provided to sites, and how data that she explicitly provided to sites conforms to her privacy preferences. This is shown as a history repository but, clearly, additional data mining tools would be useful (although not shown) for knowledgeable users who are interested in their on-line behavior and past use of their private data. Inclusion of auditing and control facilities into the design is viewed as crucial in increasing the user's awareness of privacy issues and also trust and thus increase the adoption of e-business in general.

5. Related Work

Advances in privacy is most likely to be reached through the collective efforts of privacy advocate groups, business, associations, community, government, and users. Needed are increased privacy literacy and availability of tools and models with unique functionality to users. Studies (e.g. Riegelsberger and Sasse, 2001) show that new Internet users mainly rely on recommendations, brand familiarity, and reputation mechanisms to determine a site's trustworthiness. Trust models such as McKnight's (2002) and Bhattacharjee's were discussed in section 2. Other trust models exist as part of other models such as Lee, Kim, and Moon's (2000) model of e-Commerce loyalty, but their view of trust is oversimplified, and their identification of antecedents for customer loyalty is very sparse considering the richness of the marketing literature on customer loyalty sub-constructs and measures. Robles et al (2001) approach the identification of trust dimensions from such a multi-disciplinary viewpoint but restrict attention to agent-based applications. The work concludes "as trust is domain dependent, it is hard to find a model that is suitable to all applications." Robles et al (2001) identify three trust dimensions for agents: type of control, policy provider, and mechanism provider. Each dimension is graduated on a three-point scale. Control is decomposed into none, direct, and indirect. The policy provider is categorized into "none", " individual", or a "group", capturing subjective trust towards the individual or agent, and objective trust in a group. The mechanism provider represents who provides the trust mechanism and is divided into "no party", "1st and second hand parties", and "third party".

Tan and Thoen (2001) propose a trust model that focuses on two types of transaction trust: party trust and control trust. Party trust is the trust in the other party involved in the transaction. Control trust is the trust in a control mechanism. Example control mechanisms can be objects such as a letter of credit from a reputable institution, or procedures such as a rental car company documenting all the dents on a rental car before you drive it off the lot. Tan and Thoen (2001) provide arguments that support the literature that claims that "control" complements other (subjective and objective) trust components to increase trust (Beamish, 1988, Bons, 1997, Ganzoroli et al, 1998, Holland and Lockett, 1998). Although other viewpoints criticizing the complementary, additive relationship between control and trust exist (Das and Teng, 1998), Tan and Thoen (2001) provide examples that show how control-trust is more relevant to e-commerce activities involving international trade, and for e-commerce infrastructure mechanisms involving the use of the control-procedure oriented protocols such as SET. In international trade, for example, personal trust is hard to establish, and hence trust is established through use of letters of credit and other complex certification procedures (Tan and Thoen, 2001). Such control procedures that are used to establish trust fall under the category of Web vendor or business interventions to increase trust.

The work that most resembles the architectural portion of our e-privacy business model is the iManager architecture that contains databases for personal data, personas, URLs, and rules (Jendricke and Gerd tom Markotten, 2000). The iManager does not provide a revenue/or value model to support user adoption. It does not support significant stakeholder feeds. However, a proposal for interfaces to the personal management system is made. Usability results are not yet available for the iManager to the best of our knowledge. It does not describe how the control of the personal identity is affected by the external entities/stakeholders. For instance, (Lederer, 2002) describes a conceptual model of privacy in which they propose a metaphor called a situational face. Depending on the situation/context, a user adopts a face which determines, amongst others, user's data made available to interacting party(ies) and also the user's attitude and behavior.

Several proposals exist for TTP storage of user profiles and preferences. A proposal to access a user profile, anywhere and anytime, through any device, is described in (Cingil 2002). The user is required to do a browser-login to the TTP and her surfing behavior, click-stream, is monitored and captured locally and used to update the user's profile. The updated user's profile is uploaded to the trusted authority. When a user visits a site, an agent/proxy negotiates with the server's agent to determine how much of the user's profile information should be provided to the server. The major problem is the centralized and authoritative approach that does not allow the user control over the collected information. Many users prefer their profiles to be fragmented across many devices since fragmentation provides a form of privacy protection on its own, similarly to un-synthesized databases. Thus, another problem is that both user profiles and privacy preferences are stored on the TTP site. In our approach, a user can use different TTPs, including her own system, for different purposes; or different TTPs for similar activities while storing different personae at different TTPs. To help the user keep track of which TTPs have which personae, the user site or one designated TTP is used to keep track of such information, akin to a high level directory. Protection is in the distribution and fragmentation inherent in redirection through multiple TTPs and anonymizers.

Pfitzmann and Waidner (2002) describe technical protocols for the browser-based exchange of privacy attributes. Initial implementations, as are currently evidenced, include P3P user agents and proxies, compact and non-compact policy generators, editors, and checkers, and tools and libraries for developers. Please see www.w3.org/P3P/implementations for a complete listing of initial P3P based implementations.

6. Summary and Conclusions

Enabling the *user* to control the collection and management of her data collected when (s)he accesses e-services over the web requires a workable e-privacy business model. Such a model based on the P3P privacy platform is developed in this paper. We describe target markets and stakeholders, a value model, and a supporting transactional architecture for a proposed e-privacy business model. We design the entire business model for e-privacy from the user perspective. For example, users and organizations are unwilling to hand over the control over private/personal data to one single trusted third party (TTP), such as MS Passport, and hence the proposed privacy architecture is based on the user's familiar local computing platform and fragmentation among user-selected TTPs. Indeed, Kobsa (2002) in his recommendations for future directions in e-privacy recommends that "client side instead of server-side personalization would give users exclusive control of all purposely collected personal data as well as all processes that operate on these data. Analyses of the functional privacy and data requirements have led to a client-side architecture consisting of a collection of collaborating agents, with distinct and separate tasks, that access a number of supporting repositories. The openness of the architecture also supports evolution of functionalities to support the various foreseen and yet unforeseen requirements stemming from new laws, regulations, and ethical standards and policies that are emerging.

From the most recent surveys, the proposed revenue or value model for e-privacy reflects user-opinion on what is of importance or value to the user. Stakeholders in privacy have declared themselves in many ways. Governments in conjunction with private sector around the world are working on initiatives to break the trust barriers to e-commerce adoption in their SMEs. A market for user-based privacy enhancing technologies and tools is emerging and these tools will enhance our user-focused e-privacy business model. The target market for our proposed e-privacy business model is the growing group of users that want to have more hands-on, effective control over their online privacy. With qualitative arguments, we place online privacy as an antecedent to the online trust necessary for users to engage in Internet behaviors, thereby building on Fishbein and Ajzen (1975) theory of reasoned action, and extending McKnight et al's (2002) works on online trust.

References

Ackerman, M.S., Cranor, L., Reagle, J. (1999), Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. Proceedings of the ACM Conference in Electronic Commerce: 1-8, 1999

Ackerman, M. S., Cranor, L., (1999b), Privacy Critics: UI Components to Safeguard Users' Privacy, CHI, 1999.

Ackerman, M, Darrell, T., and Weitzner D.J. (2001), " Privacy in Context", Human Computer Interaction, 16, pp. 167-176, 2001

Adams, A. (2000), Multimedia Information Changes the Whole Privacy Ballgame, Proceedings of the Tenth Conference on Computers, Freedom, and Privacy: Challenging the assumptions, " Toronto, Canada, April 2000.

Adams A., and Sasse, A. (2001), Privacy in Multimedia Communications: Protecting Users, Not Just Data. In A. Blandford et al (eds.): People and Computers XV – Interaction without Frontiers. Joint proceedings of the HCI2001 and ICM2001, Lille, Sept. 2001, pp.49-64. Springer. http://www.cs.ucl.ac.uk/staff/A.Sasse/pub.html.

Ajzen, I. (1991), "The theory of planned behavior", Organizational Behavior and Human Decision Processes, Vol. 50, pp. 179-211.

Anonymous 2003; Architecture for User-Controlled e-Privacy , ACM Symposium on Applied Computing, Electronic Commerce Track, Melbourne, Florida, March 9-12, 2003.

Beamish, P. Multinational Joint Ventures in Developing Countries. London: Routledge, 1988.

Bons, R.W.H, Lee, R.M., and Wagenaar, R.W., Designing trustworthy interorganizational trade procedures for open electronic commerce. In Global Business in Practice, Tenth International Bled Electronic Commerce, Bled, Slovenia, June 9-11, 1997, pp. 39-69.

Bhattacharjee A. (2002), "Individual Trust in Online Firms: Scale Development and Initial Test," Journal of Management Information Systems, Summer 2002, Vol. 19, No. 1, pp. 213-243.

Chellappa, R. and P. A. Pavlou (2002), "Perceived Information Security, Financial Liability, and Consumer Trust in Electronic Commerce Transactions*," Journal of Logistics Information Management*, Special Issue on 'Information Security', (forthcoming).

Cingil I. (2002), *Supporting Global User Profiles Through Trusted Authorities*, SIGMOD Record, Vol. 31, NO. 1, March 2002, 1-17.

Coyle K. (1999), "P3P: Pretty Poor Privacy? A Social Analysis of the Platfrom for Privacy Preferences (P3P)", at http://www.lcoyle.net/p3p.html, June 1999.

Craig J. and Jutla D. (2001), "e-Business Readiness: a Customer Focused Framework" Addison Wesley, Boston, USA.

Cranor, L.F., Reagle, J, Ackerman M.S. (1999), "Beyond concern: Understanding net users' attitudes about online privacy" In Proceedings of the Telecommunications Policy Research Conference; http://www.research.att.com/library/trs/TRs/99/99.4/99.4/99.4/

Darrell T., Gordon G., Harville M., and Woodfill J. (2000). Integrated person tracking using stereo, color, and pattern detection. International Journal of Computer Vision, Vol. 37, No. 2, pp. 175-185.

Das, T.K., and Teng, B.-S. (1998), Between trust and control: Developing confidence in partner cooperation in alliances. Academy of Management Review, 23, 3 (1998), pp 491-512.

Dey A. K., Ljungstrand, P., Schmidt A. (2001), "Distributed and Disappearing User Interfaces in ubiquitous Computing, " CHI Conference Companion at the Conference on Human Factors in Computing Systems, CHI' 2001, March 31-April 5, 2001.

EPIC (2000); “Pretty Poor Privacy: An Assessment of P3P and Internet Privacy”, Electronic Privacy Information Center, June 2000, at http://www.epic.org/Reports/prettypoorprivacy.html, viewed on September 2001.

Fed (2000);. A U.S. Federal Trade Commission report to Congress, “Privacy Online: Fair Information Practices in the Electronic Marketplace,” May 2000, at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf, viewed on September 2001.

Fishbein, M., and Ajzen I (1975)*., Belief, Attitude, Intention, Behaviour: An Introduction to Theory and Research.* Boston: Addison Wesley.Forrester 1999; The Privacy Best Practice. Forrester Research, Cambridge MA (1999)

Ganzaroli, A., Lee R., and Firozabadi, B., The role of trust in design of trustworthy trade procedures,. In Proceedings of the Workshop on Deception, Fraud, and Trust in Agent Societies. Autonomous Agents Conference, Minneapolis, pp. 73-87.

GVU’s 10th WWW Survey. Graphics, Visualization, and Usability Lab, Georgia Tech, 1998, http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/

Holland C.P., and Lockett A.G. (1998), Business trust and the formation of virtual organizations. In Proceedings of the 31st Annual Hawaii Conference on Systems Sciences, IEEE Society Press, 1998, pp. 602-611

Hui, M.K., Bateson, J.E.G. (1991), “Perceived Control and the Effects of Crowding and Consumer Choice on the Service Experience,” Journal of Consumer Research, Vol 18, Sept. 1991, pp. 174-184.

Ivis, M, (2001); “Analysis of barriers impeding e-Business adoption among Canadian SMEs, a Canadian e-Business Opportunities Round Table Report, March 2001.

Jendricke U., and Gerd tom Markotten,D. (2000), “Usability meets Security – The Identity-Manager as your Personal Security Agent for the Internet.” 16th Annual Computer Security Applications Conference, 11-15, 2000, New Orleans, Louisiana.

Jutla D., Bodorik P., Dhaliwal, J. (2002), “Supporting the e-Readiness of Small and Medium Sized Enterprises: Approaches & Metrics”, Internet Research Journal: Electronic Networking Applications and Policy, Vol. 12, No. 2, pp. 139-164, 2002.

Kaufmann, J., H. and Powers, C. (2002), “The Social Contract Core”, WWW 2002, May 7-11, Honolulu, Hawaii, USA, 210-220.

Kobsa A. (2001), “Tailoring Privacy to User’s Needs,” 8th International Conference on User Modeling, Southofen, Germany, http://www.ics.uci.edu/~kobsa/papers/2001-um01-kobsa.pdf.

Kobsa A. (2002), “Personalized Hypermedia and International Privacy,” Communications of the ACM, Special Issue on Adaptive Web Systems and Adaptive Hypermedia, May 2002.

Lee, J., Kim, J., Moon J.Y. (2000), What makes Internet users visit cyber stores again? Key design factors for customer loyalty. Proceedings of the CHI’2000, The Hague, Amsterdam, pp. 305-312.

Lederer S., Dey A.K., and Mankoff J. (2002), “A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments”, Intel Research Berkley Report IRB-TR-02-017, Intel Corporation, Available at http://www.intel-research.net/Publications/Berkeley/120520020944_107.pdf, viewed on January 2003.

Lumeria, (2002), available at www.lumeria.com, viewed on May 2002.

Magourik J. (2001). Partners in Privacy. Viewed on January 2003, Available at http://www.intelligententerprise.com/010918/414feat1_1.shtml?ebusiness.

Markoff J. (2002), "Microsoft has shelved its Internet Persona Service", The New York Times on the Web, available at http://www.nytimes.com/2002/02/11/technology/ebusiness/11NET.html?pagewanted=print, viewed on May 2002.

McKnight, D.H., Choudhury, V., Kacmar, C. (2002), "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," Information Systems Journal, 2002, *forthcoming*.

McLeod E. (2002), "An empirical analysis of trust from a business perspective," work-in-progress report, Dept. of Finance and Management Science, Saint Mary's University, Halifax.

Novak, T.P., Hoffman, D.L., Peralta, M. (1999), "Building consumer trust online, *Communications of the ACM,"* 42, 4:80-85.

Patrick, A., Kenny, S. (2002), "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions," July 2002, available at http://www.iit.nrc.ca/~patricka/legint/from_legislation_to_interface.pdf, viewed on July 2002.

Personalization Consortium 2000; Personalization and Privacy Survey. Personalization Consortium. Edgewater Place, MA (2000), http://www.personalization.org/SurveyResults.pdf.

Pfitzmann, B., Waidner M. (2002), "Privacy in Browser-Based Attribute Exchange," Research Report, IBM Research, Zurich Research Lab, available at http://www.research.ibm.com/privacy, viewed on July 2002.

Riegelsberger, J., and M.A. Sasse (2001), "Trustbuilders and Trustbusters: The Role of Trust Cues in Interfaces to e-Commerce Applications, 1st IFIP Conference on e-Commerce, e-Business and e-Government, Zurich, Oct 3-5, 2001.

Smith H. J., Milberg, S.J., Burke, S.J.(1996) , "Information Privacy: Measuring individuals' concerns about organizational practices, MIS Quarterly, Vol. 20, No. 2, pp. 167-188, June 1996.

Spiekermann, S., Grossklags, J., Berendt, B. (2001), "e-Privacy in 2nd Generation Commerce: Privacy Preferences versus Actual Behavior," ACM Conference on Electronic Commerce, October 14-17, 2001, Florida, USA, pp. 38-47.

Tan, Y.-H., Thoen, W. (2001), Toward a Generic Model of Trust for Electronic Commerce", International Journal of Electronic Commerce, Vol. 5, No. 2, pp 61-74.

W3C P3P Guiding Principles (1998), at http://www.w3.org/TR/NOTE-P3P10-principles), last viewed on September 2, 2002

W3C Platform (1998), W3C The platform for Privacy Preferences, available at http://www.w3.org/TR/1998/NOTE-P3P-CACM), last viewed on September 2, 2002.

Wejchert, J. (2000) The Disappearing Computer, IST Call for Proposals, February 2000. Available at http://www.cordis.lu/ist/fetdc.htm. Viewed Feb 2001.

ZeroKnowledge, (2002), available at www.zeroKnowledge.com, viewed on May 2002.