Users’ concerns regarding privacy issues are lowering their trust in e-services and, thus, affecting the widespread adoption of online services. To increase users’ perceived control over their privacy, the authors propose a novel e-privacy architecture.

Privacy lobbyists and advocates have named privacy surrounding health information, mobility, and genetic information as some of the most significant issues of our time. Financial and behavioral privacy are also at stake. Even as governments around the world offer services requiring that our personal data be moved online and prepare to upgrade systems to share data among multiple agencies, privacy advocates are working double-time to encourage these governments to build privacy into their systems from the ground up. In an ideal world, there would be no conflict among privacy and e-commerce, high-quality healthcare, and the tracking of personal movement. But in reality, we haven’t achieved such balance, although multiple stakeholders in government, business, and the community aspire to this end.

In this article, we present the Personal Context Agent Networking architecture (Pecan) for e-privacy, which we developed to support users in making informed privacy-related decisions in the presence of uncertainty and across a variety of situations and interacting entities. Pecan is currently in prototype stage, and we’re working on some user interface details—specifically, adding natural language capability. We plan to release the experimental prototype in December 2005.

We provide a holistic picture of online privacy, identifying privacy’s position in trust and the applicability of a layered model in understanding the complex privacy domain. We apply the model to build a semantic-aware privacy Web ontology, associated external privacy Web services, a client-side user architecture for privacy control, and requirements of the computer–user interface to support user-controlled e-privacy.

**Increasing users’ control over privacy**

Philosopher Charles Fried stated that “privacy is not simply the absence of information about us in the minds of others, rather it is the control we have over information about ourselves…” (italics our emphasis). According to the Electronic Privacy Information Center (EPIC; www.epic.org), “Privacy protection is widely understood as the right of individuals to control the collection, use and dissemination of their personal information that is held by others. This central principle has been adopted in US law, privacy laws outside of the United States and many international agreements, including the 1980 OECD [Organization for Economic Cooperation and Development] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (www.epic.org/Reports/prettypoornotprivacy.html). Other OECD online privacy instruments exist, such as the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks (www.oecd.org/dataoecd/39/13/1840065.pdf) and the 2002 OECD Guidelines for the Security of Information Systems and Networks (www.oecd.org/dataoecd/16/22/15582260.pdf).

Thomas Novak and his colleagues at Vanderbilt University’s eLab (http://elab.vanderbilt.edu) explored links among user control, trust, and privacy, and their results from large user surveys show 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 that “concerns of
Online Privacy

control span secondary use of information.” The 1998 World Wide Web Consortium (W3C)’s Platform for Privacy Preferences (P3P) guidelines request developers of P3P agents to follow and support principles categorized into four groups: information privacy, choice and control, fairness and integrity, and security. The choice and control principle states: “Users should retain control over their personal information and decide the conditions under which they will share it.” These principles are also in accordance with the US Principles of Fair Information Practices.

Table 1 captures the seven C’s—our extensions to describe the control inherent in privacy guidelines such as the 1995 European Union Data Directive, Canada’s 2001 Personal Information Protection and Electronic Documents Act (PIPEDA), and the US Federal Trade Commission’s guidelines for privacy protection. We synthesize three initial control elements (comprehension, consciousness, and consent), from Andrew Patrick and colleagues’ work on human–computer interaction research in privacy at Canada’s National Research Council, and other constructs from user behavior theories to form the seven C’s. They’re intended to describe the ways in which users perceive they have some measure of privacy control; that is, through understanding, being aware, choosing explicitly, giving consent, adapting privacy rules according to context, setting limits, and anticipating the familiar through consistency.

**E-business and e-government**

Businesses and governments, apart from their ethical responsibilities to uphold privacy as a human right, seek to understand individuals’ behaviors as they shop online, collaborate online for work projects or in online communities, and receive e-services. User controls directly affect these behaviors. According to some scientists, perceived behavioral control influences whether people choose to pursue an outcome, their degree of preparation, the effort they expend, their perseverance, as well as the thoughts and emotions they experience during the task.

Relevant to e-business managers’ understanding of the importance of providing control to customers are findings in Michael Hui and John Bateson’s seminal work, which shows how perceived control is a crucial variable in mediating a consumer’s emotional and behavioral response to an offline service encounter. Hui and Bateson show that in a service encounter, any situational or interpersonal characteristics that increase consumers’ perceived control will positively affect emotional and, in
turn, behavioral responses to the encounter, affecting the consumer’s choice of whether he or she stays in the service situation or a service encounter between firms and consumers. Our stress on the importance of online privacy and trust is substantiated in David Gefen and colleagues’ work, which concludes that consumer trust is as important to online e-commerce as other technology acceptance moderators, such as perceived usefulness or relative advantage and ease of use.7

Businesses and governments must provide customers, partners, and users the means within e-business applications to set limits regarding how, what, why, where, and when data is collected or presented in each possible context, and to constrain who shares it.

A new trust model

Social science literature shows us that the higher the user’s perception of control over situations and data, the more trusting the user is when engaging in an online activity. Yet, user control remains among the most under-represented in online trust models; missing from these models is the strong effect of user control and the contribution of multiple simultaneous stakeholders such as community, business, and government in the trust environment. It is for this reason that we extend D. Harrison McKnight and colleagues’ online trust model8 with new constructs consisting of stakeholder interventions (IVs) to foster trust. Figure 1 illustrates the result of our multiperspective approach to creating an online trust and privacy model for e-business and e-government. The model’s left-hand side, to the left of the red line, is our contribution and represents the interventions multiple stakeholders use. The model’s right-hand side represents a large subset of McKnight’s online trust model—one of the first fully comprehensive and scientifically validated models for online trust.8 We use their definitions for the following constructs:

- **Disposition to trust** is 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 (or Internet-based trust)** is 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 trustee’s confident perception that the trustee (such as a business or government) has attributes that benefit the trustee.
- Trusting intentions is the outcome; the trustee is securely willing to depend, or intends to depend, on the trustee.

We define the new constructs as follows:

- User interventions (user IVs) for trust are the set of mechanisms under the user’s control that may be used to increase a user’s online trust.
- Business interventions (business IVs) are the set of mechanisms under a business’s or business partner’s control that may be used to increase a user’s online trust.
- Government interventions (government IVs) are the set of mechanisms under the government’s control, or that require the government’s participation, that may be used to increase a user’s online trust.
- Association interventions (association IVs) are the set of mechanisms endorsed by one or more industry associations, or that require an association’s participation, that may be used to increase a user’s online trust.
- Community interventions (community IVs) are the set of mechanisms endorsed by a community (ad hoc or otherwise) that may be used to increase a user’s online trust.

We studied user willingness to adopt P3P, user encryption, cookie crushers, anonymizers, and pseudonymizers; empirical results support that employing user intervention-type tools for privacy can significantly impact online trust. Our analyses show that relationships exist among user IV tools and users’ trusting beliefs and institutional-based trust. In addition, our results substantiate relationships between institution-based trust and trusting intentions, and institution-based trust and trusting beliefs. These results validate the user IV portion of our trust model and contribute to the growing maturity of online trust theory with respect to different groups of Internet users, particularly Ackerman’s pragmatic majority, and the small- and medium-sized business.

Privacy is a common thread throughout all IVs for trust. Businesses raise user perceptions of online security, privacy, and trust by using semantic cueing mechanisms, including business IVs such as trust or privacy seals, closed- and open-lock icons, and opt-in versus opt-out policies. While scientists can objectively measure how much security or privacy might be present in an online transaction, the individual’s subjective perception of the security of their transaction or PII is critical to online trust. Ramnath Chepalla and Paul Pavlou define the “perceived information security” 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.”

Chepalla and Pavlou also empirically verified that when e-businesses use control mechanisms such as encryption, protection (for example, firewalls and privacy policy statements), verification (identifying an online store through familiarity with domain names), and authentication (through digital certificates and third parties), they positively influence users’ perception of security and thus enhance users’ trust in e-commerce.

Government, association, and community IVs for trust building include legislation, developing policy around trust issues, collaboration in chamber of commerce trust seals, trusted third-party (TTP) authority endorsements, PKI infrastructure support, e-government adoption, outreach programs for online trust education, and management of trust content. Privacy watchdog associations also play a role in compliance and user confidence.

Today, many users are inadvertently protected because the information various businesses have collected is fragmented. Consumers can prevent business from constructing complete user data profiles by using privacy-enhancement technology (PET) tools, such as cookie crushers, pseudonymizers, remailers, and P3P-based agent solutions, are privacy intervention solutions (user IVs) currently available to users.

**Web-side privacy ontology for agents**

A Web privacy architecture must accommodate various legal regulations, cultural and ethical guidelines, and standards created by various industries. Thus, a Web privacy ontology will form a core part of an online privacy architecture and should incorporate a hierarchical nesting. Figure 2 represents a mixture of formal and legal laws and acts, informal guidelines and standards for the general population, and specific legislation and guidelines for interest groups.

**International and federal**

Intending to capture a tiered agent perspective, each concentric circle or ring in Figure 2 represents a layer provided by another tier of governance. Internationally, the World Trade Organization and the United Nations provide one type of privacy governance; at a national level, another type of privacy governance comes into play, and so on. Each ring has laws, guidelines, or standards associated with its governance tier. Consider Canada’s federal privacy tier: it contains two federal privacy acts, the 1982 Privacy Act, applicable to government institutions, and PIPEDA, which formally regulates businesses’ collection, storage, usage, and disclosure of consumers’ personal data. The Canadian privacy champion, the privacy
Online Privacy

commissioner, investigates complaints and also comments on public policies or legislation that could impact individuals’ rights to privacy. Canada’s Office of the Privacy Commissioner provides a comprehensive Web site (www.privcom.gc.ca) that provides a guide to business responsibilities for consumers’ privacy, outlining individual privacy rights protected under PIPEDA, rulings on privacy complaints brought to the commission, links to privacy tools, opinions on current issues, and annual reports with summary statistics on issues since its inception in 1983.

Illustrating guidelines provided at the federal tier, the Canadian government’s Privacy Impact Assessments (PIAs) is a best-practice policy that mandates that each government department and agency perform a detailed assessment of a service’s potential impact on online privacy before it can be offered online. The Office of the Privacy Commissioner receives the PIA results before it gives its approval. Businesses can similarly build privacy into their services from the ground up and appoint employees who are accountable for assurance.

Canada’s federal standards, also shown in Figure 2, include the Common Look and Feel (CLF) standards for the Internet. CLF standards 5.3 and 5.4 require two types of privacy notices on Canadian government Web sites: a general privacy notice must appear on every government Web site and specific privacy notices must be present on every Web page that collects personal data and before a cookie is placed on the user’s system. These standards complement the 1982 Privacy Act’s requirement to give the individual notice.

Communities and associations

At the communities’ levels, innovation networks and associations create policies, standards, and social contracts to provide structural assurance for online privacy and trust. Proposed P3P extensions to create social norms for policy preferences use novel approaches that involve stakeholders. The idea is to use technology to speed up an association’s view (such as a parents–teachers association) on policy preferences for its membership. IBM researcher James Kaufmann and his colleagues call this proposal the social contract core.14

In the business world, the World Chambers Network, a key international association for small and medium enterprises (SMEs), provides technology backbones and secure services to support online business to business (B2B) commerce between small member firms from 12,000 chambers of commerce across the world. The allied Vancouver-based Global Innovations Enterprise and Commerce Center, launched in December 2004, provides informational guidelines on privacy and active Chamber Seals for trust (www.chambergateway.net). Privacy watchdog associations such as EPIC and privacy advocacy groups play a key role in ensuring privacy compliance and alerting users to privacy concerns, in countries in which PII is self-regulated. All of these associations provide valuable informational and technological resources for compiling this “communities” ontology layer for the privacy domain.

Organizations

Organizations take privacy concerns seriously primarily because of litigation fears, ethical concerns, and potential for enhancing customer relationship management and human capital management services. Businesses can reduce litigation risks by using effective technical privacy mechanisms to prevent employees from violating privacy practices as posted in a company’s privacy policy. For example, database privacy mechanisms are aimed at helping employees comply with privacy regulation and the company’s stated privacy policies. Solutions include using
technical languages such as the Enterprise Privacy Authorization Language (EPAL), which is implemented in an IBM Tivoli monitor that sits in front of the database, intercepting user accesses, and using EPAL policy expressions to determine whether a user can access a particular data field. Complementary privacy-preserving data mining algorithms are also being commercialized to help protect against leaking or inferring information when personally identifiable PII data from various shared data sources are synthesized.

Businesses have many other intervention mechanisms for online privacy, such as online privacy seals, privacy statements coded in XML-based P3P to support P3P agents, and corporate privacy governance. The latter consists of business policies for risk management of loss of privacy data, assessment of privacy threats, and selection of security and privacy protocols according to industry standards.

**Our sociotechnical architecture**

Our client-side architecture of cooperating agents and Web-side privacy ontology architecture facilitates the perception of enhanced user-control and focus, and thus increases users’ trust in the privacy platform. The architecture supports and provides users with control over contract negotiation, retention of information in repositories, and interaction with external agents and privacy Web services.

Our e-privacy architecture must support several privacy-related transactions:

- interact with third-party agents, such as service-site agents or external Internet privacy agents (along the lines of the proposed iCritics, which could provide services such as alerting the user that a surfed site is on the Better Business Bureau blacklist for their handling of PII) and privacy Web services;
- negotiate privacy contracts between user and the organization, possibly with a human-in-the-loop approach as well as through agent automation;
- store and manage preferences and contracts, users’ private data and personae, service-site data, audit trails, and historical data; and
- manage user privacy preferences and contracts in context.

Figure 3 shows the architecture of cooperating agents, which supports the transactions required in an e-privacy business model. The figure also shows transactional and privacy information flows, interactions between the user and stakeholder agents, and access to repositories.

Users and, in particular, a regulatory agent, must refer to, consult, and be aware of the various laws, regulations, and standards created and maintained by governments, industries, associations, and communities. This motivates the creation of several key privacy services that our client-side regulatory agent would then invoke. For example, it could ask for a comparison of a privacy policy of a company’s subsidiary in Canada and a policy belonging to its parent company in the US. Web privacy services such as the three-way comparison among business, government, and user could also provide useful results that can be stored in our privacy architecture.

**Web privacy ontology services**

Integrating the ever-changing information and knowledge inherent to the mechanisms that cross each online privacy layer (such as federal, provincial, and sector-related) in public Web privacy ontologies is useful for all users and service providers. Thus, our Web privacy ontology must support such integration services. Other examples of services that depend on Web ontology infrastructure include performing a three-way comparison among user preferences, business practices, and government regulations. By adding P3P tags to the concepts in the Web privacy ontology, we invent a fat P3P-agent with three-way comparison capability. This comparison could help Internet users in several ways. Comparing the contents of P3P elements that represent business privacy practices and those that represent privacy law could result in highlighting to the user either omissions in the business’ P3P policy statements or concerns of mismatch of privacy legislation interpretation. Accessing privacy ontologies that contain P3P tags associated with concepts and relationships can also help users populate their preferences in a more informed way. Finally, a P3P-agent comparison of user privacy preferences and the corresponding concepts in a regulatory Web privacy ontology can flag user inattention to detail in the user preferences rule set.

**Agents**

Multiple computational software agents cooperate in our sociotechnical architecture to inform the user's decision-making on his or her online privacy. These agents are internal (on the client system) or external (on the Web).

**External agents.** There are two types of external agents: service-site agents provide users with services by interacting with them or their agents, and trusted third-party (TTP) agents effect trust intervention mechanisms by the government, communities, associations, and business stakeholders. Figure 3 shows two representative TTP agents: iCritic and social core. An example of an iCritic agent’s action is an alert to the user that the site to which the user has surfed is on the better Business Bureau’s online program (BBBO) blacklist. Social core agents use guidelines or standards that communities or associations create; they assist users by providing preference recommendations for various types of sites.

In most cases, each external TTP agent has a corresponding internal agent that interacts with the external agent and stores information relevant about the user and
his or her activities for localization purposes and subsequent use. Such information can also be provided to the personal context agent for immediate use. For simplicity, Figure 3 shows only one TTP agent that represents both the internal and external agents of the particular type.

**Internal agents.** As the name indicates, internal agents execute on the user’s system, and some of them can access various repositories. For internal agents, the personal context agent maintains context within which the user operates, providing contextualized contract negotiation and transactional interaction with sites. The arbitrator agent uses a site’s proposals and user preferences to determine whether or not a privacy contract can be established with the accessed service site. The arbitrator also lets users negotiate on a triple of P3P-defined elements: for what purposes can the business use the user’s PII, who can receive PII, and how long the business or other defined recipient can retain user-provided PII. The monitor agent guards the user from unintentionally revealing private

---

**Legend**

- **Agent A**
- **Agent B**
- **Repository**
- **Employee data**
- **User agent name**
- **Inherits relationship for repositories**
- **User**
- **Service agent**
- **TTP agent group**
- **Group of trusted third-party (TTP) agents of a specific type**

---

**Figure 3.** A multiple agent system and knowledge base architecture for user-controlled e-privacy. The monitor agent oversees the user’s interaction with Web forms and other interaction mechanisms at Web service sites. The context agent manages dynamic changes of the user privacy context as the user interacts with sites on the Web, informs the user about the current privacy-related context for decision support within a Web transaction, and triggers revision of user privacy preferences either due to other agents in the architecture or actions by the user. The arbitrator agent allows users to negotiate on their PII’s usage purposes, handling recipients and PII retention periods with an organization on the Web. The regulatory agent invokes privacy Web services and utilizes external service feeds and trusted third-party (TTP) agents to obtain knowledge on privacy regulations, guidelines, and service sites in multiple jurisdictions. The iCritics and social contract core agents are external agents proposed in other research that add further stakeholder value to our sociotechnical architecture.
data that he or she didn’t intend to reveal according to the negotiated contracts. The monitor agent observes the user’s actions, captures user data input in Web forms, and uses form labels to detect whether the data entered is privacy-sensitive, and reports them to the personal context manager, which determines whether or not to interrupt the user’s activity and solicit guidance.

**Implementing semantic and dynamic contexts**

We base the implementation of the adaptive agents in Figure 3 on the rigorous AGM belief revision framework (named after its authors, Alchourron, Gardenfors, and Makinson). To support semantic contexts, the personal context manager agent (identified in Figure 3) has independent user-preference induction and context-sensitive text-mining modules. The user-preference induction module analyzes the monitor agent’s feedback on observed actions and the user’s direct input of privacy preferences for identified contexts. A user context is made up of a set of beliefs about the current situation, including privacy preference beliefs, trusting beliefs about the business or government agency, department, community, individual, or other stakeholders with which the user is currently interacting, regulatory beliefs, and beliefs around transaction types (such as surfing, buying, registering, collaborating, searching, and meeting). All feedback on user privacy preferences, whether provided indirectly by the monitor agent or directly by the user, inputs to the user-preference induction module, which analyzes the input for changes in user preferences for particular contexts. The output of the user-preference induction module modifies agents’ beliefs and is persistently stored in the time-stamped user preferences repository. In general, updates on agent repositories can update associated agents’ beliefs. Updates to agent beliefs are also time-stamped to provide a history.

In addition to user preference induction, context-sensitive text-mining methods provide semantics around privacy information in the documents coming from external feeds, such as those pushed by external privacy Web agents. In the case of providing relevance feedback for incoming privacy knowledge, the user triggers the document relevance feedback process via a browser interface icon. We don’t intend the text-mining process to operate simultaneously with the user-preference induction module; instead, the text-mining process is offline in an identified time cycle or after a fixed number \( n \) of incoming documents. To incorporate knowledge from documents, we adopted Raymond Lau’s two-phase context-sensitive text-mining method, in which term proximity factors or concept co-occurrence in a text window, and then hidden concept associations (those not occurring in a window), are discovered along with rule strengths of the asymmetric association rules among concepts. In essence, the method builds a semantic concept network with calculated weights (strengths) between concepts (nodes) on the edges. Each discovered association rule is treated as a belief and stored in the relevant repositories. Results using third-party data sets show that agents that have revised beliefs in such a system can lead to more pertinent information retrieval. Thus, the personal context manager can decide if it should present the document to the user for inspection in this user relevance feedback cycle, based on its context-sensitive text-mining module having weighted a document over a privacy threshold value.

Our architecture penalizes the user for new contexts because the system must learn with a human–in-the-loop approach to develop higher-quality semantics and reasoning. This presents a user–time penalty—the system must solicit user input more often for new contexts. Therefore, the user must take some time and care to interact with our system up front. This initial effort should stabilize reasonably quickly as the system is trained. We hypothesize that users would be willing to accept this penalty for a useful tool—just as regular users now accept a similarly up-front penalty to prevent spam from making their email tools less useful.

Dynamically changing user privacy preferences could impact existing privacy contracts. If users are unhappy with past privacy contracts, for example, they can instruct personal agents to attempt to renegotiate contracts with service sites. Most countries have laws or privacy acts that facilitate such renegotiation; users perceive heightened benevolence from business or government when allowed to amend their preferences. The arbitrator, with the help of the personal context manager, ranks a contract before storing it in the repository. The contract is ranked according to the sensitivity of the data that’s shared with a third party. The arbitrator can also rank a contract according to complexity and criticality. Users could choose to instruct the agent system to renegotiate only those contracts ranked high for criticality and contract persistence. Contracts and their amendments are time-stamped and have duration attributes, as in offline contexts. Any violations in contracts are handled, as in the offline world, through separate recourse measures that are available to a data subject–arbitration (if the data subject is the owner of the PII, such as a consumer) or through the courts. The advantage of our current architecture is that it can create an informed electronic contract.

**Implementing external agents and privacy Web services**

The external agents in our architecture must be Semantic Web-aware, capable of accessing RDF, Web Ontology language (OWL), or DAML+OIL repositories and ontologies, and able to invoke other third-
Online Privacy

User interfaces for managing online privacy

Our proposed architecture’s success hinges on human–computer interaction and the minimalism and effectiveness of such interactions. Our vision of a user interface (UI) supports privacy tasks such as those during contract negotiation, user preference population, filling out forms, and surfing.

Figure 4 provides a sample of UI privacy icons currently divided into four groups: informational, contract (transactional), maintenance, and alerts. All UI icons appear in a minimal privacy task bar, implemented as a Web browser extension. This privacy task bar, which contains privacy icons and dashboard–type indicators, lets the user invoke privacy Web services, receive warning alerts, or seek more information from internal or external sources.

Informational privacy icons, shown in Figure 4a, serve user requests for further information concerning privacy rights in the user’s current environment. Supporting various situational privacy contexts, we classify contract negotiations (Figure 4b) according to user time tolerance (tolerance in time delays) with respect to different types of transactions. Contracts for the surf transaction should be necessarily brief and preferably binary in nature—for example, “yes/no to log activity for me while I am at this site.” A slew of non-P3P-based negotiation protocols have appeared in the past year, many of which can be adapted to our architecture. We have created a client-side arbitrator agent prototype and developed a small simulator for a corresponding business site’s negotiation agent to elucidate user negotiation scenarios for the privacy domain. Contract negotiations can be much longer during the buy, registration, or collaboration transactions than when surfing.

Users manage or maintain their privacy data systems through the privacy toolbar using icons to invoke forms that interface to private data and preferences repositories (Figure 4c). They can also provide relevance feedback to information in documents that the personal context agent’s text-mining module has identified for presentation to the user to fine-tune the system.

The fourth group of interface symbols, shown in Figure 4d, is that of alerts; for example, an indicator might appear while the user was surfing that points out that a downloaded image was from an unchecked third party. It doesn’t matter whether one or all of the images are from a third-party site—what matters is what the user wants to do next. User intervention might not be necessary if user preference information about this event was already stored in the repository. Thus, either the user or his or her personal agent could direct a P3P agent to read the privacy statement from the third-party site. The alert functions similarly handle third-party cookie downloads. Figure 4d shows a warning alert for “your data is being monitored,” which our architecture supports through the integration of appropriate security algorithms.

---

party privacy Web services. Advances in Semantic Web tools will facilitate greater sophistication in informing online privacy tasks. For example, it would be useful for a P3P agent, upon reading in Business Technology Services’s privacy statement that the company “may share consumer information with its strategic partners,” to find out who its partners are. A user’s agent could issue a query, “who are BTS’s partners,” to an external agent called TellMeWho. The TellMeWho agent would then consult the appropriate ontologies and knowledge bases (coded in OWL) that deal with publicly traded companies, and then use DAML Query Language (DQL) to extract the results as names: DBMS Consulting, ABC Co., and SurfAndBuy.ca. After receiving these answers, the P3P agent could negotiate a contract with BTS’s service site to limit sharing to only DBMS Consulting. A simplified DQL query and its answer would look like:

Query: (“Who are BTS’s partners?”)
Query Pattern: (exists ? p (and (has BTS? p) (type ? p partner)))
Must-Bind Variable List: (?p)
Answer: “BTS has DBMS Consulting, ABC Co., SurfandBuy.ca”
Answer Pattern Instance: ((has DBMS Consulting, ABC Co., surfandbuy.ca, “BTS”))

For a more complex scenario, the user agent could ask, “who are and where are BTS’s partners based?” If answers include that one partner is in Japan, another in India, and a third in England, the external and internal regulatory agents will become involved. The integration service agent that synthesizes various layers of a country’s privacy acts or laws could be invoked before the user personal context agent decided on an appropriate action.

Web privacy services are useful not only for enabling for three-way comparisons among user, government, and business stakeholders, but also for single stakeholder comparisons. For example, a business policy comparison service can be useful in several areas. One such is the area of multiple jurisdictions where users might deal with a Web multinational, that is, with a company doing electronic commerce through subsidiaries in many countries (for example Amazon Japan or Amazon UK). A Web service doing such a comparison would tap resources such as the Safe Harbor initiative, which lists membership information of companies who abide by other countries’ privacy laws when doing business in those countries. Another area could be a Web service in which a user can compare many business’ privacy policies to determine which of them handle PII in a manner that is appropriate to the user.
The user interface must also support the user in instructing an agent, including performing agent recall, updating its beliefs, renegotiating contracts, and revising its tasks. We foresee the need for other icons (not shown in Figure 4), such as those that could represent a user’s request to examine an audit trail of activities with a particular service site or business.

The most pragmatic and important perspective on online privacy is that of the user. Future research on this project includes adding finer-grained privacy control for the user, improving our algorithms for maintaining agent belief systems and for automatic and contextual privacy-rule generation, adding natural language intelligence into the agent and ontology sociotechnical architecture to improve usability beyond P3P dependence, and incorporating usability results into future prototype versions. The current Collaborative User Services for Privacy project site is at http://cusp.smu.ca. With this still-evolving architecture, we take one more step toward the vision of empowering users to effectively manage their online privacy.

References
6. M.K. Hui and J.E.G. Bateson, “Perceived Control and

**Dawn Jutla** is an associate professor in the Sobey School of Business at Saint Mary’s University in Canada. She has coauthored more than 50 publications in the computing, information system, electronic commerce, electronic business, and e-government areas. She is coauthor of *e-Business Readiness: A Customer Focused Framework* (Addison-Wesley, 2000). Her latest works are in e-privacy and knowledge management. Jutla has a PhD in computer science from the Technical University of Nova Scotia. Contact her at dawn.jutla@smu.ca.

**Peter Bodorik** is a professor in the computer science department at Dalhousie University. His current research interests are in developing middleware for e-business applications. He has a PhD in systems and computer engineering from Carleton University. Contact him at bodorik@cs.dal.ca.

To receive regular updates, email dsonline@computer.org

**IEEE Distributed Systems Online** brings you peer-reviewed features, tutorials, and expert-moderated pages covering a growing spectrum of important topics:

- **Security**
- **Grid Computing**
- **Mobile and Wireless**
- **Middleware**
- **Distributed Agents**

**VISIT IEEE’S FIRST ONLINE-ONLY DIGITAL PUBLICATION**

dsonline.computer.org