PIPWatch Toolbar

© ISTOCK PHOTO

Using Social Navigation to Enhance Privacy Protection and Compliance

ANDREW CLEMENT, DAVID LEY, TERRY COSTANTINO,
DAN KURTZ, AND MIKE TISSENBAUM

Digital Object Identifier 10.1109/MTS.2010.935989

Repeated public surveys have found that people are increasingly concerned about their privacy when engaged in online activities [1]. In particular, people are concerned about how and when information is collected about them, and how that information is subsequently used. A number of strategies have been developed to assist individuals in protecting their privacy online. Privacy Enhancing Technologies (PETs) such as the Platform for Privacy Preferences (P3P) have been developed to help individuals quickly analyze the privacy practices of different websites and in doing so help raise awareness of privacy risks before submitting sensitive personal information. Also, a number of jurisdictions have passed laws and regulations governing the handling of personal information. In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA) governs how commercial companies gather and manage personal data.

Despite these efforts, people often lack sufficient information to make informed decisions about whether they should provide personal data to a data collector, and often trade their privacy for relatively small rewards [2]. The use of PETs can be limited by the need for a high level of technical expertise or by a lack of cooperation on the part of data collectors. Legislation can be difficult to enforce, especially on the Internet where national boundaries are blurred. A new approach is needed if PETs are to be made more usable and relevant, and if legislation is to become more widely understood and effective.

We have built a novel PET that uses a technique for the sharing of information known as social navigation to help Internet users determine if the privacy practices of the websites they are visiting comply with Canadian standards of fair information practices. Our PIPWatch web-browser toolbar allows a community of privacy-concerned individuals to share information on how different websites comply with Canadian legislative codes and other Canadian-centered privacy concerns. We think that our approach overcomes some of the limitations of other awareness-raising PETs such as P3P, while at the same time promoting compliance with and understanding of a particular set of privacy regulations.

We have finished two rounds of prototyping of our PIPWatch toolbar, which have helped us evaluate the community concept and gather feedback for the next iteration of the toolbar.

Responses To Online Privacy Concerns

It has become increasingly difficult for people to understand how their personal data is collected, stored, shared and transmitted, and what measures they can take to control its use. The proliferation of ways in which one leaves traces of activity behind with every commercial transaction raises the possibility that one's data will be used for undesirable purposes, with consequences ranging from embarrassment and social sanctions to identity theft, financial loss, and travel restrictions [3], [4].

The most prominent strategy for protecting privacy has been the adoption of privacy legislation. Once individuals release information, they lose control over who uses it and for what purposes. Therefore, some argue that it is necessary for governments or other bodies to regulate privacy issues, and establish guidelines on how personal data can be collected, shared, and used.

Since the mid-1970s, a set of principles known as Fair Information Practices (FIP) has been developed and incorporated into the laws and regulations of numerous jurisdictions. The most well known encoding of the FIP Principles has been the Organization of Economic Development's (OECD) Guidelines for the Protection of Privacy and Transborder flows of Personal Data [5]. In Canada, the FIP principles underpin the provisions of the Personal Information and Electronic Documents Act (PIPEDA), which came into effect for all businesses on January 1, 2004. Under PIPEDA, "personal information must be:

- collected with consent and for a reasonable purpose;
- used and disclosed for the limited purpose for which it was collected ;
- accurate;
- accessible for inspection and correction;
- stored securely" [6].

The PIPEDA legislation further requires organizations to publish a statement explaining their information collecting practices and to identify one person responsible for dealing with privacy inquiries. To comply with these requirements, many websites post a privacy policy statement and name a Privacy Officer whose job it is to explain the organization's privacy practices to the public.

A second broad approach to privacy protection suggests that market forces will provide a solution: companies that respect consumer privacy will gain more customers at the expense of those that don't [7]. A marketplace for personal information, so it is promised, will allow individuals to get more benefit for handing over their personal information and encourage companies to respect individual privacy preferences [8]. Industries will use self-regulation to enforce compliance with privacy standards. Certification and standards such as eTrust's privacy seal (http://www.truste.com/) will give consumers confidence. Websites will post privacy policies outlining their practices surrounding the collection and management of personal

information and consumers will take those practices into account when evaluating competitors.

One serious problem with the market approach is that it becomes very difficult for consumers to assimilate sufficient information in time to make an informed decision. Privacy policy statements are often lengthy and complex [9]; they are not designed to make it easy for consumers to compare them. It becomes almost impossible for a typical consumer to read the privacy statement of every website they visit [10], and even harder to intelligently choose the best among them for a particular transaction. Further discouraging this approach, many consumers do not trust what companies say in their privacy policies [11].

A third strategy has been to arm individuals with various PETs that will help them manage and protect their privacy. These include tools to encrypt e-mail communication, browse the Internet anonymously or raise awareness of privacy risks when engaging in transactions online. One of the chief complaints against many PET tools is that they have focused too much on methods for securing data against theft, while ignoring the problem that occurs when users willingly give away their information [12]. Awareness-based PETs – ones that inform a user of the privacy risks in the environment around them – are meant to help provide enough information to individuals to allow them to make rational choices.

One of the most widely touted awareness-based PETs in recent years has been P3P. P3P allows website operators to post a machine-readable version of their privacy policy on their site. Users can use a "privacy agent" to automatically compare and evaluate the privacy practices of different websites without having to read all the statements [13], [14]. However, P3P requires the cooperation of website operators, and the adoption rate of P3P has been slow. As of 2006, only about 15% of the top 5000 websites are P3P-enabled [15]. Even those sites that are P3P compliant still decide what information to include in their P3P-enabled privacy policy, potentially leaving out information about the company's privacy practices that the consumer would want to know. This lack of uniformity means that it still can be difficult to compare different websites using P3P [16].

Social Navigation

Social navigation is a strategy for using the collective knowledge and experience of a large community, integrated into an electronic communication tool, to guide individual actions and decisions [17]. Social navigation has been used successfully in online searching, collaborative writing, and e-commerce.

Some examples of social navigation or social software include the Google page rank algorithm, which ranks web pages higher when outside websites link to it – allowing in effect for a wide collection of people to vote on which web pages they think provide the best content [18]. eBay's reputation system for rating buyers and sellers is another example. Wikipedia, one of the largest collaborative, user-contributed information resources on the web (www.wikipedia.org) is an example of how a community of interested parties can collaborate for the collective good, without the need for monetary reward [19].

In the privacy sphere, a tool described by Goecks & Mynatt [20] illustrates how social navigation could be used to help individuals protect their privacy by using collective expertise to determine when cookies should be accepted. Much of the inspiration for our PIPWatch tool was drawn from their work. Netcraft's anti-phishing toolbar (http://toolbar.netcraft.com/) is the only other example we could find of how the resources of a community can be used to help identify privacy risks.

One possible application of social navigation techniques to privacy technology would be to set up some sort of communal rating system – similar to eBay's reputation system but focusing exclusively on rating the privacy practices of different organizations. This would be extremely difficult to implement in practice, since most consumers lack the expertise to effectively critique and compare privacy policies of different organizations. If contributions were restricted to "expert" users, the small number of individuals with sufficient knowledge and time to rank and compare privacy policies would make difficult for any system to obtain the necessary critical mass of users. For these reasons, our PIPWatch tool uses a relatively structured and organized system for collecting communal data, rather than following the more open-ended designs used by other social navigation-based systems. PIPWatch users are encouraged to participate in building up of the utility of the system, but their efforts are directed towards a set of very specific activities, which we describe in the next section.

PIPWatch Overview

The main goal of our project is to evaluate the prospects of combining social navigation techniques into a PET that helps Internet users identify which websites comply with Canadian privacy legislation and to honor the concerns common among Canadians who conduct personal transactions via the web. Our PIPWatch tool allows users to collect and share information about the privacy practices of various websites. Our tool works as follows:

- Every time a PIPWatch toolbar user visits a website, the server provides the user with any information it has about the website, which appears in a bar across the top of the browser (Fig. 1) and as a "privacy beaver" icon in

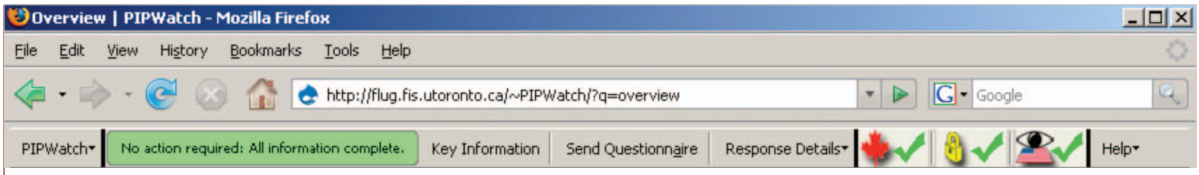
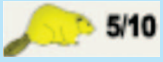


Fig. 1. The PIPWatch toolbar.

the lower right hand corner, which changes color according to an overall privacy risk (Table I).

- PIPWatch users are invited to contribute small pieces of key information about the websites they visit (Fig. 2).
- The PIPWatch tool includes an interface to send an email to the Privacy Officer of a website, asking them to fill out a short questionnaire about their privacy practices. The key information gathered beforehand by PIPWatch users makes this task easy to accomplish.
- Responses by the various Privacy Officers are stored on the central server. Whenever a PIPWatch user visits a website where a questionnaire has been completed, they are provided with the responses via the toolbar and the beaver.
- With responses of several businesses in the same sector displayed in a readily comparable format, it is easy to choose from among them the one that best suits one's privacy preferences (Fig. 3).

Table I
Privacy Beaver Icons

Icon	Color	Meaning
	Grey	The PIPWatch system has been turned off
	Grey	The privacy officer not been identified or contacted
	Grey	The privacy officer has not responded to the questionnaire
	Red	The current website's privacy practices DOES NOT match the user's preferences
	Yellow	The current website's privacy practices PARTIALLY matches the user's preferences
	Green	The current website's privacy practices matches the user's preferences

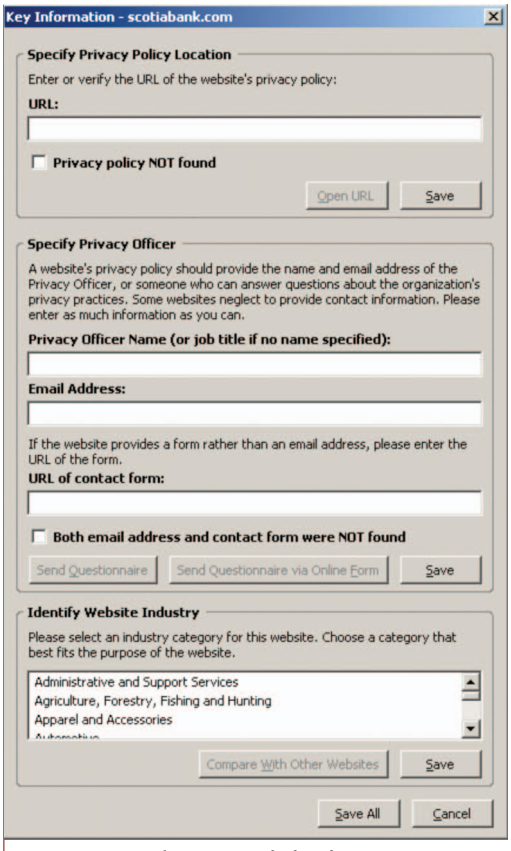


Fig. 2. Key information dialog box.

The current implementation of PIPWatch includes three questions on the questionnaire sent to Privacy Officers (Table II).

While these three questions are by no means an exhaustive list of the concerns of Canadian Internet users, they are among those most frequently mentioned. We decided that starting with a small number of questions would improve the likelihood of cooperation by Privacy Officers. Since the PIPEDA legislation calls for organizations to appoint a Privacy Officer who is responsible for fielding questions from the public, there should by law be someone at every Canadian-operated commercial website able to answer the questions posed.

We do not expect every website to be PIPEDA compliant. Indeed, since a majority of websites are not located in Canada, we expect that most website operators will not even know what PIPEDA is. We expect that some such operators who are not obliged to do so will nevertheless want to attract business from Canadians. Others that have international clientele will want or

need to comply with the comparable European Data Protection Directive, and should have little difficulty meeting the Canadian criteria. To assist non-Canadian operators, we include information in the questionnaire indicating what PIPEDA is and how to achieve compliance.

In addition to the main goal of testing the feasibility of PIPWatch, the project has several additional sub-goals in the areas of privacy research, education, and advocacy. Some past research has indicated problems with the adoption of privacy regulations, noting that "the implementation of PIPEDA has been ad hoc at best and nonexistent at worst" [21]. A high response rate from Privacy Officers would indicate a high compliance with at least one aspect of PIPEDA: the requirement for openness about an organization's privacy policies. Their specific answers will further help indicate how well Canadian companies are complying with other aspects of PIPEDA.

PIPWatch has also been designed with an educational purpose in mind. Information screens about PIPEDA and other privacy issues are embedded in the toolbar. It will be useful to evaluate how well the PIPWatch tool works in educating users who are concerned about privacy issues but may not know specific details.

Lastly, it will be interesting to see if the PIPWatch tool encourages compliance on the part of websites. When websites receive the emailed questionnaires, they may be prompted to review their privacy policies to determine if they are PIPEDA compliant. Furthermore, if consumers prefer sites that are more forthcoming in their responses and demonstrate stronger privacy protection, that will exert new market pressure to improve privacy protection.

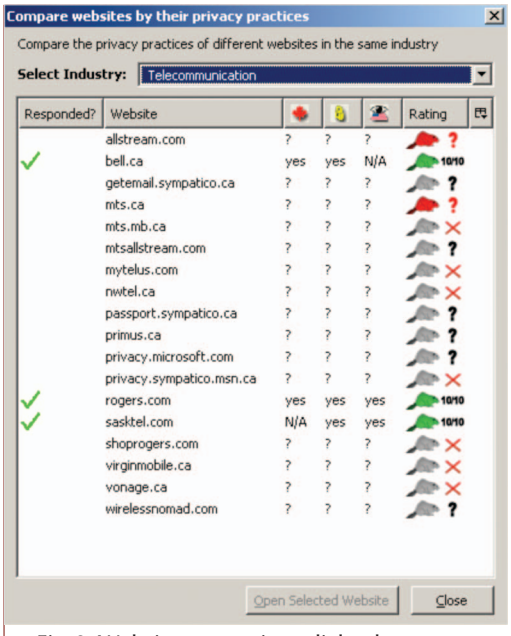


Fig. 3. Website comparison dialog box.

Other PIPWatch Features

P3P tools such as PrivacyBird (http://www.privacybird.com/) allow users to specify their privacy settings, and give a warning when a website does not match the user's stated preferences. PIPWatch adopts a similar strategy with our Privacy Beaver. In their privacy preferences, each user can specify the degree of their concern about each of the three privacy questions. These preferences, coupled with a privacy officer's responses to these questions, determine how the Privacy Beaver is displayed in the bottom right corner of the user's Firefox browser and the website comparison dialog box (Fig. 3). The degree of risk is calculated as the sum of the Yes/No answers to each question, weighted by the numerical preference score and is indicated by both the color of the beaver as well as the numerical score out of 10. The range of possible states and meaning of the beaver icons are displayed in Table I.

Table II
Privacy Questions and Icons

1. Do your organization's policies and procedures comply with Canadian privacy laws and regulations? In particular, do they comply with the provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA), or with similar legislation in the provinces of British Columbia, Alberta and Quebec?

2. Do you take reasonable measures to ensure that personal information you collect from Canadians will only be shared with organizations that are compliant with PIPEDA (or similar provincial legislation)?

3. All data that is stored in or transmitted through the United States or processed by a company covered by US laws, is subject to the provisions of the USA Patriot Act. Do you take reasonable measures to ensure that all personal information you collect from Canadians will not become subject to the USA Patriot Act?

Implementation Details

The PIPWatch toolbar is built as an add-on extension for the Firefox browser using the XML User Interface Language (XUL). The toolbar resides in the user's browser window and communicates with the PIPWatch server when the user requests a page. The server interface to the toolbar runs a web services application currently written in Java and connected to a MySQL database. The servlet assembles responses by querying this database containing information about users and sites.

This database is also used by the public-facing PIPWatch.ca website.

The website, created with the Drupal content management system, is where users can learn about the system, register as members, and download the toolbar.

The site also includes a forum, where users can discuss with each other and with the research team various aspects of PIPWatch and the sites they visit. The current version of the toolbar can be found and tested at the project website: http://PIPWatch.ca

Design Justification and Discussion

During our initial discussion with prospective users of PIPWatch, there was some concern raised about the prospect of the "screen real estate" being used up by the PIPWatch toolbar. Other options were considered, including hosting a website with detailed ratings for each website in our database. Other users expressed the desire for a "beginner" and "expert" view, with the former having one small icon only (similar to the Privacy Bird) and the latter with more detailed feedback. We felt that a web-browser toolbar was the most appropriate method for embedding signals to give users instant feedback on the privacy practices of the website they are currently visiting as well to invite them to contribute information when needed.

Usability testing was undertaken on the first prototype and resulted in a number of design changes. The Key Information dialog box was reworked, making the pieces of information independent. The privacy officer response dialog boxes were merged into one dialog box. The Privacy Beaver indicator was de-coupled from the toolbar so that it is visible even when the toolbar is hidden.

During usability testing, a participant pointed out that exclusive use of color to indicate the privacy risk would not be accessible for color-blind individuals. Based on this feedback, a redundant risk indicator was added – the numerical score of out 10.

Currently the user community is small, with about 100 participants registered, but fewer than that are active. Cumulatively they have already visited more than 60 000 websites, thereby anonymously building the database. PIPWatch users have explicitly contributed information about more than 400 websites and made over 200 requests to privacy officers, some repeatedly. However, so far only 31 Privacy Officers have answered our questionnaire. This lack of responsiveness by Privacy Officers is currently the most serious challenge for us, since the value of the tool comes from the information they provide, and user interest wanes when there is no basis for differentiating between sites.

In essence, like social networking sites more generally, we face a chicken-and-egg problem. Until there is a significant amount of useful material, PIPWatch will not be attractive to new members, but gathering these materials requires contributions from previous members. In our case, this difficulty is compounded by the indifference and even active resistance from a key component of the user base – privacy officers. One way to get around this is to target the high-profile sites that many PIPWatch visit regularly, and by pooling our efforts put pressure on these sites to avoid bad publicity and reap some benefit by being recognized as setting a good example.

We have had some success in turning up the pressure on non-responding officers. The CPO of Facebook, the most popular site among PIPWatch users, finally answered our questionnaire after having received 28 requests followed-up by direct personal contact.

While the current operation reflects a notable proof-of-concept, PIPWatch is not yet an effective and self-sustaining tool for enhancing personal privacy. A major shortcoming has already been identified – the lack of response by privacy officers. But there are a number of other problems:

- The questions posed are general and limited in scope, allowing only coarse comparisons.
- The privacy ratings depend exclusively on how privacy officers respond. There are no other independent sources of assessment.
- The toolbar only operates with Mozilla Firefox 2, not with the more common Internet Explorer web browser.
- The user base is not yet of sufficient size to generate new content on an ongoing basis.
- The contributions by individual users are not sufficiently visible to give recognition to regulars and to give encouragement to newcomers.
- There is little sense of a rewarding collective enterprise.

Most of these limitations reflect the still early stage of development, and in some cases are deliberate, intended to keep matters manageably simple. The next steps are to significantly expand the capabilities of the toolbar and to recruit a larger user community.

Future Plans

A priority is to recruiting individuals to use the PIPWatch toolbar, asking them to gather key information and to send questionnaires to privacy officers. We adopt a participatory action research approach to actively engage these individuals in using the toolbar and providing feedback about the subject matter, the interface design, and the technical design. To address the shortcomings we have identified so far, we will:

- Provide users with summarized information about particular websites, drawn from a significantly wider range of sources, such as more detailed questions posed to privacy officers, news reports, consumer complaints, industry awards, Privacy Commissioner rulings, expert assessments, and ratings by other PIPWatch users.
- Give greater prominence to the contributions of users who wish to be recognized.
- Enable users to register specific complaints and compliments about the organizations' privacy practices, and track any response to users' complaints and compliments.
- Develop a more substantial rating system, where users can rate websites on their privacy practices.
- Incorporate a "Privacy Wiki" functionality similar to the Wikipedia approach, where users can construct and share their own evaluation schemes about privacy issues and practices.
- Collaborate with willing privacy officers in refining the questionnaire and related data gathering tools.

Novel On-Line Privacy Protection Approach

The PIPWatch tool is a novel approach to the problem of protecting privacy online. By combining social navigation techniques into a PET, the tool allows a group of privacy-concerned users to evaluate the privacy practices of websites they visit and to encourage compliance when it is lacking. Previous approaches to privacy protection have suggested that a solution lies with legislation or with market pressures or with PETs. We argue that PIPWatch combines these three approaches.

With a working prototype that has undergone several rounds of testing with users, the next stage is to extend the technical capabilities and build a user community. We want to assess how Privacy Officers respond when faced with a community of concerned and mobilized users. The degree and kind of cooperation from Privacy Officers (or the lack of cooperation) will indicate the effectiveness of our tool, and will also give us a sense of how Privacy Officers are complying with the openness and accountability principles of the PIPEDA legislation.

An expanded member base and a more refined privacy assessment tool will be needed for proper research about the effectiveness of this approach and about individual and privacy officer behavior. But, some preliminary conclusions can be made about these issues. We have shown that people can install and use the toolbar with relative ease, and will do so even when there is little immediate reward. Users will also provide some basic site information and send messages to privacy officers at least for an initial trial period.

More challenging is the reluctance of privacy officers to respond to member queries, even when repeatedly reminded that they are not fulfilling their legal obligation to be open about their privacy practices. As has been noted in other research, privacy compliance is often grudging and more oriented to giving the appearance than delivering the substance of privacy protection [9]. Evidently, at the current low level of PIPWatch activity, privacy officers conclude they can safely ignore the mild negative publicity. This does not mean the tool cannot succeed, and demonstrates the need for some form of more effective consumer mobilization – something the PIPWatch toolbar still holds promise of providing.

In addition to its potential value in the privacy area, the underlying technology of PIPWatch – a browser embedded toolbar displaying convenient, real-time feedback on the practices of web-owning organizations as reported by a collaborative community of fellow users – offers a model for organizational accountability in other areas where users want to selectively exercise their consumer preferences based on organizational behavior. It is not hard to imagine how watch-dog communities focused on such issues as pollution, global warming, labor practices, civil liberties, and human rights, may find this approach useful in pooling their experiences in a way that it is readily available at the moment of a web transaction.

Acknowledgment

We thank the volunteers who have contributed vital information to the PIPWatch database, who have solicited answers to key privacy questions from website privacy officers, who have posted comments in the discussion forum, and who have responded to our recurring requests for feedback. The first version of the PIPWatch software developed by David Ley was subsequently refined and expanded by Jeff Orchard, Afshin Lotfi and Parsa Shabani. This work has been supported financially by the Social Sciences and Humanities Research Council as well as by Bell University Labs at the University of Toronto. We appreciate the comments of the anonymous reviewers in revising this paper.

Author Information

The authors are with the University of Toronto, Toronto, Ont., Canada. Email: andrew.clement@utoronto.ca.

References

[1] Electronic Privacy Information Center, "Public opinion on privacy," *Epic.org*, Oct. 9, 2005; http://www.epic.org/privacy/survey/.

[2] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making", *IEEE Security & Privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[3] S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*. Beijing, China, and Cambridge, MA: O'Reilly & Assoc., 2001.

[4] D. Solove, *The Digital Person*. New York, NY: New York Univ, Press, 2004.

[5] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Cooperation and Development, 1980; http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.htm.

[6] Industry Canada, *PIPEDA Overview: What*. 2004; http://privacyforbusiness.ic.gc.ca.

[7] A. Cavoukian and T. Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust*. McGraw-Hill Ryerson, 2002.

[8] K. Laudon, "Markets and privacy," *Commun. ACM*, vol. 39, no. 9, pp. 92–104, 1996.

[9] C. Jensen, and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Computer Human Interaction*. Vienna, 2004.

[10] T. Vila, R. Greenstadt, and D. Molnar, "Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market," in *Proc. 5th Int. Conf. Electronic Commerce*, Pittsburg, PA, 2003.

[11] Ernst & Young, "Privacy promises are not enough," 2001; HYPERLINK "http://www.ey.com/global/download.nsf/" http://www.ey.com/global/download.nsf/US/Privacy_Promises/$file/EYPrivacy%20Promises.pdf.

[12] H. Burkert, "Privacy-enhancing technologies: Typology, critique, vision," in *Technology and Privacy: The New Landscape*, P. Agre and M. Rotenberg, Eds. London, U.K.: M.I.T. Press, 1997.

[13] L.F. Cranor, *Web Privacy with P3P*. O'Reilly & Assoc., 2002.

[14] W3C, *The Platform for Privacy Preferences. World Wide Web Consortium Initiatives*, 2005; http://www.w3.org/P3P/.

[15] L.F. Cranor, A.M. McDonald, S.Egelman, and S. Sheng, *CyLab Privacy Interest Group 2006 Privacy Policy Trends Report*, 2007; http://www.chariotsfire.com/pub/cpig-jan2007.pdf.

[16] EPIC & Junkbusters, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*, 2000; http://www.epic.org/reports/prettypoorprivacy.html.

[17] K. Höök, D. Benyon, and A.J. Munro. *Designing Information Spaces: The Social Navigation Approach*. London, U.K.: Springer, 2003.

[18] S. Brin and L. Page, "The anatomy of a large-scale hypertextual Web search engine," in *Seventh Int. World Wide Web Conf*., Brisbane, Australia: Elsevier, 1998.

[19] A. Lih, "Wikipedia as participatory journalism: reliable sources? Metrics for evaluating collaborative media as a news resource," in *Proc. 5th Int. Symp.Online Journalism* (Austin, TX), April 16–17, 2004; http://journalism.utexas.edu/onlinejournalism/wikipedia.pdf.

[20] J. Goecks and E.D. Mynatt, "Supporting privacy management via *community experience and expertise," in Communities and Technologies, Proc. Second Communities and Technologies Conf*. (Milano, Italy), P. van den Besselaar, G. de Michelis, J. Preece, and C. Simone, Eds., 2005.

[21] R. Akalu, "Implementing PIPEDA: A review of internet privacy statements and on-line practices," Office of the Privacy Commissioner of Canada, 2005; http://pipedaproject.atrc.utoronto.ca/upload/PIPEDAfinal.pdf.