Abstract

Lack of trust in the infrastructure has been reported by many as a major impediment to the broader adoption of e-Commerce and other Internet applications and services – e.g. (Georgetown Internet Privacy Policy Survey 1999, Wang 2001, JRC 2001, Zobel and Sadeh, 2001). Many users perceive solutions deployed over the Internet to collect, analyze and disseminate information as potential threats to their privacy, sometimes for good reasons and sometimes simply out of a lack of understanding of what these solutions actually do with their information.

As the information and communication infrastructure helps mediate an ever broader range of activities, corporations, lawmakers, regulation agencies and consumer advocacy groups have to grapple with a broad range of ill-understood issues that directly impact people’s privacy. The explosion in mobile phone ownership, the emergence of authentication services such as .NET Passport or the deployment of “context-aware” functionality that makes it possible to track people’s location and other aspects of their daily activities further exacerbates this situation. While it can be argued that consumers may benefit from disclosing some information about themselves (e.g. through greater degrees of personalization or context awareness), they also run the risk of seeing their information misused. The scenarios range from being bombarded with annoying location-sensitive ads to downright scary situations where sensitive financial, health or other information could fall into the hands of unscrupulous third parties.

Within this context, black-and-white policies that would strictly limit the disclosure and use of private information would fall short, as they would close the door on a number of potentially appealing scenarios. Similarly, too loose an approach would likely fail to provide consumers with sufficient trust in the Internet environment. It would seem therefore that, in many situations, it would be best to provide consumers with a framework within which they could decide for themselves what the best tradeoffs are, namely what information to disclose to whom and under which conditions. This view, which has been advocated by many, is in line with the approach taken by the World Wide Web Consortium (W3C) and its Platform for Privacy Preferences (P3P) project, which is quickly emerging as the industry standard for providing users with more control over the use of their personal information (W3C-P3P, 2001).

Under P3P, web servers send machine-readable privacy proposals to the browsers of users who attempt to connect to their site. The browser then compares the proposal with the consumer’s own privacy preferences and determines whether or not to proceed or possibly prompt the user for a decision. While well-intentioned, this approach creates a tension between privacy and usability. To what extent can we expect users to specify their privacy preferences? Do users know their preferences ahead of time and do they actually understand the implications of different privacy options? If users are not willing to sit down for hours, specifying their preferences, what alternatives do we have to capture these preferences? Is it possible to identify key factors influencing user privacy preferences (e.g. nature of information being disclosed, nature of the site the information is disclosed to, whether or not the information is stored in an identifying manner, whether it is shared with third parties, prior interactions the user might have had with the site, nature of the interaction between the user and the site such as browsing versus shopping, etc.).

By attempting to answer these and related questions in a scientific manner, we hope to help lawmakers, regulation bodies, businesses, consumer advocacy groups and other relevant actors to make better-informed decisions. In the process, we also hope to inform key standardization efforts such as those conducted by the World Wide Web Consortium under its ongoing P3P project.

By: Zhuo, Yi’nan
Prof. Norman Sadeh (Advisor)