Online Privacy and P3P

An analysis of the current state of privacy practices, perceptions, and how if affects your organization

Zach Evans

October 31, 2003

Why is online privacy important? This complex question is one that has been haunting businesses and individuals alike since the dawn of the Internet. The World Wide Web—and the technologies that drive it—has broken down cultural, ideological, and geographical barriers but this 'closeness' has come at a cost. The commercial enterprises that have shouldered a large portion of the development costs of the Internet are looking for a reward for their efforts: information. The Internet has significantly reduced the costs of obtaining information about individuals, resulting in a widespread perception by consumers that their privacy is being eroded (Kannan, et. al. 2002).

The Internet allows for the collection, enhancement, and aggregation of data almost instantaneously. All the parties involved with the online world bring certain expectations to the table and have specific responsibilities they must fulfill. Customers and 'browsers' expect to be able to find what they are looking for in a relatively easy fashion and the attention span of the average online consumer is getting shorter and shorter. Businesses expect browsers to be willing to exchange *something* for the production and distribution of what largely is free content and services. This is where the waters begin to become a little murky. Depending on whom you ask, the responsibilities of each party may vary greatly.

Driving this information-driven focus are new technologies, including database tools that let companies gather information about their customers, sales force automation tools that let them deliver better service, and Web technologies that let them establish more personalized relationships with customers. E-commerce is

booming, partially because of the unprecedented access many companies have to information about their customers on the web (Nakra 2001).

Businesses take on substantial risk when they develop their online presence but they must remember one very key fact: online, their competitors are only a click away. To obtain and retain a loyal customer they must accept that privacy and permission are the cornerstones to customer trust. Businesses that want to survive have to learn to walk the fine line between customer *wants* and business *needs*. Equilibrium must be reached that balances the privacy and confidentiality of consumer information while allowing commercial web sites to "efficaciously target their online marketing strategy" (Hemphill 2002).

Factors in Deciding to Visit a Web Site

In a recent survey performed by Consumer WebWatch, respondents identified nine key factors that influenced their decision to visit a web site (Princeton Survey Research Associates 2003).

	Very Important	Somewhat Important	Not Too Important	Not At All Important
The site is easy to navigate and to find what you want	80	16	2	1
Being able to trust the information	80	14	3	1
Being able to easily identify the sources of information	68	25	4	2
Knowing the site is updated frequently with new information	65	28	4	2
Being able to find out important facts about a web site	50	36	8	4
Knowing who owns a web site	32	33	22	12
What organizations financially support the site	24	37	27	11
The site displays seals of approval from other groups	19	41	26	12
The site displays awards and certificates from other groups	9	30	36	23

The same survey asked respondents to rank six factors that directly apply to their choice of an e-commerce site (Princeton Survey Research Associates 2003).

	Very Important	Somewhat Important	Not Too Important	Not At All Important
A statement of fees that you will be charged for using the site	95	3	0	1
A statement of how the site will use the personal information you provide	93	4	1	1
An explanation of when you can expect delivery	89	9	1	1
A statement of the site's policies for returning unwanted items	85	8	1	2
The email address, street address, or phone number where you can reach the site's staff	81	14	2	2
The site's privacy policy	76	18	4	2

Again, in the same survey, respondents were asked to rank the importance of various policies and pages on a site as well as being asked about how often they viewed those policies. The results were that 76 percent of the users surveyed felt that a web site having a privacy policy was very important, second only to the credit card protection policy, which 93 percent of users felt was very important (Princeton Survey Research Associates 2003).

So what is the bottom line of all of these surveys? Forrester Research estimates that businesses lost **$15 billion** in potential revenue due to consumer concerns over privacy protection online (Haller 2002).

Making Privacy a Top-Level Issue

Many companies are already taking issues of privacy very seriously in light of the Internet. At the very least they are posting detailed privacy policies on their web sites and making printed copies of these policies available to customers that request them.

Larger organizations have even gone as far as creating a new C-level position titled the Chief Privacy Officer (the "CPO"). They have also developed programs designed to increase employee awareness and training about the issue of customer privacy while also establishing self-regulatory initiatives.

The CPO position serves as a liaison between the organization and the consumers. These high-powered officers often have veto power over: new product launches, marketing campaigns, and strategic partnerships. Any and all customer-facing programs or internal practices that deal with sensitive information come under the direct supervision and regulation of the CPO (Consumers International 2001). Privacy must be a "corporate-wide initiative, launched and supported from the executive suites, with input and enforcement from all areas of the business. The corporate leadership must get serious about creating a company-wide privacy policy that encompasses all processes and procedures, not just web-related transactions" (Nakra 2001).

Guidelines for Online Privacy Policies

Strong corporate privacy initiatives start with the adoption and implementation of an organization-wide privacy policy. The organization has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. The organization should also take steps to foster the adoption of effective privacy policies by the other organizations they interact with.

Once the privacy policy has been adopted the organization must implement a policy of notice and disclosure. The corporate privacy policy must be easy to find, read, and understand. It must also be available prior to or at the time that the individually identifiable information is collected or requested. The policy should clearly state several

things: what information is being collected; the use of the information being collected; the choices available regarding collection, use, and distribution of the information collected; a statement of an organization's commitment to data security; and the steps the organization takes to ensure data quality and access. Finally, the policy should also disclose the consequences, if any, of an individual's refusal to provide information to the organization.

After notifying and disclosing the privacy policy to its customers, the company must also allow their customers the right to choose. Individuals must be given the opportunity to exercise their right to choose regarding how the information collected may be used when such use is unrelated to the purpose for which it was collected. At the very minimum, individuals must be given the option to opt-out of receiving any future information from the company or any of the company's partners.

Finally, the company has three distinct responsibilities for the data that they have collected: security, quality, and access. The company should take all appropriate steps and measures to assure the data is reliable as well as taking all reasonable precautions to protect it from loss, misuse, or alteration. The company should also take all reasonable steps to assure the data is accurate, complete, and timely for the purposes for which it is to be used. Appropriate processes or mechanisms need to be implemented so that inaccuracies in the data may be corrected and reasonable consumer access to, and correction of, the data need to be planned for as well.

P3P: An Introduction

The Platform for Privacy Preferences (P3P) is a technical protocol, delivered through XML, whose specification include the following: (1) To enable privacy practice

disclosure on the web, a web site must be able to inform consumers of their privacy practices on request; (2) To ensure that any data exchange should happen in the context of disclosure, data exchange can only happen within the context of a consumer's acceptable privacy practice; (3) To specify the necessary grammar and vocabularies for making machine-readable disclosures, standardized keywords and concepts will be employed; and (4) To develop the protocols for exchanging disclosures—and possibly data—as appropriate (Hemphill 2002).

P3P proposes the development of an elaborate range of privacy 'choices' that require individual Internet users to make selections about the collection and use of personal data, even for online activities that would not normally require the disclosure of personal information, such as simply visiting a web site (Electronic Privacy Information Center 2000). For example, assume that Joe Surfer configures his P3P-enabled web browser to say that he does not want to disclose his home address unless he is purchasing a product that will be delivered to his home. When Joe connects to a popular news site that requires the disclosure of his home address before he can view content on the web site, Joe's P3P-enabled browser will block access to the site. If other popular news services also require home addresses, Joe's P3P-enabled browser will prevent Joe from receiving news over the Internet. Or he will have to give up his choice to keep his home address private.

In its simplest form, P3P's architecture consists of the user agent and the service. The technical component of the protocol consists of grammar (or syntax) and a vocabulary for user privacy statements and the interaction between the user and the service. In a P3P-less world, Internet users communicate directly with the web site or

service. In a P3P-enabled world, however, the direct link is severed and an intermediary is established to handle the numerous requests for user information. If the web site uses P3P privacy vocabulary, then the user agent can easily determine if there is a match between the user and the site (Birchman 1998).

The original goal of P3P was transaction-based: users get something by giving web sites personal information. The P3P Project has evolved into web users managing privacy preferences and the privacy policies of each web site (Hemphill 2002). The simple fact that users will not have to reenter the same personal data on numerous occasions to access sites and information is a small victory in itself (Birchman 1998). A simplified description of the basic P3P process begins when a P3P-compliant web browser acquires from a P3P-compliant web server a web site's proposal, for example, its statements of its practices. The web browser then compares the proposal with the web user's preferences.

If the proposal satisfies the preferences, the web browser and web server proceed (transparently to the web user) to communicate via the HTTP protocol. If the practices statement does not satisfy the preferences statement the web browser may: (1) attempt negotiation with the web server in order to achieve an outcome consistent with the preferences statement; or (2) notify the web user, enabling the web user to make a choice. The choices left to the user are: (1) provide informed consent to release the data, despite the mismatch; (2) attempt negotiation manually; or (3) withdraw from further interaction with the web site (Clarke 1998, July).

P3P: A Critique

P3P is primarily concerned with practices relating to data collection from the web user, the limitations on use and disclosure by the web site operator or its associates, and the openness of use and disclosure practices (Clarke 1998, August). Unfortunately, P3P assumes that some external mechanism exists to provide assurance that the practice will be conformed with. Any efficacy that P3P has is dependent upon the "substantive privacy rules established through other processes—be they result of regulatory, self-regulatory or public pressure" (Cavoukian, et. al. 2000).

The P3P protocol is dangerously myopic in five critical areas: (1) More specificity in declaring the purpose behind a web site's taking of the web user's information; (2) A means to establish a negotiated contract; (3) A means in the law for policing the contracts that are obtained; (4) A means for transitivity and universality of the protection of information; and (5) an IETF (Internet Engineering Task Force) definition that does not require the web and specifically HTTP (Thibadeau 2000). P3P cannot protect the privacy of users in jurisdictions with insufficient data privacy laws or ensure that companies will follow their privacy policies (Cavoukian, et. al. 2000).

As an example of the limitations that need to be addressed if P3P has a hope of succeeding, take Joe Surfer as an example again. Joe wishes to purchase a book online. His P3P-enabled web browser communicates with the P3P-enabled web server to pass his name, credit card, and address information to the site to complete his order. Basically, if the site wants Joe to feel safe about his transaction it can say that this information will be used for its 'current purpose' as explained on the page that he saw during checkout. Good. But, what if, buried on the fourth page of a very-wordy FAQ

page, the site tells the user in plain text that its 'current purpose' is to give Joe's credit card number to the first thief they can find. Under this P3P-enabled scenario, Joe has agreed to the 'current purpose', the site has fulfilled its obligations, and a lucky thief is going to become very rich. Likewise, a web site may employ a completely reasonable P3P privacy policy and simply choose to ignore its implementation once they have received Joe's information.

P3P alone is not sufficient by itself to protect web user's information. Effective protection is dependent on a multi-party, tiered privacy statement, in which layers of technology, organizational practices, and law combine to ensure reasonable behavior (Clarke 1998, August).

Recent Changes in Information Collection

More and more, companies are beginning to better define the line between their customer's personal need for privacy and their business needs to have access to information about their customers. A study sponsored by The Progress and Freedom Foundation ("PFF") looked at 85 of the Internet's most popular web sites—such as Amazon.com, CNN.com, and Yahoo.com—as well as a random sample of sites receiving more than 39,000 visitors a month in order to better understand the use of privacy policies and whether or not companies are taking privacy seriously or not (Fish 2002).

The study found that web sites are collecting 'significantly less' information about browsers than they were as reported in a 2000 study and the use of 'cookies' (small text files a site stores on a user's computer) by web sites to track browser behavior has fallen by 30 percent. Furthermore, sites are more likely to "offer visitors choices in how personal information might be used or shared outside the company." The survey cluster

that included the Internet's most popular sites showed that 93 percent of them offered visitors 'opt-in' choices, up from 77 percent in the previous study. While the PFF admits that these changes are largely evolutionary, not revolutionary, it is widely held that they signal a move in the right direction for consumer privacy advocates (Fish 2002).

Final Thoughts

Any organization that exists online today must face the reality that consumer privacy protection concerns are important, not only to the consumers they effect, but to their own survival as well. Organizations that provide high-quality privacy protection and offer their consumers something valuable in return for the information they provide will be able to truly reap the benefits of communication and community the Internet allows. Before any organization can make that leap however, they must first do a better job of educating their consumers about their data access needs and the methods and means they are using to collect that data.

A study by the Annenberg Public Policy Center of the University of Pennsylvania ("APPC") recently found that 57 percent of the adults that used the Internet at home believed "incorrectly that when a web site has a privacy policy, it will not share their personal information with other web sites or companies." More than half of the adults they surveyed—without knowing the contents of the policies—felt that simply having a privacy policy posted by a company meant that the company would guard their personal information and would not give it to anyone else. Any one that has ever signed up for an email newsletter and then started getting inundated with SPAM knows that this is not the case: most of the web sites that have such unsavory practices have privacy policies posted on their web sites (Turow 2003).

Percentage of adults who 'Agreed' or 'Strongly Agreed' with these statements:	
I should have a legal right to know everything that a web site knows about me.	94
I am nervous about web sites having information about me.	70
I look to see if a web site has a privacy policy before answering any questions.	71
I trust web sites not to share information with other companies or advertisers when they say they won't.	49
Web site privacy policies are easy to understand.	47

Organizations must take a much more proactive role in educating their users on online privacy truths, practices, and principles.

APPC also found that users are fairly positive and upbeat when it comes to the possible effectiveness of privacy policies (Turow 2003).

	Very or Somewhat	Neither Effective nor Ineffective	Not Very or Not at All
A law that requires web site policies to have easy to understand rules and the same format.	86	0.5	12
A law that gives you the right to control how web sites use and share the information they collect about you.	84	0.5	15
A law that requires companies that collect personal information online to help pay for courses that teach Internet users how to protect their privacy online.	74	0.5	25

Since no organization likes to be legislated into compliance if they can help it, they should take advantage of the opportunity to reduce consumer's concerns, educate them, and become compliant with both domestic and global privacy laws.

References

1. Birchman, Jeremy (1998). *Is P3P the Devil?* Retrieved August 26, 2003, from the University of Miami School of Law web site: http://www.law.miami.edu/~froomkin/sem97/birchman.html
2. Cavoukian, Ann, Gurski, Michael, Mulligan, Deirdre, and Schwartz, Ari. Center for Democracy & Technology (2000). *P3P and Privacy: An Update for the Privacy Community*. Retreived August 26, 2003, from http://www.cdt.org/privacy/pet/p3pprivacy.shtml
3. Consumers International Office for Developed and Transition Economies (2001). *Privacy@net: An international comparative study of consumer privacy on the Internet*. Retrieved August 26, 2003, from http://www.consumersinternational.org
4. Clarke, Roger (1998, August) Platform for Privacy Preferences: A Critique. *Privacy Law & Policy Reporter*, pp. 46-48.
5. Clarke, Roger (1998, July) Platform for Privacy Preferences: An Overview. *Privacy Law & Policy Reporter*, pp. 35-39.
6. Electronic Privacy Information Center (2000). *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*. Retreived August 26, 2003, from http://www.epic.org/reports/prettypoorprivacy.html
7. Fish, David (2002, March). On-line Survey Shows Progress on Privacy: Web Sites Collect Less Info, Provide More Notice & Choice. *The Progress & Freedom Foundation*. Retrieved August 26, 2003, from http://www.pff.org/pr/pr032702privacyonline.htm
8. Haller, Susan (2002, May/June). Privacy: What Every Manager Should Know. *The Information Management Journal*, pp. 33-40.
9. Hemphill, Thomas (2002). Electronic Commerce and Consumer Privacy: Establishing Online Trust in the U.S. Digital Economy. *Business and Society Review*, 107 (2), 221-239.

10. Kannan, P.K., Peng, Na, & Rust, Roland (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30 (4), 455-464.
11. Nakra, Prema (2001). Consumer privacy rights: CPR and the age of the Internet. *Management Decision*, 39 (4), 272-279.
12. Princeton Survey Research Associates (2003, January). *A Matter of Trust: What Users Want from Web Sites*. Retrieved August 26, 2003 from the Consumer WebWatch web site: http://www.consumerwebwatch.com
13. Thibadeau, Robert (2000). *A Critique of P3P: Privacy on the Web*. Retrieved August 26, 2003 from School of Computer Science, Carnegie Mellon University web site: http://dollar.ecom.cmu.edu/p3pcritique/
14. Turow, Joseph (2003). *Americans & Online Privacy: The System is Broken*. Retrieved August 26, 2003 from Annenberg Public Policy Center of the University of Pennsylvania web site: http://www.appcpenn.org