

## Online Privacy – Best Practice Pays

Online Privacy: it is at once both a libertarian's cause célèbre' and a thorn in the side of business and government. Consumers' passions erupt as marketers seek to 'leverage' market intelligence; sometimes questionably gained. Privacy and its attendant concerns are shaping where dollars are spent – particularly on the Internet – and businesses better sit up and take notice.

In a survey of the adult online population, conducted by the Customer Respect Group in February 2004, the importance of respectful treatment of consumers' privacy concerns was underlined by some dramatic findings. When survey participants were asked how much they care about a company's privacy policy when invited to enter personal information to a website, 22.4 percent responded that unless the website had a privacy policy, they would not offer the information. A further 26.6 percent echoed this sentiment by indicating that if they were unhappy with a company's privacy policy they would leave the site. (See table).

How much do you care about their privacy policy?		
Response	Chart	%
Don't care		0.4%
Don't look at the privacy policy	■	4%
Read the privacy policy sometimes	■	13.6%
If they don't have a privacy policy I don't provide information	■	22.4%
If I am not happy with the privacy policy I leave the site	■	26.6%
I usually input false data	■	3.2%
I look for secure (SSL) sites	■	29.8%

Why is it that some large corporations seem so out of tune with the deep seated concerns of some of their audience? The legalistic approach that some adopt when crafting their online privacy policy is both unfriendly and counter-productive. It serves only to foment anger and distrust while simultaneously perpetuating the 'us and them' culture so graphically exhibited by the major corporate scandals of recent years. Non-existent, inaccessible, or confusing declarations about how a company will treat the personal data of an individual is demonstrative of an uncaring attitude and is highly disrespectful of the customer the company purports to serve.

Let us consider the following. When asked to prioritize the reasons why they chose to abandon a website, one in every six respondents indicated that they were not happy with the company's privacy policy or the transparency of its business practices. The survey constituents were not the loony left, or a collection of disenfranchised liberal students hoping to watch capitalism crumble. These are the hard-working professional, clerical, technical and administrative employees who are keeping business moving.

The good news is that many companies are now putting the customer at the center of their online presence design, getting the balance right and reaping the rewards. Hewlett Packard is one company that is committed to online privacy and data protection. The tone of HP's online privacy policy is reassuring and informative. HP is a founding member of the BBB online Privacy Program and adheres to the EU/US Safe Harbor principles. The information provided is clear and written in plain English, avoiding legal-speak. There is a separate page containing detailed information on the company's use of cookies, including a general description of the technology and links to full instructions on how cookies may be disabled. Every page on the site provides a clear link to the privacy policy. A link to HP's privacy policy can be found at the bottom of the page on [www.hp.com](http://www.hp.com).

Good privacy practices are not limited to the technology sector. Other leaders in this area include Southwest Airlines ([www.southwest.com](http://www.southwest.com)), the Texas based low fares airline, BT Group ([www.btplc.com](http://www.btplc.com)), the leading UK telecommunications provider, Cincinatti Financial ([www.cinfin.com](http://www.cinfin.com)), and Investor's Business Daily ([www.investors.com](http://www.investors.com)). These companies are varied in their business objectives. Some have short privacy policies and other have extensive descriptions of how they use personal data proffered online. They converge through a basic philosophy of customer respect, explaining clearly how they use personal data, not choosing to sell or share data outside their organizations, and electing to have the customer opt-in, or consciously decide to receive communications from them.

Some of the worst examples would be almost laughable if the underlying sentiment was not so disrespectful. One of the largest media companies in the world chooses to have a disclaimer rather than a privacy policy. When the disclaimer link is clicked on the following text is displayed.

**Lorem ipsum dolor sit amet**, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae. Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium. . . .

Yes, it's Latin. No, even if you translate it it does not explain the privacy policy of the company. This standard piece of Latin text is what is referred to as 'pig-latin' and is often used by website designers as placeholder text until the real text has been written to replace it. I guess it wasn't that important to the company and they just forgot. Shame.

Here is another example of what not to do. The following is an extract from the privacy policy posted by one of the world's largest companies (with name deleted to protect the guilty).

By accessing the Site, you voluntarily, expressly and knowingly acknowledge and agree with all of the foregoing and further agree to each and all of the following: (i) such Information belongs to Company and is not personal or private proprietary information; (ii) such Information, wherever collected, may be processed, used, reproduced, modified, adapted, translated, used to create derivative works, shared, published and distributed by Company in its sole and absolute discretion in any media and manner irrevocably in perpetuity in any location throughout the universe without royalty or payment of any kind, without, however, any obligation by Company to do so; (iii) Company does not represent, warrant, or guaranty the Information or its processing, use, reproduction, modification, adaptation, translation, derivation, sharing, publishing or distribution, including without limitation the accuracy, reliability, security, or any other feature relating thereto or its processing, use, reproduction, modification, adaptation, translation, derivation, sharing, publishing or distribution; (iv) Company will try to provide you a way to review, correct or update the User Information you give Company directly, but cannot guaranty that such will be possible or that changes will be reflected throughout all uses of such Information; and ... blah, blah, blah ...

Ouch, my head hurts. This is just so hard. When you read through this many times you can figure it out but why make it this difficult? You can also see that the information 'may be ... shared, published and distributed' without your say so. Now it may well be that this company has no intention of distributing my personal data and I certainly hope that is the case. But you know what – I'm not taking that chance. I have choices. Click, I'm gone.

Good privacy practices make good commercial sense. As mentioned earlier, unless you get it right, half of your online audience will vote with their mouse-click and not provide the information you request. Not only have you lost a prospect or potentially an existing customer, but you will probably not know. When visitors to your site leave because of an unsatisfactory experience, two out of every three go to a competitor's site.

It is not hard to find out the best practices around online privacy. The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see. More information is available on P3P at [www.w3.org/p3p](http://www.w3.org/p3p).

The prevailing problem at the moment is that while a lot of companies have respectful policies, treat customers' data appropriately, request only relevant information, and only place cookies on a customer's PC to enhance the customer's experience, they fail to explain things adequately or with sufficient clarity to win the customer's trust. Be clear, be concise and be complete.

This is important to business and not just to eCommerce companies. Privacy is not just an issue for sites that transact online. Equally it applies to companies who use their Internet presence as a clearing house for information distribution, sites that re-direct you to partners or distributors for order fulfilment, or investor relations sites that provide shareholders with financial information. If you ask for personal data of any kind, ranging from my email address to my age, gender, income or credit information, then please tell me how you propose to use it and only ask for pertinent data.

#### About The Customer Respect Group

The Customer Respect Group is an international research and consulting firm that uses its Customer Respect Index (CRI™) methodology to help companies improve how they treat their customers online. It provides leadership in the objective and scientific measurement of a customer's online experience. By looking at more than 1000 Web sites across a spectrum of industries in detail, The Customer Respect Group has determined 60+ different attributes that combine to create the entire online customer experience. These attributes have been grouped together and measured as indicators of Simplicity (ease of navigation), Privacy (respects customer privacy), Attitude (customer-focus of site), Transparency (open and honest policies), Responsiveness (quick and thorough responses to inquiries) and Principles (values and respects customer data). Combined they measure a company's overall Customer Respect. More than 50 Fortune 500 companies have already adopted the CRI methodology to improve online customer satisfaction and loyalty. The Customer Respect Group is headquartered in Bellevue, WA. For additional information, visit [www.customerrespect.com](http://www.customerrespect.com)

Here are some guidelines that you might find valuable when crafting your own online privacy policy.

What To Do	How To Do It
Highlight your privacy policies	Prominent link on every page Link to 'Privacy' / 'Privacy Policy' not 'Legals' Draw site user's attention to it when they are filling out forms Use P3P
Make them easy to understand	Do not use legal verbiage Use "we" or "us", not "The Company" or "Company Name" Use clear, concise language
Give all of the information	Do you use cookies? Where? How? Why? How can the user control this? Do you record site usage? How does it affect the user? Where do you collect information / allow users to provide you with information? What is this information used for? Is it ever passed on to partners / 3rd parties, even to fulfil the request? Do you destroy data supplied after the request is fulfilled? Do you use the data to market to the person subsequently? Do you use opt-in / opt-out? If not, how does the user ensure he has control over what he receives?
Be respectful of users' data	Only use information for purpose it was collected Allow users to opt-in to things that might be of interest Consider what you might do in the future
Only ask for what is needed	Keep online forms as short as possible Allow users to submit inquiries without providing you with personal information other than a way for you to reply
Give the user control	Give users access to review / edit their own information at all times Allow them to update their preferences If they have opted in, with every subsequent communication, allow them to opt-out