

Making the most of online privacy policies

Much more than just a legal requirement, your online privacy policy can bring a business boost to customer confidence. Vanessa Smith Holburn looks at the issues.

Pro-privacy groups such as Junkbusters ensure that issues of data protection are always in the news. Indeed, companies as large and as web-savvy as Amazon.com have found themselves on the wrong side of such organisations – unceremoniously hauled up in front of authorities like the US Federal Trade Commission (FTC) – rightly or wrongly – to explain procedures and policies covering the retention, use and transfer of customer details. Increasingly then, all companies must decide how best to handle the issue of privacy. To ignore the increasing transparency demanded by society surely runs the risk of a ruined reputation – and is a missed opportunity for brand loyalty.

Communications a study carried out by KDB and Marketing UK found that while 97 per cent of UK top 500 companies posted a policy that brought it into compliance with current legislation, just 22 per cent offered an opt-in option for expressing marketing preferences.

ARE COMPANIES FAILING CONSUMERS?

The results of a Harris Interactive survey in February last year showed that consumers did not trust companies to handle personal information appropriately, with chief concerns being that data would be passed on to third parties without their permission, that hackers could retrieve their personal informa-

anxieties over data protection as a problem. Matthew Ellis of Ernst & Young's privacy practice explains that a privacy policy is a communication tool which "gives organisations the ability to clearly communicate their procedures and the use of customer data to help set expectations with customers and employees that allows them...to make assurances that what they say they are doing, is what they are doing". In this way, in many cases the policy will serve as an introduction to the corporation for the consumer – and will affect how that customer goes forward to relate to the corporation's brand. He argues "privacy gives you the ability, again and again, to create products and services that will enhance customer [relations] without violating their privacy."

Interestingly though, while consumers report that they are worried about privacy, many confess that they do not read the available policies. A Harris Interactive poll undertaken in 2001 suggested that nearly 64 per cent of online shoppers either do not read, or skim through, a website's privacy policy. Likewise, Jupiter Research findings (June 2002) suggest that only 40 per cent of online consumers read such statements.

Nick McConnell, UK general manager of e-mail marketing firm Digital Impact, and chairman of the UK Direct Marketing Association's E-mail Marketing Council, says "I suspect very few people actually read these [privacy policies], although they are becoming savvy to the phrase 'share data with third parties', which suggests their personal data will be found on the open market."

But Ellis disagrees. He believes that the number of people reading privacy policies is growing because consumers

"Consumers in the marketplace are much more aware of where their information is going and how it is being used, and I think that's driving consumers, more so than anything else, to read the [privacy] policy and look for some kind of trusted assurance."

- Mathew Ellis, Ernst & Young

Despite this new and intense focus on privacy policies, many companies still have room for improvement. A PA Consulting Group benchmarking study, published in June last year, revealed that while 74 per cent of the FTSE 100 websites studied gathered data on site visitors, over 50 per cent either had a privacy policy that the study rated as poor, or no privacy policy at all. In fact the results rated only 13 per cent of the companies as 'good' on their 'overall quality of privacy management'.

Likewise, six months ahead of the implementation of the revised EU Directive on Privacy and Electronic

tion and that online transactions were not secure. Shane Baylis, founder and managing director of KDB, says the KDB/Marketing UK results show that "companies are failing to recognise that consumer trust in e-business is faltering and the longer they postpone the inevitable, the worse the situation will become." He cites a recent KPMG report (see *PL&B UK*, May 2003, p.7) which suggests that data privacy is the consumer's greatest fear when shopping online and adds "this is simply not being addressed".

However, companies with an online presence need not see consumer

are becoming more aware of the issues around privacy, more technically savvy and because the media is increasingly communicating what can be considered as ideal standards and good practices. He argues “consumers in the marketplace are much more aware of where their information is going and how it is being used, and I think that’s driving consumers, more so than anything else, to read the policy and look for some kind of trusted assurance.” This is a view shared by Fran Maier, executive director of online privacy seal provider TRUSTe. She quotes a January 2003 BizRate survey which showed that 82 per cent of online shoppers have reviewed a privacy policy.

USE PRIVACY TO INCREASE CUSTOMER TRUST

Either way, if online privacy policies are viewed as an opportunity to build a relationship of trust with a customer base, rather than a chore (at a recent Deloitte & Touche European leadership forum, 70 per cent of e-business leaders believed that legal and regulatory hurdles hamper development), companies should look to encouraging all site visitors to access, read, understand and trust the published policy. This will ultimately transfer the trust achieved to the corporate brand. If privacy is of increasing public concern – and if at least a proportion of that public is reading the policies available – then it is high time organisations proactively used their policies effectively to build business, rather than just to maintain it.

In the past, online policies have been criticised for being too technical (indeed a *USA Today* article once suggested you need a PhD to understand some), too cluttered with legal jargon and too based on marketing and PR. Ellis explains “I think five years ago, privacy policies were much more technical than they are today, but I don’t think leading company privacy policies are marketing or technically driven.” He adds that if companies do not produce policies free from legalese and marketing “you’re not going to build the level of trust you need to have that long-term customer.”

Likewise, experts at retail technology solutions provider Hyperlink

Interactive always recommend that clients “provide a straightforward policy that says what they will and won’t do and provides clear access to the company in cases of doubt or concern.” Client strategy director, Stephen Morris adds “my personal opinion is that it is far more important that the customer can understand the policy and feel comfortable about opting-in than for the policy to be a typical legal document.” Like Ellis, he believes that the provision of clear privacy policies that demonstrate respectful behaviour to customer data “is essential for companies trading online – in terms of repeat business as well as customer service.” He describes privacy policies as “a manifesto for the customer relationship.”

...you can generate around 63 per cent more trust in your customers by using an independent auditing firm to verify that what you promise in your policy is really what happens

A POLICY TO HELP YOUR BUSINESS

But, alongside ensuring that your policy is accessible, how else can you ensure that your policy is working for both you and your customers? Maier recommends independent seal programmes like TRUSTe that can be seen to monitor sites – and act as a third party in disputes. Such endorsements can quickly amalgamate global legal requirements and evolve as the market needs. She says “58 per cent of online shoppers felt a non-profit, business or trade association was the best third party to ensure a company is honouring its privacy statement.”

However, the systems are more often seen as a “step in the right direction” rather than a catchall, according to Deloitte & Touche’s EU Data Privacy Coordinator Erik Luysterborg. Accordingly, Shane

Baylis points out that the KDB survey results shows that self-regulation often doesn’t work, even though he agrees regulators like TRUSTe can be effective.

Instead, Ellis tends towards deeper third party audit and verification, such as that earned from the AICPA (WebTrust), which gives the consumer “true assurance”. He believes that having “a form of independent verification on that [your privacy policy] is a great trust enhancer.” He also argues that you can generate around 63 per cent more trust in your customers by using an independent auditing firm to verify that what you promise in your policy is really what happens. If handled correctly, Ellis believes, privacy policies “should make a positive impact for both customer and organisation.”

READ IT AND STICK TO IT

But Luysterborg warns your policy must be more than a page of text, is not just an issue of “ticking the box” and that it must act as a guide for the actual “back office infrastructure”. He explains that “most of the companies who fell foul of data privacy regulations, did so not merely because they did not have data privacy policies...but because they had not acted in accordance with them.” He adds “you need to adopt a coordinated and pragmatic corporate approach and work out a plan to apply to your particular organisation’s processing and transfer of data.” Avoid a “paper tiger syndrome” he warns, which serves to lull companies into a false sense of security, believing that legal safety is simply obtained by putting a data privacy policy on display. Instead, he argues that policies should be ever changing, and that a one-size-fits-all formula cannot work. Perhaps then, it is companies themselves who have most to gain by reading their own policies?



AUTHOR: Vanessa Smith Holburn is a freelance journalist specialising in IT and new media law.