Web privacy will drive e-commerce forward

Report by Alan Pedersen

PRIVACY ENHANCING TECHNOLOGIES (PETs) could be the key to ensuring consumer confidence in online browsing and shopping. But a new report by the OECD suggests there is still work to do.

Recent polls have suggested companies could lose up to 40 per cent of their customers if they fail to take into account and act upon their privacy concerns. Last year, a poll conducted by *Business Week/Harris Interactive* showed that 63 per cent of non-online shoppers were worried over security and privacy. 41 per cent of online shoppers were unhappy that personal information may be misused, and 82 per cent were concerned that their online activities could be merged with identifiable data.

The early trail blazing days of the Internet threw up a host of companies, operating within an unregulated environment and employing unscrupulous tactics to the detriment of consumer privacy. It undermined public confidence in the Internet and has resulted in privacy issues emerging, along with security of online transactions, as a key reason for the slow development of e-commerce.

Although most consumers have some kind of privacy setting on their browsers, it is currently an all-or-nothing-deal; either leave yourself wide open to all sorts of tracking technologies and cookies, or have such high security that you will never get past the home page. But now, an increasing demand for more effective and customisable privacy has led to the emergence of PETs; technologies that empower consumers by allowing them to set their own privacy preferences when surfing the Internet. And because of the ease with which they can avoid websites with insufficient privacy policies, businesses are now finding themselves challenged to change their practices.

Some companies have seen the slow take-up of PETs as justification for sticking to their guns and maintaining the status quo. Last year's *Harris Interactive* poll revealed that only 15 per cent of web users have installed additional privacy enhancing software onto their computers. But following the August release of Microsoft's Internet Explorer 6.0 (IE 6), complete with privacy *enabling* software, businesses are being forced to sit up and take notice.

Already, according to PricewaterhouseCoopers, 12 per cent of US web users have adopted IE 6 and are potentially customising their privacy preferences.

Consumers are becoming increasingly aware of their rights and the ways in which they can protect themselves. Many organisations, therefore, now understand and accept that they have to prepare for a new way of dealing with customers. In fact, rather than a hindrance, many companies see a change in privacy policy as the ideal opportunity to promote good customer service and attract more business. Rigo Wenning, Policy Advisor at the World Wide Web Consortium (W3C), sees PETs as the key to achieving that target. "What you need," he says, "is a way of using technology to help you create a trust environment in order to help people make informed decisions and

Report on the OECD Forum session on privacy enhancing technologies (PETs)

In Paris on October 8th 2001, the OECD Forum gathered together representatives of government, the private sector, NGOs and academia. The Forum's objectives were to demonstrate and discuss the policy implications of PETs, challenges of implementation, and the education of both consumers and business. Included in the forum were demonstrations of a number of PETs that were compared and contrasted with the OECD's eight privacy principles. These principles are:

1: Collection limitation
2: Data quality
3: Purpose specification
4: Use limitation
5: Security safeguards
6: Openness
7: Individual Participation
8: Accountability

Of 135 sites surveyed only one site managed to meet five of the principles. None met all of the principles. The majority of sites only addressed one of the OECD's principles.

The OECD report, published in December last year is available in PDF or Word format at the following URL: www.olis.oecd.org/olis/2001doc.nsf/LinkTo/dsti-iccp-reg(2001)6-final

empower the user. And by empowering the user you enable business. That's why business needs PETs."

Drawbacks

There is a confusing array of privacy enhancing products available, most of which cater only for one specific aspect of privacy, leaving other aspects to other products. The OECD report details a survey carried out on 135 websites offering PETs. The survey found that, in general, individual PETs are not comprehensive enough to fully satisfy the privacy needs of consumers. None of the sites surveyed fulfilled all of the OECD's privacy principles, and only one site met five of its eight principles. In general, most offered protection for just one of these principle. Of the 135 sites surveyed, 45 per cent catered for collection limitation/choice, 40 per cent dealt with collection avoidance, and 27 per cent provided security measures.

The result is confusion for consumers. They want a technology that takes away the inconvenience of reading through what are often extremely long and complicated privacy policies. But if the technology they install creates more problems than it solves, then what is the point? Ideally, consumers are looking for one product that caters for all their needs, a product that is easy to install, simple to use and understand.

The creation of the Platform for Privacy Preferences (P3P) standard, developed by the W3C, could be the answer. Although primarily dealing with just cookies, rather than anonymous browsing, P3P is currently the clearest and simplest way for consumers to protect their privacy. Its incorporation into Microsoft's IE 6 ensures it will be widely available and become the dominant force in privacy enhancing technology, if enough consumers configure their software in an appropriate way.

But whilst P3P is widely supported by both business and some privacy groups, since its conception there have been critics of the technology. One such criticism, noted by the Electronic Privacy Information Centre (EPIC) in its paper *P3P: Pretty Poor Privacy*, is in its failure to interact with non-P3P compliant websites, regardless of how strong its privacy policy is.

Other critics suggest P3P does not go far enough. In 1998, the EU's Data Protection Working Party expressed concern saying that P3P "has not been developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalise lower common standards."

Many believe, that it is a misconception to regard P3P as a complete and total solution to online privacy. It should instead be regarded as one aspect, albeit an important one, of an organisation's privacy policy. Attempting to make P3P fully compliant with EU directives would be too complicated, so there is a need to maintain some simplicity. The W3C's Rigo Wenning says that "the only way you get things done on the Internet is to get them deployed. To get them deployed you have to keep things simple and the EU directive isn't simple at all."

David Klaus, Executive Director of the US-based Privacy Leadership Initiative, believes P3P still has some policy and technological issues to be resolved. But it should be noted that the technology is still in its first version. "The P3P vocabulary is already very powerful," says Wenning, "but we might think of extending it in some form." He went on to note that discussions and recommendations have taken place for possible future enhancements.

Barriers to implementation

Incorporating comprehensive and scalable privacy technology into a business is inevitably going to be a headache for any IT or compliance manager. There is no 'one-size-fits-all' solution to the problem; each company has a multitude of different demands and obligations to meet. Depending upon size, structure, and services delivered, the technologies and policies a company puts together will be varied. The OECD points out that sectors dealing in more sensitive data, such as finance, insurance and health, will encounter more demand for privacy than, say, online music suppliers or book retailers.

Larger companies will find it far more difficult to implement PETs simply because the complex structure of their organisations require a massive assessment of their information processes and management of data. A company like Deutsche Telekom, for example, not only operates a fixed telephony business, but also has mobile phone subsidiaries, cable TV units, and an ISP business. Implementation is, therefore, difficult for these companies because they have to spread their PET policies over

A brief guide to Privacy Enhancing Technology (PET)

The term PET was penned by John Borking, former Vice President of the Dutch Data Protection Authority. PETs consist of a range of web-based technologies designed for the enhancement of consumer privacy and security. The EU's Data Protection Working Party describes them as "a variety of technologies that safeguard personal privacy, notably by minimising or eliminating the collection or further processing of identifiable data."

PETs offer a range of functions from filtering cookies and tracking technologies, enabling anonymous web and e-mail browsing, to protecting data transfer by the use of encryption.

The majority of PETs are designed with the consumer in mind. Although some do cater for business purposes, very few cater for both.

Although there are a wide range of technologies offering different solutions, the most prominent is Platform for Privacy Preferences (P3P); an industry standard developed by the World Wide Web Consortium (W3C). P3P works by turning companies' privacy policy into machine-readable syntax. A user with P3P on their browser can then determine if the website they are looking at complies with their privacy needs. The result is a quick, standardised, and simple way of accepting or refusing a company's privacy policy without having to read through many pages of text.

a number of businesses, all supplying different services, across many countries, and to a variable customer base. But whilst smaller companies may find it easier to incorporate PETs into their business from a logistical angle, they are somewhat hindered by the cost factor. They are faced with the decision of whether or not to externalise or internalise the costs of implementation. If they minimise operational costs by placing the burden onto the consumer, do they risk being undercut by a competitor who has chosen an alternative approach? The OECD leans towards the view that companies who shoulder the burden of cost will benefit in the long term.

Education, according to the OECD, will be vital in helping business to make the right choices. Fortunately, because privacy has become so important, there are currently a number of consultancies and implementation guides that can direct businesses towards the right solution.

Advantage Europe?

PETs are designed to work within both a legislative framework and a self-regulatory environment. But, according to Rigo Wenner, Europe has a distinct advantage over the rest of the world because businesses are more accustomed to working in a highly regulated environment. If European businesses are quick to adopt PET solutions, Wenner believes they will be provided with a unique opportunity to place themselves at the forefront of e-commerce. "We are more accustomed to a much higher privacy level," he says, "and we understand privacy more in Europe. We are the privacy leaders in the world."

David Klaus, representing a US perspective, agrees that "in general, European companies are ahead of the US with regards to utilising privacy technologies designed to protect personal information maintained on networked computers." However, he also points out that the US has legislation on sensitive information such as medical and financial data, information on children, and government records. So he concedes that "US companies may be catching up with Europe in implementing protective technologies for computerised records." On the other hand, he believes that "European privacy protection schemes need to catch up with the US with regards to the protections afforded to sensitive personal information" in specific sectors.

A cautionary note

The consensus of opinion among experts is that e-business cannot afford to delay. The burst of the dotcom bubble has dented the e-commerce aspirations of many companies, leaving heavy investments in new technology unrewarded and unfulfilled. If they are to survive and flourish, there is an urgent need for businesses to change their thinking and respond to customers' demands. Adopting new privacy technology may lead to higher costs and the loss of potential and profitable marketing data. But if the alternative is losing customers to PET compliant competitors, these short-term burdens pale into insignificance.

The World Wide Web Consortium has detailed information about P3P. For more details visit: www.w3c.org/P3P/EPIC's P3P:

Pretty Poor Privacy report: www.epic.org/Reports/prettypoorprivacy.html. A deployment guide for P3P can be found at: www.w3.org/TR/p3pdeployment.

PricewaterhouseCoopers offers consultation on the implementation of P3P. Contact David Petraitis: Tel: +41 (0)227 107 509.

Japan, Singapore and Hong Kong aim to cut down on e-privacy violations

A number of countries in the Asia-Pacific region have introduced new laws or codes of practice aimed at cutting down on unsolicited advertising over the Internet.

Japan: On February 1st, the Japanese Ministry of Economy, Trade and Industry passed tough amendments to an ordinance regulating unsolicited mail over fixed and mobile internet connections. Companies will now be required to label e-mails as advertisements in both the subject and body of the message, and enable consumers to opt-out of future marketing campaigns. Far from being a voluntary code of practice, the amendments also include provisions for prosecuting companies (through fines and suspension of services) which fail to comply.

Singapore: Earlier this month, a Singapore Internet advisory body launched two codes of practice with the aim of protecting online personal data. The codes - the Model Data Protection Code for the Private Sector and the Industry Content Code - have been brought in on a voluntary basis with the hope of persuading organisations to adopt responsible web policies that protect the privacy of consumers.

Hong Kong: There have been attempts to cut down on mobile 'spam', through the introduction, in December 2001, of a code of practice on short messaging services (SMS). The voluntary code states that advertisements should be sent only with prior consent from the recipient. A spokesman for Hong Kong's telecoms regulator also said that in some situations, mobile operators could be permitted to block unwanted messages from being sent out to recipients who had lodged complaints.