E-privacy: a key asset for winning customer loyalty
What is e-privacy?
E-privacy, and privacy generally, includes the right of individuals to determine for themselves when, how, and to what extent, information about them is communicated to others. It also incorporates the individual’s right to opt in/opt out of unsolicited incoming e-mail marketing.

It is important to distinguish e-privacy from e-security. E-privacy is concerned with the usage of customer data. E-security is concerned with securing the flow and storage of electronic data or e-commerce to reduce the risk of fraud, loss and misuse of confidential information, right across the company.

Privacy is at the heart of the business and consumer relationship. It involves crucial issues about the power and value – and the use and potential for abuse – of personal information.
E-privacy is a critical enabler for e-business. Far from being a hindrance or a cost of doing business on-line, e-privacy is now emerging as a key differentiator in the digital marketplace – and an absolute prerequisite to building the high levels of consumer loyalty and corporate trust that enable e-business to flourish.

As organisations of all types expand their on-line presences and develop their e-commerce strategies, they are inevitably coming face-to-face with the pivotal issue of how to ensure the privacy of their customers. At the same time, a plethora of new data protection legislation is forcing firms to scrutinise the ways in which they collect, manage and use data to market goods and services to consumers.

As a result, awareness of e-privacy as an issue has never been higher – and is rising all the time. But much of that awareness is based on a fundamental misconception: that e-privacy is a barrier to on-line commerce. Under this mindset, e-privacy is viewed narrowly as an overhead, a hazard, or a threat to business. Nothing could be further from the truth.

Either way, these organisations are missing the opportunity to build value for stakeholders, which a strategic, proactive and customer-orientated approach to e-privacy provides.

This paper analyses the insights provided by three sources:

1. The e-privacy experts of PricewaterhouseCoopers (PwC) and Landwell, its correspondent legal practice.
2. The results of in-depth interviews carried out over six months, with senior business managers across a range of European and South African businesses.
3. Extensive research into consumer attitudes towards privacy on the Internet carried out during the end of 2000 (E-privacy solutions: bridging the B2C divide).

This analysis leads us at PwC to believe that e-privacy should now occupy a prime place on the agenda of every business involved with, or contemplating, on-line commerce.

Our message is clear. If you are managing an organisation in the e-business environment, your approach to e-privacy will determine your success or failure in getting close to your customers, winning their loyalty – and thereby building crucial competitive advantage in the marketplace. The choice is that simple.

― I take responsibility for e-privacy...I don’t want to go to jail for malpractice! ""

(Swedish software industry dot.com)
For any provider of goods or services via either traditional or web-based channels, customer loyalty is crucial. Increasingly, a prerequisite to securing this loyalty is getting relationship management right – which is why companies are investing so much time and resources in gathering, storing, managing and utilising customer preference data.

As a result, businesses are using increasingly sophisticated data collection, mining and segmentation techniques and carefully targeted direct marketing campaigns. The emergence of the Internet has opened up further opportunities for the extraction of detailed customer information, helping propel customer relationship management (CRM) to a new level.

Businesses have realised that greater knowledge and information about customers is a competitive differentiator – and that competing on price alone, without the service to support it, is not. Organisations that understand their customer base can meet and exceed customers’ expectations, both by enhancing and personalising their service, and targeting offers, such as product discounts, in return for loyalty.

Getting close – then closer still
But loyalty requires more than personalisation. It also needs trust.

Put simply, businesses that want to build loyalty by getting ‘close to their customers’ have to respect the privacy of those customers. And those that protect their customers’ privacy are in a far better position to fend off attempts by competitors looking to supplant that loyalty.

This is because customers do care about what happens to their personal details. Our research has demonstrated serious concern among consumers over their privacy on-line. Customer loyalty on the Internet is notoriously fickle – so businesses that do not provide reassurance about how they manage customer data are at a significant disadvantage when it comes to attracting on-line sales or loyalty.

What is more, privacy concerns dictate what consumers are willing to do on-line. There is a general unwillingness to divulge personally identifiable information, with only a fifth of consumers being “willing to share information with companies in exchange for products and services that better meet their needs.” This trust gap between businesses and consumers is widening as a result of privacy concerns (see box for more details).

Overhead or opportunity?
As our findings indicate, trust and transparency are now vital ingredients in maintaining and building customer relationships. Those players that succeed in engendering both elements are likely to stand head and shoulders above their competitors.

This means that businesses should not view e-privacy as an unnecessary nuisance or hindrance. On the contrary, e-privacy creates the opportunity to develop sustainable and profitable customer relationships. And applying rigorous e-privacy standards represents an opportunity to increase trust and further a business’s strategic objectives.
What are consumers worried about?
PwC recently commissioned an independent survey of consumers in Europe and South Africa to examine their attitudes towards privacy on the Internet.* Our research revealed that, in many cases, concern about privacy dictates and restricts what consumers are prepared to do on-line.

Cultural differences further complicate the position. For example, consumers in the UK, South Africa and Spain expressed high levels of concern, whilst others in markets such as Scandinavia are less worried. Our research also demonstrated that the more experienced users of the Internet were more inclined to worry about privacy breaches – indicating, perhaps surprisingly, that privacy concerns do not diminish with growing usage.

The research revealed that consumers’ concerns about their privacy centred on two main areas: intrusion, or the fear of being monitored or spied on; and the risk of misuse of information or fraud when buying goods or services on the Internet. One in three European Internet users rated their level of concern as “high”.

These findings have clear implications for marketing and CRM, since the fear of privacy abuse means real barriers stand in the way of free information flows between the consumer and businesses over the Internet. Generally, this fear means consumers are unwilling to divulge their personal information in a relaxed and open way. Only a fifth of consumers are “willing to share information with companies in exchange for products and services that better meet their needs.”

The majority of consumers – nearly three-quarters – prefer to opt out of providing information when they are given the choice to do so on the Internet. They choose to opt out because of a perception that they may receive junk e-mails or “spam” some time in the future.

*E-privacy solutions: bridging the B2C divide
To date, e-privacy has often been interpreted as a hazard or threat facing an organisation. Already, several household name companies have faced negative publicity for infringing the privacy of their customers. One bank recently discovered to its horror that certain customer account details were accessible from its general website. Others have incurred the wrath of consumers and regulators when passing on personal information held in databases to third parties or countries. As all these cases demonstrate, companies that fail to protect customer data can damage their existing reputations – or, for start-ups, create negative brand perception from day one.

On the other hand, an overly defensive approach to e-privacy also brings its own problems. It runs the risk that companies will miss out on maximising the value of their data by, for instance, unnecessarily curtailing marketing activities for fear of breaching regulations. In turn, consumers may then miss out on special promotions and price reductions that would interest them.

What companies need to do is adopt a positive and pro-active attitude to risk, and apply this to e-privacy. Research carried out by PwC found that executives perceive risk in either one of three main ways (see Figure 1):

- Hazard – the potential for a negative event to occur such as financial loss, fraud, theft, damage to reputation, systems failure and litigation;
- Uncertainty – a state where risk is hard to calculate in a formal way; or
- Opportunity – a proactive and offensive (as opposed to defensive) approach, under which actions are taken by management to achieve positive outcomes.

Each of the three elements of risk in the continuum is usually linked with particular functions within an organisation. Typically, ‘hazard’ risk is associated with compliance and prevention functions such as internal audit, financial control, insurance and security. Risk as ‘uncertainty’ tends to be the governing perception among senior finance officials and line management responsible for sales and commercial operations. Risk as ‘opportunity’ reflects the outlook of senior management – and tends to be embodied in corporate strategy.

Figure 1: The risk continuum
Risk and e-privacy: three levels of response

All three definitions of risk apply clearly in the context of e-privacy.

Failing to protect e-privacy poses the hazard risk of damage to reputation. Breaches of privacy have meant that various organisations around the world have found themselves the target of angry consumers and increasingly stringent regulation. Hazards include unwanted media exposure, litigation, and punishment because of non-compliance with new regulations. Indeed, company directors are often personally liable and face the risk of criminal convictions.

Our research has also found that e-privacy generates significant uncertainty within organisations. For some, e-privacy has become a high profile internal issue, tying up significant management time and effort. For example, organisations considering major operational change may be confronted with the task of re-engineering IT systems and processes in order to better protect privacy on-line. They could be faced with the complexity and cost of contacting every customer on their databases in order to confirm their “opt-in” status. They may even have cut back or cancelled marketing activities because of a lack of certainty about the legitimacy and legality of particular marketing activities.

“People in our marketing department see privacy as an obstacle and a nightmare...the need to obtain consent from the consumer for each and every marketing activity is very onerous on us...”

(Global airline)

Finally, e-privacy brings opportunity for business to make major gains. Sound e-privacy protection can create a virtuous circle in which both the business and its customers benefit. If customers trust the business, in return they will trade better quality personal information. This allows the business to address customer needs more accurately -- and, more cost-effectively. All these factors mean that organisations that engender greater trust through sound protection of privacy are more likely to get closer to customers, so retaining their loyalty -- and their business.

In the next section, we discuss how firms can begin to view e-privacy in a strategic way, and offer some practical steps to ensure early build-in of e-privacy principles and practices.
To achieve the full benefits of an e-privacy strategy, companies would ideally have incorporated e-privacy into their systems, processes and management culture right from the start. Nonetheless, once the concept is embraced, significant gains can be made in thinking and acting strategically, and for the long term.

We do have an e-privacy officer – because you have to nominate someone by Swiss law and he looks after the security side of the business. But all of us take responsibility for maintaining e-privacy as we would be liable if anything went wrong. It is not too much of an issue for us as it is something that we sorted out early on when the company was set up.

(Swiss travel dotcom)

The problems of short-term thinking are frequently evident. Firms have had to wipe databases, pay fines to data protection authorities, and risk “naming and shaming” incidents because of a failure to comply with e-privacy issues fully from the start.

Another consequence of failing to build in e-privacy is an excessive risk aversion. Our research shows that some organisations ‘play it safe’ by curtailing or even cancelling activities that could bring them significant gains. Others question whether personal data needs to be collected in the first place.

We have also found that companies based in one country may think twice about expanding into another for fear of unwittingly breaching local regulations. Again, this means that companies are missing the opportunity to exploit databases that they’ve invested time and money developing.

Strategy and customer relationships

A further benefit is that early build-in creates a wider range of strategic options for the future. At present, some companies may not have an immediate strategic imperative to make e-privacy a business priority, because they have simple and relatively low-value customer relationships that work fine for their current business model. However, such companies considering moving to new business models and/or planning on deepening their relations with customers, perhaps drawing on cross-selling techniques, direct marketing and more sophisticated CRM practices, should build in the required level of e-privacy now.

As confirmed by our research, there is no one-size-fits-all strategy for achieving optimum levels of e-privacy. Companies have to make choices depending on the complexity and value of their evolving customer relationships. Often they may want to migrate towards the top right of the matrix, (see Figure 2), but by no means will that always be the case.
Organisations in industries such as insurance, airlines and mobile communications are engaged in relationships with multiple types of customer (see our category Happily married). To prevent or reduce customer churn, they may have launched loyalty schemes, and engaged in cross-selling and direct marketing. Their customer relationships are both complex and high value. For example, an insurance company is likely to be marketing to many different customer types, across product and business lines. At the same time, from pricing a product to investigating a claim, it also requires detailed personal information from its customers.

Other types of organisation, such as those selling simple commodity products, have relatively simple operations and simple relationships with customers (see our category, Brief encounter). They perceive little need to delve into consumers’ lives and therefore do not use loyalty schemes, customer relationship management systems, or complex data segmentation. Basic and mainstream advertising is preferred to direct marketing, which may be considered intrusive and a breach of privacy. Many dotcoms which fall into this category may well have more basic business priorities that take centre stage, such as winning new customers.

“We do have purchase-history data, but don’t use it much. We don’t ask for any of the types of data that are sensitive...all we need is a name and delivery address – there is no problem with getting this.”

(CPO, on-line operation of major bricks-and-clicks e-tailer)

Further quadrants in the matrix are occupied by companies with simple but high-value relationships with customers (banks – see the Friends category), and firms with complex but low-value relationships (see the Working relationships category).
Practical steps

Integrating e-privacy strategy with the overall business strategy is imperative for all organisations. Our research has revealed a number of widely applicable practical steps for firms to ensure early build-in of e-privacy. We have identified the following six issues:

- Put the consumer in control
- Adopt the highest standards of compliance
- Develop an enterprise-wide approach and resolve internal conflicts
- Address the issue of legacy systems
- Re-engineer data management
- Forge trust relationships with regulators

Put the consumer in control

Some of our interviewees expressed doubts that they could easily reassure consumers about their commitment to e-privacy. Some believed that consumer trust is too intangible to be easily influenced by the actions of one company. In contrast however, more organisations are now taking a lead by being open and clear with the consumer from the outset.

The ultimate way to safeguard e-privacy is to empower the customer. The key is to gain consent for data collected and move towards a model of ‘permission marketing’.

One of our interviewees took the step of allowing consumers to create their own profiles. These profiles are created, filled in and accessed (via a secure site) by the customer, not the company. Customers are obliged to provide very basic data, such as name and address, but after that may provide as much or as little additional data as they wish. From there on, the customer maintains the profile and can access, edit, or delete it at any time.

“In principle, as long as one explains why one wants data and obtains consent, one can ask any number of questions and hold all types of data if these two conditions are met…”

(German data protection commissioner)

Elsewhere, companies are creating greater corporate transparency by incorporating messages about security and privacy into the more general content of their web-sites. Rather than confining their entire e-privacy message to a web-page or two, some firms are communicating their approach through more general branding content, terms and conditions and delivery procedures.
P3P: putting the consumer in control

P3P refers to the Platform for Privacy Preferences Project, a new industry standard established by the World Wide Web Consortium (W3C). Its aim is to enable privacy practices and policies of individual web-sites to be expressed in a user-friendly, standardised format to permit consumers to make informed choices about their preferred levels of privacy protection. In time, the hope is that this will help foster and increase consumer trust and confidence in the web.

With P3P, users can quickly tell if web-sites are using cookies – small data files placed onto a user’s computer – which can then identify a user when revisiting a particular site. For instance, a new privacy tab has been added to the ‘Internet Options’ in Microsoft’s Internet Explorer Version 6, allowing users to block cookies. A small privacy icon appears on screen to confirm this. This removes the need for users to have to wade through individual privacy policies at each web-site.

However P3P is about much more than blocking cookies. The wider objective is to educate consumers about privacy, enabling them to make informed decisions regarding data disclosure. It does this by automating the process whereby consumers make choices, and giving them information about policy before any personal information is released. Companies that implement the P3P standard are obliged to store information about the data they collect, and convey it automatically to the user. Where there are discrepancies between a site’s practices and the user’s preferences, the user can be automatically alerted.

P3P is intended to be complementary to existing legislative and self-regulatory programmes. It cannot provide absolute assurance that web-sites act in accordance with their policies, or act as a silver bullet for securely controlling, transferring, and storing personal data. However, some firms may build P3P-aware tools that combine data encryption and security in their functions.
Adopt the highest standards of compliance

E-privacy is currently subject to a plethora of competing standards. Whilst Europe has been at the forefront in developing legislation, the interpretation and implementation of common legislative sources, such as the Data Protection Directive, has varied enormously. As a result, organisations are finding that they may need to implement differing e-privacy measures to ensure local compliance.

One example of this variance is the continuing debate between proponents of the ‘opt-in’ and ‘opt-out’ approaches to seeking consent for the collection and use of personal information. Opt-in consent is gained positively when consumers tick a box. Opt-out, on the other hand, means consumers may receive marketing material if they do not tick a box specifically declining acceptance. Such differences have meant that the European Commission is already considering further privacy legislation to ensure the harmonisation and standardisation of the differing regimes.

PwC believes that such debates are increasingly becoming side issues, and can distract organisations from moving upwards on the risk continuum, from implementing compliance to the opportunities with customers that e-privacy brings.

Organisations that want to ensure customer loyalty should aim to adopt the highest possible standards, and the highest possible alignment with the customer’s view of e-privacy. It makes sense for companies to put themselves in the position of consumers and address their concerns. Consumers do not want to see their data being used or processed for reasons that are inconsistent with the purposes for which it was freely given. Consumers want to be reassured that only those organisations collecting their data will use it, and no other, and that they will keep it secure and accurate. Giving consumers this reassurance will undoubtedly enhance an organisation’s profile and standing.

Seals of approval are not the answer – just the first step

Seals of approval are certificates issued by private bodies. They signal to users that a particular company web-site has an independently monitored privacy policy, and that the company has pledged to abide by such self-regulatory standards. However, many argue that seals are ineffective, and there is a growing consensus that they can only be one step towards facilitating e-privacy.

To begin with, there are many competing seals of approval. This tends to confuse consumers, undermine confidence in any particular one, and compromise the value of seals in general. Second, only a minority of firms have chosen to adopt them. For companies that have adopted seals of approval, the dilemma has been which seal to apply. As technology develops, will the seal that organisations select today be capable of providing the level of privacy such organisations want to apply tomorrow? Also, does applying a seal give implicit approval that such seal that has the highest standard and should be applied by all organisations?

Perhaps most importantly, seals cannot protect consumers if their privacy is breached. Unlike national regulatory authorities, privacy certification associations have limited powers to enforce consumer rights.

Our survey on consumer attitudes to privacy discovered that security features, such as seals, do not particularly inspire consumer confidence. For instance, in countries such as Germany and the UK, only 52 per cent and 57 per cent of respondents respectively felt reassured by seals to protect their privacy.
Develop an enterprise-wide approach and resolve internal conflicts

Early build-in of e-privacy is not just a matter of technology. It is also an issue of management culture and consensus. Organisations that are able to address points of conflict internally (by creating multidisciplinary teams to promote enterprise-wide awareness) will be better placed to make progress.

Our interviews with business leaders often revealed internal conflicts between legal and marketing departments. Marketing feel that over-cautious in-house lawyers charged with compliance responsibilities prevent them from doing their jobs. In this scenario, marketing departments can feel paralysed by over-regulation while lawyers simply want to ensure that their organisation’s marketing department adopts privacy standards and works within them to their organisation’s advantage.

“I have a problem with making our marketing people take e-privacy seriously. Low consumer confidence is often regarded as someone else’s problem. I will continue to keep an eye on what they are doing.”

(German mobile communications company)

Similarly, Chief Privacy Officers (CPOs) can find themselves in a policing role inside the organisation. In extreme cases, CPOs may be at loggerheads with marketing departments that are unaware of the dangers they are posing to the brand – and even to the organisation itself – through continuing to carry out particular marketing practices, and ignoring the advice of the lawyers and the CPOs.

“Marketing tries to be innovative but ends up pushing the limits of what is acceptable on e-privacy...the marketing department has a good understanding of the e-privacy laws and do their best to get around them. Ultimately the lawyers and IT security people determine what marketing are allowed to do.”

(Finnish insurance company)

Address the issue of legacy systems

Firms that continue to use legacy systems, but attempt to ‘bolt-on’ e-privacy solutions, are likely to run into significant problems in the future.

Legacy systems continue to hamper many organisations in their e-privacy efforts. Some insurance companies, for example, still rely on mainframe computer applications that are 20 years old, for the simple reason that they can still manage and process huge volumes of data speedily enough for business requirements, and are compatible to a degree with other systems.

However, such legacy systems often lack the flexibility to register and process individual customer data preferences, such as opt-in and opt-out choices. In addition, data contained within such systems often pre-dates and may not, necessarily, be compliant with existing legislation. Whilst it may have been possible to collect certain data in the past, companies must address the issue of how to use that data in the context of both current legislation, and the company’s desired relationships with the customer. As a result, these systems cannot provide the depth of e-privacy needed for customer-facing staff in their marketing operations.

In addition, legislation implemented following the Data Protection Directive, allows customers, in certain circumstances, the right to ensure that data held about them is accurate and up-to-date – a further demand that legacy systems are just not geared up to handle. Similarly, old or unsophisticated databases cannot cope with new segmentations of data.

Legacy systems can undoubtedly create problems with regulatory compliance; but, more fundamentally, they can also stand in the way of strategic opportunity – for organisations, and for their clients.
**Re-engineer data management**

E-privacy requires a new approach to data management. There are four crucial areas to address: data segmentation; internal data access; data transfer; and the right of data access for consumers (including access to data storage, whether in a company’s own systems, through a third party, or on the Internet).

**The need to re-segment data**

Traditional lines of segmentation, such as purchase histories, have long enabled companies to target specific customers with particular discounts and offers. But such lines of segmentation are rapidly becoming inapplicable in the face of new e-privacy regulations.

To comply with regulations, companies now need to re-segment data along new lines of opt-out/opt-in. Data mining and marketing activity through old lines of segmentation are now increasingly useless. Loyal customers may choose to opt-out, for instance, stopping targeted marketing dead in its tracks. The marketing department needs to address this issue, such as making it more attractive for these customers to opt-in.

**Internal data access issues**

E-privacy changes the rules of data access, meaning that certain people have access to particular new and old data, while others do not. For instance, customer-facing staff have to know whether a customer has opted-in or out of receiving marketing material but they do not need access to the customer’s personal information.

Organisations should ensure that only those employees requiring access to clients’ personal data for the performance of their responsibilities are granted access. To do otherwise may expose the organisation to risks, should employees be granted free access to all data. Until new data protection regulations came into force, such distinctions did not have to be in place within organisations.

Similarly, new data management requirements mean that protecting customer data may clash with the drive to form a ‘single view’ of customers for CRM purposes.

Compliance with new legislation, such as the Data Protection Directive, means the separation of personal data, rather than its centralisation. Organisations that have formed centralised databases, with a view to increasing revenue per customer through cross selling and targeted marketing, could find that such a concentration of personal information about customers may become a liability.

A best practice response may involve the sanitation of such data or the construction of internal ‘Chinese Walls’ so that various marketing and sales departments are unable to access any unauthorised data for their own specific purposes.

“We have lots of databases, some of which contain confidential items like health data. It is all very compartmentalised...customer services and claims people can view all the data but marketing cannot...this restricts what marketing can do in the area of matching databases and cross-selling.”

(Finnish insurance company)
**Data transfer**

In the context of privacy, international companies collecting personal information now face the challenge of keeping close control of its movement across national borders. The implementation of the Data Protection Directive in Europe, and similar laws elsewhere, has meant a limitation on the transfer of data to countries without adequate protections. The transfer between countries with different regulatory regimes now has a new dimension. Switzerland and Hungary have been formally recognised by the European Commission as having adequate data protection laws in place and hence transfers are allowed.

But what about transfer to the US? In this regard, the *Safe Harbor* principles are intended as a means for organisations to voluntarily implement privacy solutions, which are deemed by the European Commission to meet the “adequacy” standards for Europe. However, it must be emphasised that it is voluntary and only a few organisations have signed up. Also individuals do not have the means of redress, rather is it the US Department of Commerce and Federal Trade Commission who have to act as enforcer. (Further information can be found at: http://www.export.gov/safeharbor/).
When it comes to e-privacy, matters are even more complicated. A web-site can be hosted anywhere in the world and can collect personal data either explicitly or surreptitiously. The degree of privacy protection is determined by who is doing the collecting – and the laws with which they are obliged to comply.

An old issue that is now being re-examined is the buying and selling of databases, or customer lists. The widespread realisation of the asset value of personal information has created a ready market for databases. However, privacy concerns have triggered closer regulation and scrutiny of this market – including the commercial use of data collected by governments and public bodies. Clearly, a consumer may feel it to be a breach of privacy when personal information given to one organisation is passed onto a third party without their consent, resulting in the receipt of unwanted marketing material.

The right of data access for consumers
As mentioned earlier, organisations now need to ensure that the customers, about whom it collects data, have access to their personal data files and records upon request. This may sound easy enough in theory, but can be hampered by poor internal organisational procedures and administration – and failure to comply may be considered a breach of regulations.

Forge trust relationships with regulators
Relationships between companies and regulators are important. Companies that approach regulators in an open and responsive way are far more likely to overcome difficult e-privacy legal issues. Some of our clients view the dual role of the commissioners as both an advisor and enforcer as a block to this openness.

“If we go to the authorities and ask for more guidance, we run the risk of being fined or getting into trouble in some way, even though we may be in the right.”

(Global airline)

Companies must work on a strategy, which will lead to positive relationships with regulators, as well as minimising regulatory hazard.
Relationships between business and consumers are changing. Consumers expect socially responsible behaviour, and they expect businesses to be transparent and accountable in their dealings with them. It is becoming clearer by the day that such considerations increasingly influence where consumers shop, what they buy and which brands they trust.

I think the future will become even more complex... with more competitors, more alliances, more selling through on-line portals, more attempts from marketing to push the limits. Systems will become more complex, and there will be more risk of errors... I think consumer confidence in Finland will go down in the future, not up, for these reasons.

(Finnish insurance company)

In this environment, it is logical that consumer expectations regarding e-privacy are on the rise. As consumers become more aware of their rights, they will automatically expect high standards of privacy protection – and begin to hold businesses to account for perceived lapses in the management of their personal information.

At the same time, we live in a world where our ability to process, manage and share information has grown tremendously. The Internet's open and accessible character has greatly facilitated information flows across geographical borders and between different economic groups. Clearly, this strength is also a potential source of conflict in the form of privacy infringement.

Branding: privacy and respect
These trends present organisations with both risks and opportunities. Businesses that get it wrong face the risk damage to their reputation. Organisations deemed to be secretive and underhand will turn consumers away from their brand. But businesses that get it right can develop valued relationships with customers founded on respect for privacy.

These factors, and others discussed in this report, mean that there are very real grounds for incorporating e-privacy into business strategy. More specifically, a clear rationale is developing for firms to incorporate e-privacy into their brand proposition.

In this respect, banks and other financial institutions may provide a model of best practice. More than most, such organisations view privacy as underpinning the trust consumers have in the brand, and so making a fundamental contribution to the brand value. Creating trust and reassuring consumers is at the heart of what they do.

This does not mean pledging to guarantee e-privacy through grand public statements. What it does suggest is a sophisticated insight into the links between security, trust, e-privacy and brand value. Banks, on the whole, are not willing to sacrifice privacy protection for short-term gains. They take a long-term strategic view of privacy. Not surprisingly, perhaps, they enjoy higher levels of consumer trust.

PwC’s consumer research, carried out in October 2000, found that, banks were the most trusted commercial institutions, coming second only to public health authorities as the most trusted institutions of all. Clearly, banks have not got everything right. But considering the volume and sensitivity of the personal data they hold, their reputation for privacy has proved, so far, to be resilient.

There may be a lesson for other organisations looking to tap into the huge potential of e-business. Privacy in general – and e-privacy in particular – matters to people. As our case study on Buongiorno illustrates, there are real benefits in looking at e-privacy through the customer’s eyes, and building that perspective into the strategy from day one. In the long run, we believe the winners in the on-line marketplaces of the future will be those players who do exactly that.
Research profile
During the first six months of 2001, PricewaterhouseCoopers commissioned arnold+bolingbroke to conduct independent research into the views of major European and South African corporates on the key issues surrounding their e-privacy strategy and its implementation. In addition, the views of a selection of data protection commissioners across Europe were also sought on this topic. Interviews were conducted in Belgium, Finland, France, Germany, Italy, Netherlands, South Africa, Spain, Sweden, Switzerland, and the UK.

The business interviews were conducted as a follow-up exercise to research conducted in October 2000, which looked at consumer attitudes towards privacy on the Internet in twelve European countries and South Africa. The consumer research highlighted that businesses which struggle to protect customer privacy will find it hard to increase on-line sales and ‘get close to the customer’.

The business interviews were conducted to communicate this finding to organisations and capture their responses as to how this has or will influence the importance and direction of their current and future e-privacy strategy.

The companies included in the study are mostly well known strongly branded industry leaders or players and the interviews were conducted with a range of responsibilities including heads of e-commerce, e-privacy and marketing.

In total 33 qualitative interviews were conducted across Europe and South Africa. Respondents were spread across a number of vertical sectors and included Telecommunications, Utilities, Financial Services, Pharmaceutical, Retail, Travel and Airlines. All respondents are currently participating or involved in selling their products or services on-line.

For further information regarding PricewaterhouseCoopers and the content of this report, please contact –

David Petraitis (Geneva/Switzerland) Tel: +41 (22) 748 51 11
Karel De Baere (Ghent/Belgium) Tel: +32 (9) 286 82 11
Latika Sharma (Landwell) Tel: +44 (20) 7 212 1616

www.pwglobal.com/ebusinessinsights