EU Electronic Communications Privacy Directive – a step closer

By Gary Brooks

THE BUSINESS COMMUNITY needs to start preparing itself for the impending EU communications directive and the impact it will have on the e-commerce industry. Gary Brooks, of Berwin Leighton Paisner, looks at the issues that lie ahead.

On July 12th 2000, the European Commission adopted a proposal for a directive concerning the processing of personal data and the protection of privacy in the electronic communications sector. The draft directive is currently awaiting a second reading before the European Parliament, and is likely to be adopted in June or July of this year.

This article concentrates on two of the most controversial aspects of the directive, namely the use of cookies and similar devices to collect personal data, and the use of e-mail for direct marketing purposes. The European Council of Ministers and the European Parliament have adopted contrasting positions on these issues during the passage of the legislation.

COOKIES

A cookie is a small text file sent by a web server to the user's Internet browser, which enables the server to then collect information from the browser. A cookie will normally be used by a website operator to identify and authenticate the user and to tailor the website for their visit.

The European Parliament favoured an 'opt-in' approach regarding the use of cookies, whereby businesses are required to obtain the prior consent of website users before they can use cookies. Whilst the European authorities recognise that cookies can be a 'legitimate and useful tool' for businesses wanting to enhance a consumer's visit to their website, they are also viewed as a threat to personal privacy as they collect data on consumers' Internet browsing patterns without requesting consent.

> "Cookies are an essential piece of Internet browsing architecture"

The approach taken by the European Council – which now represents the latest text of the draft directive – is to allow the use of cookies. This is on condition that the individual receives, in advance, clear and comprehensive information about the purposes of the processing via cookies, and is also offered the opportunity to refuse such processing. The Council's approach is more favourable than that of the Parliament, but it would still pose compliance problems for e-businesses.

Commercial website operators will obviously be very reluctant to replace their home page with a legal warning about the use of cookies every time someone attempts to access the site for the first time. If implemented, the measure could have an adverse impact on online advertising sales, the primary revenue source for many Internet businesses.

Cookies are an essential piece of Internet browsing architecture. Critics have argued that this directive is further evidence that legislators and regulators fail to understand the use of cookies in assuming that they infringe consumers' privacy.

The long-term solution with regard to the privacy issues surrounding cookies may lie with Privacy Enhancing Technology. Almost all Internet browsers allow a user to prohibit cookies by customising their cookie settings. This issue may best be resolved by shifting responsibility for the protection of privacy rights to the consumers themselves rather than leaving businesses struggling to comply with restrictive legislation.

MARKETING E-MAILS

The version of the directive submitted by the European Council to the Parliament on February 5th – which, at the time of writing, was being disputed in a draft paper prepared by the Parliament's Committee on Citizens' Freedoms and Rights – currently favours an 'opt-in' approach in respect of unsolicited direct marketing e-mails

(i.e. such e-mails can be sent only to individuals who have given their prior consent). It does, however, allow for e-mails to be sent out to existing customers when advertising products or services that are similar to those purchased by the customer in the past. In the latter case, customers need only be given the right to opt-out of receiving such communications.

This raises a potentially difficult compliance issue; namely that the process of targeting existing customers by e-mail with substantially different products from those previously bought would be regarded as a privacy breach. It is likely that the Parliament will wish to remove this requirement, so that businesses targeting existing customers will have to provide an opt-out, irrespective of whether or not the product is similar to those previously purchased.

The practice of "list selling" would also be affected (where a business makes a profit out of selling e-mail addresses to other businesses which then use those addresses for direct marketing).

Businesses engaged in direct marketing by e-mail should be aware of the e-commerce directive which should have been implemented by Member States by January 17th 2002. Article 7 requires unsolicited commercial e-mails to be 'clearly identifiable' as such. In some member states, businesses may require further guidance on what 'clearly identifiable' means. It can probably be assumed that the 'Subject' box of the e-mail must always make it clear that this is a commercial communication.

Conclusion

The broad aims of the draft directive are to be welcomed in seeking to clarify the law in these two contentious areas. However, the European Council's proposal regarding marketing e-mails involves a degree of subjectivity in deciding whether a product is 'substantially different' from those previously bought by the customer. Businesses should be aware that some data protection authorities may interpret the law by looking at issues from the point of view of the individual, so that the sender of the e-mail should consider how that message will be perceived by its recipients.

As far as cookies are concerned, it is difficult to predict how the directive will be implemented across member states. Any business wishing to 'stay ahead of the game' should inform consumers in their privacy policies not only of the purposes for which it uses cookies, but how a user can switch off cookies e.g. by visiting the 'Help' menu on his/her browser.

The text of the Common Position of the Council is available at: www.register.consilium.eu.int/pdf/en/01/st15/15396-r2en1.pdf

Gary Brooks is a solicitor specialising in data protection issues at Berwin Leighton Paisner in London.

American security agency calls on Internet content providers to conduct security review of website content

By Eugene Oscapella

In an important reminder to many governments and businesses, the US National Infrastructure Protection Center (NIPC) has warned Internet content providers of the possible misuse of information displayed on their websites. Among its concerns are the posting of personal data and use of data from a website to target personnel or resources.

An NIPC Internet Content Advisory, dated January 17th, cautions that, "Among the information available to Internet users are details on critical infrastructures, emergency response plans and other data of potential use to persons with criminal intent. The National Infrastructure Protection Center has received reports that infrastructure related information, available on the Internet, is being accessed from sites around the world. While in and of itself this information is not significant, it highlights a potential vulnerability."

The Advisory encourages reviewing website data and offers some guidance online:

When evaluating Internet content from a security perspective, some points to consider include:

1. Has the information been cleared and authorised for public release?

2. Does the information provide details concerning enterprise safety and security? Are there alternative means of delivering sensitive security information to the intended audience?

3. Is any personal data posted (such as biographical data, addresses, etc.)?

4. How could someone intent on causing harm misuse this information?

5. Could this information be dangerous if it were used in conjunction with other publicly available data?

6. Could someone use the information to target your personnel or resources?

7. Many archival sites exist on the Internet, and that information removed from an official site might nevertheless remain publicly available elsewhere.

For further information:
http://www.nipc.gov/warnings/advisories/2002/02-001.htm