News in brief

Research carried out by the Business Software Alliance (BSA) has revealed that online shoppers are equally concerned over privacy as they are over security. A survey of 4,000 consumers in the UK, US, Japan and Mexico showed that while 56 per cent expressed fears over online security breaches, 56 per cent said they were concerned that businesses might sell their data on to third parties. 46 per cent were concerned that disclosing personal data would lead to unsolicited spam e-mail.

The UK Advertising Standards Authority has upheld a complaint against mobile phone retailer, Carphone Warehouse, for sending unsolicited SMS advertising. The company was judged to have bought in a list of mobile phone numbers that were collected without consumers' prior consent.

The US-based Association for Interactive Advertising has published a set of best practice guidelines for e-mail marketing. The guidelines provide advice on obtaining consent from consumers when collecting data, list suppression, data accuracy, and dispute resolution. See www.imarketing.org for more details.

Auditors in the US state of Virginia have found that state-owned computers have been sold on to third parties without adequately ensuring that personal data has been removed.

Virginia's State Auditor of Public Accounts randomly tested 25 computers that were to be sold and found that 22 (88 per cent) still contained sensitive information such as credit card details, student records and employee evaluations. The data exposed was either not deleted at all, or was easily restored using data recovery software.

Virginia has since stopped any further sale of computer equipment until new security procedures have been put in place.

European Court delivers landmark privacy ruling

Clare Goodman and **Mark Watts** explain how a recent ruling from the European Court of Justice (ECJ) could have important implications for the business community.

On November 6th, the European Court of Justice ruled that a Swedish District Court was entitled to fine a church worker SEK4000 (approximately €400) for failing to obtain the consent of individuals before writing about them on her home page. It is perhaps not surprising that it was held that the Data Protection Directive does apply to the publishing of personal data on the Internet, however inoffensive or trivial. However, what is more surprising is that this case about a parish magazine might have implications for multinational corporations sharing personal data about their employees and customers with group companies outside Europe.

The facts

In one of the first cases to consider the Data Protection Directive, the ECJ found that Swedish church worker, Bodil Lindqvist, who published a local parish magazine on her own personal website was bound by the Data Protection Directive.

Lindqvist set up Internet pages on her home computer to help parishioners preparing for their confirmation. The pages included information about other parish workers, such as their names, hobbies and telephone numbers. But Lindqvist had not obtained the individuals' consent. Criminal proceedings were brought on the grounds that she had:

- processed personal data without notifying the Swedish data protection regulator
- processed sensitive personal data without authorisation (Lindqvist reported that one parish worker had injured her foot and was working half-time on "medical grounds"); and
- transferred personal data to a third country without authorisation.

Scope of the Data Protection Directive

It is not surprising that the ECJ found that placing personal data on a website constitutes "processing by automatic means" under the Data Protection Directive. "Processing" is widely defined in the directive so as to cover any operation that can be performed on information, including collecting, recording, retrieving, consulting, disseminating and storing information. And the act of loading an Internet page onto a server and making it available to other Internet users must involve some automatic operations.

Contrary to the opinion of the Advocate General, the ECJ found that the Data Protection Directive does apply to non-economic activities. In this and another case (joined cases C-465/00, C-138/01 and C-139/01 Osterreichischer Rundfunk and Others [2003] ECR I-0000), Advocate General Tizzano had argued that the directive could only be used to fulfil the purposes of the EC Treaty – in other words, the establishment and functioning of the internal market, and that the directive could not be used to protect human rights generally, and could not apply to a non-economic activity, such as Lindqvist's parish magazine.

However, in both cases, the ECJ disagreed. The ECJ held that trying to distinguish between economic and non-economic activities, as the Advocate General suggested, would make "the field of application of the directive particularly unsure and uncertain".

The exception in Article 3(2) of the directive for purely personal or household processing also did not apply to this case. Although Lindqvist's website

was for religious and charitable purposes and not for profit, by publishing on the Internet, she had made her colleague's personal data accessible to an indefinite number of people. The ECJ held that such wide publication could not be said to be for purely personal or household reasons. Any publication of personal data by an individual on the Internet – even of, say, holiday snaps – may now need to comply with the Data Protection Directive.

It was for the Swedish District Court, not the ECJ, to balance Lindqvist's right to freedom of expression against her failure to comply with the directive. The information published by Lindqvist was, to a large extent, trivial and in the public domain. Moreover, she removed the offending pages upon becoming aware that some of her colleagues objected. So it seems bizarre that she became subject to criminal proceedings for such an 'innocent' and well-intentioned act.

The ECJ seems to have had some sympathy with Lindqvist, but held that it was for the Swedish government and courts to take into account her right to freedom of expression and to judge whether or not the penalty was disproportionate to the offence.

Transfers outside Europe

The ECJ found that the loading of personal data onto an Internet page by Lindqvist was not a transfer of that data to a third country, despite the fact that the page could be accessed from any country in the world. Article 25 of the Data Protection Directive states that personal data can be transferred to a country outside the EEA only if that country provides an adequate level of protection for the rights of data subjects. So far, the European Commission has approved only a small handful of countries, so individuals in countries without "adequate" data protection regimes would certainly have had access to Lindqvist's website and the material it contained.

Nevertheless, the ECJ held that there was no transfer. It reasoned that to find otherwise would make all personal data loaded on the Internet (and so potentially accessible in all countries with Internet access) subject to the restrictions of Article 25 in a manner that was not the objective of Chapter IV of the Data Protection Directive (as stated in recitals 56 to 60). It concluded that given the state of development of the Internet at the time the directive was drawn up, it cannot be presumed that the word "transfer", which is not actually defined in the directive, was intended to cover the loading by an individual of data onto an Internet page.

Multinational corporations face difficulties sharing personal data with affiliates in the United States and elsewhere, because of the rules about transfer of data outside the EEA and that in the EU, the United States is not regarded as providing adequate protection.

If a European company wishes to share personal data, about customers or staff, with its US parent or sister companies, its options are currently limited. Relying upon the consent of the data subject can be cumbersome and risky – particularly in relation to employees, and while US companies can sign up to the EU-US Safe Harbor, many have concerns regarding enforcement by the US Federal Trade Commission. Currently, the only other alternative is for the sender and recipient to enter into a contract, perhaps on the prescriptive terms of one of the European Commission's two Model Contracts.

The lack of practical options and the sheer volume and complexity of data transfers in a typical multinational means that even the best multinationals find themselves in a state of 'pretty good' rather than 'complete' compliance, despite implementing the various options above.

While the Lindqvist case does not suggest another option, it may provide comfort for such multinationals to know that the meaning of "transfer" may not be as broad as previously thought. The personal data on Lindqvist's website was not transferred direct to third countries by her but rather it was transferred "through the computer infrastructure of the hosting provider where the page is stored". And the reasoning of the ECJ would seem to apply in principle to the use of other systems using Internet or browser technology, say, the use of a worldwide intranet in a multinational and perhaps other technology too.

Could the act of an EU company entering personal data into its databases and allowing US users remote access be regarded as analogous to Lindqvist loading personal data onto her website?

However, before everyone gets carried away, it should be noted that the ECJ was careful to limit its ruling about transfers to the facts of this case and was only asked to consider Lindqvist's activities, and not those of her hosting company. Nevertheless, the Lindqvist case raises some intriguing questions regarding transfers to third countries and may offer some – if only a little – extra comfort to those multinationals with residual concerns regarding the 'completeness' of their data transfer solution.

The ECJ found that the loading of personal data onto an Internet page by Lindqvist was not a transfer of that data to a third country, despite the fact that the page could be accessed from any country in the world.

Authors: Clare Goodman (senior solicitor) and Mark Watts (partner) advise on data protection issues for London-based law firm Bristows. They can be contacted by telephone at: +44 (0)207 400 800, or by E-mail: clare.goodman@bristows.com and mark.watts@bristows.com. Website: www.bristows.com.

Lindqvist ruling: For a copy of the European Court of Justice ruling (Case number C101/01), see: http://curia.eu.int/en/actu/communiques/index.htm