**Berwin Leighton
Paisner's Business
and Technology
Services group is
one of the largest
dedicated commercial
contracts teams in
the City. They have
kindly agreed to
contribute to our
Legal and Regulatory
Update over the next
year. For further
information on any
of the topics covered
in the Legal Update,
please email Paul
Langford at Berwin
Leighton Paisner LLP
([paul.langford@
blplaw.com](mailto:paul.langford@blplaw.com), 020 7760
4911).**

Legal and Regulatory Update

Data protection: Call centre criminals

Katherine Williams

Journal of Direct, Data and Digital Marketing Practice (2007) **8**, 259–267.
doi:10.1057/palgrave.dddmp.4350056

The Information Commissioner recently launched an investigation following Channel 4's *Dispatches* programme, which showed that criminal networks are trading British consumers' bank details and other confidential information obtained from Indian telephone call centres.

Investigation

The Channel 4 programme focused on telephone call centres, but the findings have implications for all businesses engaged in transferring personal data outside the UK. The programme highlights that there are security failures in a number of commercial call centres in India, and that although many businesses have sophisticated security measures in place to protect customer information, customers' personal details are being made illegally available.

The law

Under the Data Protection Act (DPA), when UK businesses send personal data to companies outside the UK, they remain responsible for ensuring that adequate security is in place to protect that information. So if an employee of the Indian supplier of a UK bank decides to sell bank customers' details to a third party, the UK bank will be liable for this DPA breach and the customers who are affected have a right to claim compensation against the bank for the breach.

UK companies need to ensure that their overseas suppliers are adhering to UK data protection standards, particularly concerning data security and the reliability and integrity of staff who have access to personal data. Businesses that transfer data outside the UK will typically have entered into data processing agreements with the overseas service provider and they must ensure that they carry out regular audits of the service provider's operations to ensure that there is no risk of that information being illegally used or disclosed.

Commentary

The Information Commissioner's willingness to use his enforcement powers means that this may be a worrying time for some companies with outsourced operations outside the UK. David Smith, the deputy Information Commissioner said the following: 'Depending on the

Paul Langford
Berwin Leighton Paisner LLP
Adelaide House
London Bridge
London EC4R 9HA, UK
Tel: 020 7760 4911
E-mail: paul.langford@blplaw.com

outcome of our investigation we will consider whether we need to use our formal enforcement powers to prevent incidents like this happening again in the future. Ultimately this could include ordering a company to stop processing personal information outside the UK.'

Katherine Williams, Associate, Business & Technology Services
katherine.williams@blplaw.com

Internet advertising: Websites to be regulated by ASA?

Paul Langford

The ASA

The Advertising Standards Authority (ASA) regulates advertisements, sales promotion and direct marketing in the UK, but the content of websites falls outside its remit. Despite this, the ASA recently adjudicated on unclear information on a retailer's website. This decision provides some important lessons for marketers who design combined marketing campaigns.

The advertisement

The action stemmed from a television commercial for Dell Computers that included the following statement:

'Whatever you need a PC for, Dell has the one you want for less than you might expect. Right now get this Dell Inspiron notebook featuring an Intel Celeron processor for only £299.'

On-screen text gave a website address and a phone number. The ASA received a number of complaints from disgruntled customers who claimed that the laptop was not available on the website for £299, but was in fact offered for £349. Further, complainants said the laptop was offered for £299 on the website, but the price rose when they selected it.

The Broadcast Advertising Clearance Centre (BACC) — the specialist body responsible for the pre-transmission examination and clearance of television advertisements — said they had been assured by the advertising agency for Dell that the laptop was available for £299. Dell said the model was available through telephone sales only for a short time, after which it was still available from its website.

Dell's defence in respect of the claims focused on the pre-selected options that were offered with the laptop. Prominently displayed text informed customers that the price included an 'upgraded service package' and that they could reach the advertised price by downgrading certain elements of the package. Dell said it was 'accepted industry practice' to automatically upgrade service options.

The ASA assessment

The ASA considered that, because the advert featured both a phone number and a website address, viewers would expect the laptop to be available for purchase at the advertised price by both means when the advert was first broadcast.

However, because the product initially was not available on the website at the advertised price, the ASA considered that the advertisement was misleading and breached various provisions of CAP (Broadcast) TV Advertising Standards Code.

Looking specifically at the website text, it considered the following:

‘For your added protection the above price includes an upgraded service package. To reach the advertised price please select a downgraded service from the Support Services section below.’

This, it felt, was an adequate indication to users that the package they had selected had been upgraded and that they could deselect this upgrade to reach the advertised price. Therefore, there was no breach on this point.

The complainants were frustrated that they could not find the prices stated in press and TV advertisements when they tried to order goods on the advertiser’s website. The advertised prices could be obtained, but only when a pre-selected, upgraded support package option was de-selected. Although the website included the following text:

‘Price includes an upgraded support service. For an alternative, choose from Support Services options below and update price,’

ASA adjudication

the ASA ruled that the text was not explicit enough in telling customers, especially those less experienced at internet shopping, how to obtain the advertised prices. Accordingly, the ASA adjudicated that the advertisement must not be broadcast again in its current form.

Commentary

Although the ordinary content of advertisers’ websites is outside the ASA’s remit, the clarity of the information on a website could determine whether advertisements appearing on television, in the press or elsewhere are likely to mislead.

In the short term, there are lessons to be learned by those businesses that include an upgraded support package for products sold online. The ASA advises being explicit in telling customers how to select (or deselect) options to obtain goods at their advertised prices, and recommends the use of very clear instructions.

In the longer term, it is likely that further advertisements will fall within the remit of the ASA, as website and other methods of advertising combine to form part of the same campaigns. Where there

are concerns, text should be submitted to the CAP Copy Advice team and/or appropriate legal advice sought, prior to publication.

Paul Langford, Professional Support Lawyer, Business & Technology Services
paul.langford@blplaw.com

Ecommerce: RSS feeds — Negotiate contracts or click on the accept button?

Marcus Pearl

RSS is widely used

RSS ('Really Simple Syndication') is now widely used as a method of delivering news or other Web content to Web users. Increasingly, commercial deals are revolving around RSS, often without an appreciation of the legal issues raised.

Subscribing

Subscribing to an RSS feed can be as easy as a click of a button (or, more specifically, the dragging of a URL into your newsreader). The feed is then delivered to the customer, typically under the standard terms and conditions of the provider and often for no charge.

However, when involved in more sophisticated arrangements, where RSS feeds are provided on a bespoke basis for what is often a substantial fee, the standard terms and conditions, which, typically, highly favour the provider and provide the customer with little if no protection, should, if possible, be avoided in favour of a properly negotiated contract. So, what are the principal issues for the customer when negotiating a bespoke contract and can it ever get a good deal?

Identity of provider

Firstly, should a customer ever worry about the identity of the provider? Surely, if the content is not yours, why worry? Even if the provider is a recognised company of good standing, a customer will not want to incorporate content that impairs its reputation, through claims by third parties or otherwise. As such, it should try to negotiate a warranty that the content is not libellous, defamatory, obscene, pornographic or in breach of any applicable law. It would be even better to obtain an indemnity covering any claims made

against the customer as a result of such content not meeting the above criteria. It is unlikely that either forms of protection would be offered in standard Terms and Conditions for the provision of RSS feeds.

Without the above protection, the customer would be exposed to content over which it has no (or little) control. Indeed, even in a bespoke RSS contract, the provider will want sole editorial control over the content, usually asking for the right to terminate the contract if the customer interferes with the content in any way.

Licence for use

Trade Marks

So as to ensure that its content is properly accredited, the provider will grant the customer a licence to use the provider's Trade Marks on the customer's website for the purpose of its use of the content. The customer should obtain assurance from the provider that, at the time the licence is granted, the customer's use of such Trade Marks are not in breach of any third-party rights and that it will be indemnified in the event of any such third-party intellectual property infringement. This would protect the customer in the event that it is displaying an infringing Trade Mark on its website. This is clearly better for the customer than a standard clause entitling a provider to revoke its licence if it considers that there is a material risk that the customer's use of the provider's Trade Marks are infringing third-party rights.

Flexibility and control

Another question for the customer is the flexibility and control with which it can operate the webpage on which the RSS feed is displayed and incorporated. Commonly, a provider will want to restrict the customer's ability to advertise third-party companies and/or their products on the same webpage as the RSS feed. Faced with a blacklist of commercially undesirable third parties (in addition to the provider's direct competitors), the customer may assert a right to advertise generally, subject to such blacklist, by arguing that the RSS feed takes up only a certain percentage of space on the webpage.

Commentary

It often makes sense for a customer to avoid contracting on the standard terms and conditions of a provider (if they exist) and to negotiate a bespoke arrangement. While the resulting deal will often depend on the parties' bargaining positions, there are a number of important protections which a customer would need. However enticing though it may be simply to click 'We accept', it is well worth the effort to negotiate in order to obtain as much protection as possible.

Marcus Pearl, Senior Associate, Business & Technology Services
marcus.pearl@blplaw.com

Data protection: Cold calling ruling

Gary Brooks

Is 'direct marketing' limited to commercial communications? A recent high profile case illustrates that, for the purposes of UK data protection law, a broader view of the term will be taken. It provides some important reminders for all businesses.

The decision

The Information Tribunal upheld a decision of the Information Commissioner that unsolicited canvassing communications made by political parties to individuals do constitute 'direct marketing' for the purposes of UK data protection law. The Information Tribunal is the body that hears appeals from notices issued by the Commissioner under the Data Protection Act.

The provisions in the United Kingdom relating to unsolicited communications stem from the European Union's Directive on Privacy and Electronic Communications (2002/58/EC), which was implemented in the United Kingdom by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the 'Regulations').

What constitutes direct marketing?

The case turned in part on the interpretation of what constitutes a direct marketing communication. 'Direct marketing' is defined in Section 1 of the Data Protection Act as

'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.'

It was the regulator's interpretation of this statutory definition that was at issue in this case. The Information Commissioner has made it clear since 1999 (via its legal guidance) that the term 'direct marketing' applies not just to communications which constitute the

'offer for sale of goods or services, but also the promotion of an organisation's aims and ideals. This would include a charity or a political party making an appeal for funds or support.'

This approach was reaffirmed in guidance to the Regulations released by the Commissioner in 2004.

Use of automated calling systems

The particular provision that was relevant to the Information Tribunal's decision in this case was Regulation 19, which states that the use of

Definition of direct marketing

automated calling systems for direct marketing purposes is prohibited except where the recipient has

‘previously notified the caller that for the time being he consents to such communications being sent by, or at the instigation of, the caller on that line.’

This ‘opt-in’ requirement requires the recipient to take some positive action to consent to the automated marketing calls.

Use of live telephone calls

Another part of the Regulations that was discussed in the Information Tribunal’s decision was Regulation 21, which governs the use of live telephone calls for direct marketing purposes. While this case did not concern live telephone calls, the Information Tribunal stated the position in law that an organisation cannot make such calls to a subscriber (ie, the recipient of the call) who has previously notified the caller that they do not wish to receive such calls or an individual who is registered with the Telephone Preference Service (TPS). This opt-out approach for telephone marketing effectively mirrors the basic opt-out right enshrined in the Data Protection Act 1998.

Facts of the case

Facts

The case involves the Scottish National Party (SNP). Prior to the General Election in 2005, the SNP initially undertook a test trial referred to as the Automated Voice Polling (AVP) of potential supporters, who were called and played a message asking whether they agreed or disagreed with statements and to respond using a touch-tone phone. This allowed the SNP to gauge whether there were any actual supporters within the household. The SNP did not receive any complaints about this pilot run, and undertook further campaigns using automated calls.

Throughout April and March of 2005, the SNP launched a similar scheme using the voice of Sir Sean Connery, who read out a message to households, saying, ‘If Scotland matters to you, then make it matter in Westminster. Vote for the SNP and get Scotland’s voice heard in London. I thank you for listening’. The message then allowed the recipient to indicate whether they intended to vote for the SNP. During this period, the SNP had in fact received a letter from the Information Commissioner reminding it that political parties may not undertake automated marketing calls to individuals without first gaining their consent. A number of individuals made complaints about the calls saying that they had not given their consent. Furthermore, the SNP, despite trying to avoid doing so, had made some automated calls to voters registered with the TPS. As is apparent, the Information Commissioner had consistently made it clear to political parties that it regarded canvassing calls as ‘direct marketing’ and therefore within the remit of the Regulations.

Outcome

The Information Commissioner issued an enforcement notice against the SNP for breaching the Regulations and the SNP appealed the notice to the Information Tribunal.

The SNP argued that its activities did not amount to ‘direct marketing’ since they were not commercial communications and their view was that the Regulations do not apply to not-for-profit organisations and political parties. The Tribunal agreed with the Information Commissioner and found that the ‘Regulations do apply to political parties and their campaigning activities’ and that a phone call seeking support or funds amounts to ‘direct marketing’. According to the Tribunal, one primary reason for the prohibition contained in Regulation 19 is that recipients find automated calls intrusive into their private lives, and the ease with which such calls may be made facilitates (and encourages) wide-scale cold calling by automated means.

Therefore, the Regulations apply equally to the activities of political and not-for-profit organisations as they do to commercial organisations, and the SNP had contravened Regulation 19 by not obtaining the consent of the voters before making the automated calls. The Tribunal did note that the SNP had made an effort to avoid calling those voters registered with the TPS; however, this is not applicable in the case of automated calls, and this was cited by the Tribunal as evidence of the SNP believing that the Regulations did apply to it.

Decision of the Tribunal

The Tribunal remarked that if a political party’s activities did not constitute direct marketing then it would be able to make ‘automated calls without restraint’ — and similarly for other means of communication, it would not need to consider providing individuals with the ‘opt-out’ of such calls and it would not need to consult the Telephone Preference Service. Not-for-profit and charitable organisations would also benefit from this loophole. This was viewed as undesirable and inconsistent with the aims of data protection laws.

The SNP had also argued that the Information Commissioner’s decision interfered with their right to freedom of expression under the European Convention on Human Rights. The Information Tribunal found again in favour of the Information Commissioner’s decision, stating that there was very little interference with the right to freedom of expression. Only the method of communication was being limited, not the content of that communication, and the method was only limited to the extent that the individual must have given their consent to the automated calls.

Commentary

The Tribunal’s decision is a timely reminder that the Regulations do not just apply to commercial organisations but they apply equally to all not-for-profit organisations and political parties. Given that charities and political parties are by their very nature some of the most proactive marketers in the United Kingdom, this confirmation of the Information

Commissioner's approach to the regulation of their marketing activities is of particular significance to them.

Nevertheless, this case also serves as a reminder to all businesses that the UK data protection regulator is prepared to take a broad view of what constitutes 'direct marketing'. Any communication intended to promote the aims or ideals of an organisation will qualify as marketing in the eyes of the regulator and this has significant implications for how businesses structure their communications with individuals so as not to breach their privacy rights.

It is clear from practical experience that the reasonable expectations of the recipient of the communication are a factor to be considered when analysing whether a particular communication can be defended as a service-related communication (in which case there are no data protection restrictions) or whether it constitutes direct marketing (which will be subject to individuals' opt-out rights, and in the case of automated calls, to the prior consent requirement). Organisations would be well advised to put themselves in the shoes of the recipient of the communication and consider whether individuals would reasonably view the communication as part of the service or alternatively as a promotional communication that they are entitled to object to.

Marketing departments need to ensure that any marketing exercise complies with the Regulations. Any communications by means of automated calls will fall foul of the Regulations if there is some promotional element and the recipient has not previously communicated consent. The high number of complaints from individuals in the SNP case highlights the risk of using automated calling systems for marketing; people tend to find these particularly intrusive and an interference with their privacy. Automated calls generally lead to a higher level of complaints, which in turn generates bad publicity for organisations (irrespective of whether there has actually been a technical breach of data protection law).

The Regulations are best known for their application to the use of e-mail and SMS for marketing, but businesses must remember that the rules governing direct marketing differ depending on the means of communication used. For example, the opt-out approach that governs live telephone calls is a less onerous standard than the strict opt-in requirement that applies to marketing by means of automated calls, fax and e-mail/SMS. While a one-off breach of the rules on direct marketing is unlikely to result in an organisation receiving a stringent penalty from the Information Commissioner (frankly his priorities currently lie elsewhere), a more pressing concern is the negative publicity and brand damage that can arise when an organisation is portrayed in the media as not taking customers' privacy rights seriously.

Gary Brooks, Senior Associate, Business & Technology Services
gary.brooks@blplaw.com
© Berwin Leighton Paisner LLP

Need to ensure compliance with Regulations