Field Fisher Waterhouse LLP is a full service European law firm with offices in Brussels, Hamburg, Paris, London and Manchester and exclusive relationships with Spanish firm, Jiménez de Parga and Italian firm, La Scala. Its main areas of practice are corporate and commercial, IP and technology, banking and finance, regulatory and real estate, with particular expertise in employment & pensions, dispute resolution, tax and competition & EU law.

What is behavioural advertising?

The recent outlook

What is different about behavioural advertising?

Legal and Regulatory Update

On good behaviour: An overview of the rules and proposals around behavioural advertising

Victoria Hordern

Journal of Direct, Data and Digital Marketing Practice (2009) **11**, 147–150.
doi:10.1057/dddmp.2009.23

Behavioural advertising is designed to make online advertising more relevant to internet users. It is behavioural because it deliberately tracks a user's behaviour as they move from website to website, and, in doing so, it builds up a picture of that user's interests. As a result of collecting this information, the advertiser can place the user within an audience segment that then enables the advertiser to serve up relevant adverts. Of course, in reality it is more complicated than this, with a number of different parties from ad exchanges and ad agencies involved, but the end result is, for instance, that a car company that has paid for online advertising space will get its ads seen by those whose online behaviour indicates a predisposition for seeking information on cars. A win-win situation then surely?

However, recent news reports and commentary on behavioural advertising has indicated that it is far from straightforward. In fact the matter is considered sufficiently serious that the EU Commission in April this year took legal action against the UK for failing to protect internet users from a behavioural advertising technology called Phorm that had been tested by BT without BT's customers' knowledge. The EU alleged that the UK has failed to implement the EU rules around electronic privacy and data protection to ensure the confidentiality of communications by prohibiting interception and surveillance without user consent. The fallout of this action has been such that Phorm has now lost most of its partners, including, earlier in July, BT. The controversy around behavioural advertising has not been without other casualties. The US behavioural targeting solutions company Nebuad generated controversy for its use of deep packet inspection technology. Last year it was on the receiving end of a class action in San Francisco, and has since shut down.

Other types of online advertising are considered more benign. So, for instance, first-party advertising, whereby the website operator serves up adverts based on your use of that particular website (eg Amazon), and contextual advertising, where the adverts served up are based on the information on the webpage you are currently browsing, are less

privacy-intrusive and have not generally been the subject of regulatory scrutiny. Behavioural advertising attracts greater concern because it involves tracking a user's journey across specific websites (that participate in an advertising network), allowing a detailed profile of the user to be constructed. Tracking occurs through cookies and/or through (more rarely) deep packet inspection techniques. The cookie stores information about a user's web history and provides it to the ad exchange operator. Persistent cookies (as opposed to transient session cookies) remain stored on a user's browser until the user chooses to delete them or they expire.

Support for relevant advertising

Against this background, it is important to note that surveys show that users favour the receipt of adverts that are relevant to them and a reduction in unwanted adverts. Furthermore, users prefer an internet that includes advertising on the basis that this helps to maintain (and pay for) free access to online content. Despite the fact that privacy lobbyists are concerned by the perceived threat of behavioural advertising, those engaged in this form of advertising must still comply with the relevant rules.

EU rules

At the EU level, the collection and use of data through behavioural advertising is governed by the Data Protection Directive and the E-Privacy Directive. The Data Protection Directive is concerned with the use of personal data, while the E-Privacy Directive sets out rules for the use of cookies and the confidentiality of communications. Arguments that behavioural advertising technology does not collect personal, identifiable information usually come unstuck by the broader interpretation of personal data under European law. Even though a name is not collected, where a profile is built of a user and they are treated differently according to that profile, this may be personal data. Likewise, if IP addresses are used to distinguish between users, most regulators consider this piece of information to be personal data.

Where the Data Protection Directive applies, those parties in the behavioural advertising chain that control the use of personal data (eg publisher and ad exchange) must comply with the Directive's rules. Furthermore, the E-Privacy Directive prohibits the use of cookies unless clear, comprehensive information about the purposes of storage and access is given along with the opportunity to refuse the cookie. If a user opts out of behavioural advertising and in doing so places a cookie on their browser notifying that they have opted-out, there is a risk that a privacy-conscious user might delete that opt-out cookie when they clear out their cookies. So far only Google appears to have come up with a solution, by devising a browser plug-in that ensures that the opt-out cookie remains on the browser.

Which model?

Where the behavioural advertising chain is structured so that the advertiser or its service provider takes a feed of user data from the user's ISP, this will probably involve an interception of communications data whereby the contents of the communication are monitored by a third party while in the course of transmission. It is a criminal offence under the UK Regulation of Investigatory Powers

Act 2000 to intentionally intercept a communication in the course of transmission without lawful authority. Lawful authority can be obtained when the sender and recipient consent to the interception. But in the context of behavioural advertising, it will not be easy to achieve the consent of both parties. Therefore, behavioural advertising models should ideally move away from structures involving the interception of communications data.

An alternative model that moves away from the ISP approach employs application-based technology (eg a cookie) that obtains the user's data without intercepting the data during the course of a transmission. The cookie sits on the user's computer and is not connected to the user's ISP. However, it picks up browsing activity, which is provided to advertisers so that they can serve up relevant ads accordingly. Such activity would still need to comply with relevant rules on notice and consent, but this solution offers a means to avoid the more draconian rules around interceptions.

Will self-regulation help?

Without doubt, the current rules would benefit from greater clarity for those involved in behavioural advertising. Due to the heightened concerns but also the uncertainty of the rules, bodies both in the US and the UK have developed self-regulatory guidelines in a bid to give those in the advertising community a remit within which to operate. First out of the starting blocks was the Federal Trade Commission (FTC) in February of this year. The FTC had been examining online profiling for some years, and the guidelines set out four principles: (i) transparency and consumer control; (ii) reasonable security, and limited data retention, for consumer data; (iii) affirmative express consent for material changes to existing privacy promises; and (iv) affirmative express consent to using sensitive data, for example health data or children's data. While there is general acceptance with regard to implementing safeguards such as notification outside the privacy policy enabling consumer choice, there is resistance in the industry to the principle requiring the obtaining of consent to material retroactive changes. In the event that compliance with these principles is widely unworkable, it is possible that the FTC may ultimately refer the matter to Congress. Indeed, there are signs that the US Congress will consider a bill regulating behavioural advertising that is currently in the process of being drafted. Initial indications reveal that the bill will emphasise the need to provide full transparency to web users on what data is collected and for what purpose, user opt-in would be required for sharing user data with other advertising networks (although there may be some scope for opt-outs in this context), and the use of sensitive personal information would always be on an opt-in basis. Whether or not this meets the concerns of privacy activists whilst being workable from an internet advertising perspective remains to be seen. In July of this year, a collection of US advertising interest groups followed up with their own seven self-regulatory principles for online behavioural advertising, which seek to complement the FTC principles and emphasise education and accountability. Not long after the FTC published its guidelines, the UK's Internet Advertising Bureau

published a set of three good practice principles for online behavioural advertising with the blessing of the UK Information Commissioner. These principles highlight notice, user choice and education, but have been criticised as being less sophisticated than the FTC offering. How effective these self-regulatory attempts will be remains to be seen, although it seems possible that black letter law may emerge in some shape.

Proposals at EU level

In March of this year the Council of Europe produced a draft recommendation on profiling that seeks to introduce stricter control mechanisms for those engaged in profiling activity (broader than online behavioural advertising). Under the recommendation profiling is defined as a type of processing held to a stricter standard than other forms of processing so that the use of sensitive data in profiling is prohibited and profiling may only occur on the basis of consent, legitimate interests or if not prohibited by law. Of course, it is important to note that the Council of Europe's recommendation does not carry the full weight of EU law. At the EU level, although it does not appear that the EU is considering legislating specifically in this area, recent proposals to amend the rules on cookies are of serious concern. If the proposals are implemented, unless the use of cookies is strictly necessary for the provision of a service requested by the user, cookies can only be delivered to a computer if the user has consented beforehand. Consequently, for the application-based model, behavioural advertising would only be able to take place if the user has consented *in advance* to the placing of a cookie on his computer. This shift would, among other things, pose real obstacles to organisations seeking to use behavioural advertising. Greater clarity from the EU on the issue generally would be helpful. The recent Article 29 Working Party Opinion on online social networking recommends somewhat nebulously in passing that sensitive data should not be used in behavioural marketing models unless all requirements of the law are met.

Final words

In the current economic climate, businesses are keener than ever to ensure that advertising spend is used effectively. Behavioural advertising offers a sophisticated, tailored approach that they would do well to consider. The current regulatory and legal environments pose several challenges, but should not be a barrier to businesses seeking to target their goods and services to a receptive audience.

Victoria Hordern,
Senior Associate, Field Fisher Waterhouse LLP
victoria.hordern@ffw.com

The following articles were contributed by members of Osborne Clarke's Marketing Law team. The team is recognised as one of the UK's leading practices in this area of law and advises a wide range of marketing agencies and brand owners. Any queries arising from this article should be directed by email to Stephen Groom (stephen.groom@osborneclarke.com)

Consumer regulation responsibility split between OFT and FSA

Possible extension of FSA's role

Who should regulate consumer credit advertising and sales?

Zoe Hare

Journal of Direct, Data and Digital Marketing Practice (2009) **11**, 151–155.
doi:10.1057/ddmp.2009.25

Law stated as at: 22 June 2009

The Financial Services Consumer Panel (FSCP) has urged the Financial Services Authority (FSA) and Government to change the rules in relation to consumer credit regulation.

The FSCP has issued a paper in response to the Turner Review stating that the regulation of consumer credit should be passed from the Office of Fair Trading (OFT) to the FSA.

At present, there is a split in consumer regulation between the OFT and the FSA, although they do work together to ensure a consistent approach. In a joint statement published in May 2008, the FSA and OFT set out the division of responsibilities in relation to the Consumer Protection from Unfair Trading Regulations 2008.

The FSA's responsibilities were to consider the fairness of commercial practices with regard to financial services of FSA-authorised firms and appointed representatives undertaking regulated activities (under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001). The OFT stated that it was responsible for unfair commercial practices in financial services where the activities were governed by the Consumer Credit Act 1974 or where the issue did not relate to an FSA-authorised firm or appointed representative.

The FSCP's view is that since the majority of regulation in the financial services sector is carried out by the FSA, this role should be extended to encompass the regulation of consumer credit. Adam Philips, Acting Chairman of the FSCP, has said that the FSA 'should regulate all aspects of business of the firms it authorises, including provision of consumer credit, which is presently regulated by the OFT'.

The present split could cause confusion, the FSCP says, as it may be unclear to some which body regulates which areas. The key issues raised by the FSCP in its paper are:

1. the FSA must deliver on its promise to increase its supervision of how firms conduct their business;
2. the FSA must increase its scrutiny of firms' business models;
3. the FSA should become a more transparent regulator;
4. the FSA should regulate all aspects of business of the firms it authorises, including provision of consumer credit, at present regulated by the OFT; and
5. the FSA should take a tougher stance on enforcement.

**Changes intended
to drive responsible
lending**

Why this matters

The consolidation of all financial services regulation will certainly create a smoother approach that would be more understandable to financial services institutions and consumers.

The FSCP is also hoping that this will result in financial services institutions lending more responsibly, and that it would help to reduce excessive debt caused by such lending. The FSCP believes that a dramatic change of the kind suggested would be beneficial to consumers.

However, there are obvious flaws with this approach. Consumer credit activities are not only carried on by FSA authorised firms. The FSCP proposals only seem to relate to FSA-authorised firms. Therefore, it appears that non-FSA-authorised firms will remain under the present regime with the OFT. This may lead to inconsistent approaches between the OFT and the FSA. In particular, the FSA has notoriously stringent rules by which its authorised firms must abide.

It remains to be seen whether the views of the FSCP are taken into account and whether this area of regulation is radically changed.

Zoe Hare, Osborne Clarke, London
zoe.hare@osborneclarke.com

Data protection

Emily Jones

Law stated as at: 27 July 2009

What happened

The Information Commissioner's Office (ICO) published its Annual Report for 2008/09 on 6 July 2009. The report summarises the ICO's activities over the past year and the way it has informed and ignited debate on privacy issues, as well as providing detailed information on the cases and complaints that it has handled. Of particular interest is the focus on marketing activities as a source of complaints to the ICO.

Complaints about marketing communications

As part of the Annual Report, the ICO has published statistics on the top-10 reasons for complaining. According to the report, complaints about email, automated calls, live phone calls and SMS account for 27 per cent of the complaints it receives.

**Top reasons for
complaints identified**

**Direct marketing
responsible for high
level of complaints**

Direct marketing businesses still have some work to do

The ICO has also published a top-10 list of the business areas that are generating the most complaints, with direct marketing businesses being

the second largest cause for complaints, accounting for 14 per cent. This indicates that the marketing industry still has some work to do in terms of complying with the Data Protection Act and Privacy and Electronic Communications Regulations (the 'PEC Regs').

So what are organisations getting wrong?

There are no more details in the report on the exact nature of the complaints, but enforcement action by the ICO to date gives a flavour of the specific reasons why some organisations get into hot water about their marketing methods. For example, the Liberal Democrats were issued with an Enforcement Notice in September 2008 for making automated calls, which constituted direct marketing, to individuals who had previously not given their consent to receive calls. Weatherseal Holdings was also served with an Enforcement Notice after it failed to comply with undertakings it has given to comply with the PEC Regs. These related to unsolicited telephone calls made on behalf of the company to individuals who were registered with the Telephone Preference Service and had also made complaints to Weatherseal directly about continuing to receive such calls.

The Advertising Standards Authority has also been, and continues to be, active in this area via the obligations in the Committee of Advertising Practice Code (the CAP Code) relating to data protection compliance. Earlier this year, adverts run in the national press by Direct Home Shopping Brands Limited, trading as Kaleidoscope Limited, were held to have breached the CAP Code because they could not get opt-in consent using the wording in their advert.

An overview of electronic marketing rules

The rules for marketing by email, phone or SMS, and by fax are set out in the PEC Regs, and essentially (and very briefly) require the following:

Rules for communications to individuals

- For unsolicited marketing sent to individuals:
 - by fax, email or SMS: organisations must get opt-in consent unless it is marketing by email or SMS where what's known as 'soft opt-in' consent will be sufficient. This can be used where the email address or mobile number has been fairly and lawfully obtained in the context of a sale or negotiation for similar goods or services to those that are being marketed and the recipient is given the opportunity to opt-out free of charge each time they receive a communication.
 - by post and phone: permitted unless the individual opts-out

Rules for communications to corporate recipients

- For marketing sent to corporate recipients:
 - by all digital and non-digital methods: permitted unless the recipient has opted-out having been pre-notified about the possibility of receiving marketing materials from the organisation which sends them.

Rules for automated call systems

- For marketing using automated call systems prior consent must be obtained whether the calls are directed at individuals or corporate subscribers.

Before marketing to individuals or corporate recipients by fax or telephone, the Telephone Preference Service and Fax Preference Service should be screened to ensure that people on those lists do not receive marketing communications by these means. More detailed guidance for marketers is available on the ICO's website.

The new information commissioner and increased enforcement action?

The report is especially significant because it is the last report issued by Richard Thomas as Information Commissioner.

Christopher Graham has now taken, over having previously been the Director General of the Advertising Standards Agency (ASA). If the ASA's past activity levels in bringing enforcement actions for failure to obtain correct of marketing consents are anything to go by, we can expect Mr Graham to encourage his colleagues at the ICO to actively enforce against non-compliance with the PEC Regs. A new fee structure for data protection notification also comes into force on 1 October 2009, allowing the ICO to increase the fees payable by large organisations to £500. This is likely to boost the ICO's budget and fund additional enforcement action.

Why this matters

The Annual Report shows that marketing is a significant problem that is likely to lead to a special focus on this area in 2009/10. With the ICO's increased income plus a new commissioner at the helm, together with the public's higher awareness of their rights, it is more important than ever to make sure that your organisation complies with its privacy obligations.

Emily Jones, Senior Solicitor, Osborne Clarke, Bristol
emily.jones@osborneclarke.com

ICO likely to focus on marketing in coming year

Further changes proposed to UK consumer law

Nick Johnson

Law stated as at: 3 August 2009

What happened

The Department for Business, Innovation and Skills (BIS — formerly 'BERR') has issued a 102 page White Paper outlining its proposals for reshaping consumer protection legislation.

White paper on reshaping consumer protection legislation

The document ('A Better Deal for Consumers — Delivering Real Help Now and Change for the Future') focuses on four main themes:

- help for vulnerable consumers;
- consumer credit;
- better enforcement and information for consumers; and
- modernising consumer law.

Highlights

Key highlights for advertisers include the following proposals:

- a new approach to enforcement that encourages businesses to compensate consumers appropriately for consumer protection law breaches;
- the appointment in 2010 of a new 'Consumer Advocate' to champion the cause of groups of consumers who have suffered a loss at the hands of a business, and who would have rights to bring collective action on behalf of consumers — a form of 'class action';
- a new strategy and a new specialist team for internet enforcement on consumer issues;
- implementation of the Consumer Credit Directive, including new disclosure requirements;
- greater clarity as to how consumer laws apply to digital products;
- a review of the law on misrepresentation and duress; and
- implementation of the proposed EU Consumer Rights Directive.

Why this matters

While the changes set out in the document are still only at proposal stage, they may be a good indication of which way the wind is blowing.

In particular, the proposal for a Consumer Advocate is one to keep tabs on. This development could significantly increase the risk associated with advertising claims that are not fully substantiated. Under the current regime, the prospect of individual consumers seeking to sue on an individual basis for misrepresentation can often be regarded as a low or even negligible risk; the new proposals raise the prospect of a potential form of class action litigation. Accordingly in scenarios where to date the key risk may have been an upheld ASA adjudication, all of a sudden there could be a major financial risk too. This will make the need for proper legal clearance of advertising claims more acute than ever before.

Nick Johnson, Partner, Osborne Clarke, London
nick.johnson@osborneclarke.com

**Proposed legislation
raises prospect of
class actions**