As for the terms of that licence, the agreement between LSHA and Susan did not limit LSHA's ability to exploit the deliverables, and gave Susan no right to control or veto their use.

Therefore, the implied licence effectively conferred on LSHA the full benefit of Susan's copyright in the Original Works and was not limited in such a way as to prevent LSHA exploiting the Original Works in the form of the Pack and Manual.

Why this matters

This judgment underlines the need to take extreme care with the drafting of intellectual property provisions in all agreements involving the supply of copyright works, such as agreements for the provision of creative advertising services.

In this case, LSHA's submissions on the implication of a licence were successful; however, it cannot be best practice to leave such key aspects to the vagaries of judicial interpretation, and the parties here could have saved themselves considerable cost and time if the IP rights disposition and usage provisions had been crafted with more care.

Stephen Groom, Head of Marketing and Privacy Law, Osborne Clarke
E-mail: stephen.groom@osborneclarke.com

New ASA 'do-not-track' regime

Stephen Groom

Journal of Direct, Data and Digital Marketing Practice (2013) **14**, 263–268.
doi:10.1057/dddmp.2013.9

Topic: Online advertising

Who: Advertising Standards Authority

When: November 2012 — new rules in force from 4 February 2013

Where: The United Kingdom

Law stated as at: 8 December 2012

What happened?

The United Kingdom's national advertising watchdog has announced a new third party cookie control regime featuring compulsory links to a 'do-not-track' mechanism, an obligation to cooperate imposed on advertisers benefiting from third party behavioural targeting and 'explicit consent' for the most intrusive forms of behavioural tracking. In launching this scheme, the Advertising Standards Authority (ASA) has gone further than the current legal regime and created more regulatory hurdles for the online advertising ecosystem.

Background

The ASA's groundbreaking 'Transparency and choice rules for Online Behavioural Advertising' (OBA Rules) apply to third-party cookies and come into effect on 4 February 2013. Third-party cookies come into play if a user visits a website, and a separate company from the one operating the site sets a cookie on that user's computer.

The OBA Rules apply to third-party cookies used for OBA, where the cookie collects data about the web behaviour of those using the device, across multiple websites visited, and uses this data to deliver advertising based on preferences inferred from the data collected. A new Appendix containing the OBA Rules has been added to the CAP Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing¹.

Legal compliance

The ASA makes it clear that the New Rules are not designed to deliver compliance with privacy and data protection law, and therefore this new regime will operate separately and in parallel with relevant legal control systems. The legal control system for cookies is based in the United Kingdom on amendments made by Directive 2009/136/EC (the ePrivacy Directive) to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

Regulation 6 of PECR requires that ‘a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user’ unless that user or subscriber is provided with ‘clear and comprehensive information about the purposes of that storage or access’ and has ‘given his or her consent’.

Note the absence here of requiring the consent to be either before the access or storage takes place or ‘explicit’.

Prior ‘explicit consent’ needed

Both will now be expressly required by the OBA Rules at Rule 31.2 for the use of:

technology to collect and use information about all or substantially all websites that are visited by web users on a particular computer in order to deliver OBA to that computer.

In its explanatory Help Note, the Committee of Advertising Practice (CAP), sister body to the ASA, which writes the CAP Code, explains that this does not apply to the everyday dropping of third-party cookies triggered by a visit to a website linked to a third-party online advertising network, but to the more intrusive form of behavioural tracking, using so-called ‘deep packet inspection.’

This type of tracking operates at Internet Service Provider (ISP) level and therefore covers all web browsing activities by users of a computer. The practice gained notoriety in 2006 when launched by an organization called Phorm in conjunction with British Telecom (BT). Concerns were raised by regulators and the practice has now to all intents and purposes discontinued in the United Kingdom.

Therefore, it is believed that this new rule will have limited impact. However, there have to be residual concerns that, with the increased sophistication of tracking technology, the wording of Rule 31.2 may be or become wide enough to catch third-party cookies that may not use deep packet inspection but have equivalent or semi-equivalent tracking capability.

ICO-implied consent

Returning to the legal requirements, guidance by the Information Commissioner’s Office (ICO) on the use of cookies and similar technologies indicates that in many cases of cookie use ‘implied consent’ should suffice. The ICO also said that obtaining consent after

the cookie was dropped may be acceptable, provided it was not possible to do this beforehand and that websites did ‘as much as possible’ to reduce the delay between receiving information about the cookies and being given the opportunity to stop the cookie’s operation.

On this basis, the online advertising community warmly welcomed ‘implied consent’. But does this approach suffice for more intrusive tracking technology such as third-party cookies? The ICO Guidance stopped short of providing a clear answer, and all appearances suggest that UK OBA stakeholders have gone with ‘implied consent’ and hoped for the best.

A few days before the ASA announced the OBA Rules, the ICO reported on enforcement of the new cookie laws since May 2012. Between May and September 2012, 388 complaints were received on about 207 websites, with the ICO so far having gone no further than writing to 68 organizations in May 2012 and 86 organizations in October 2012. As the ICO says, based on this, ‘consumer awareness and concerns about cookies appear relatively low’.

Therefore, against this backdrop of enlightened interpretation of the law allowing implied consent in some cases, limited apparent consumer concern about the use of cookies and a hardly frenetic approach to enforcement so far, some might ask why another UK regulator has seen fit to wade in with another cookie control regime.

Like it or not, compliance with these new OBA Rules is compulsory for all those affected, and, with no grace period and full enforcement starting in just a few weeks’ time, all those involved need to quickly get to grips with the new regime.

The OBA Rules lay down six new requirements:

1. Third Parties engaging in OBA must provide ‘clear and comprehensive notice’ on their own websites about their OBA activity;
2. Third Parties must provide the same notice in or around online display ads delivered to all other sites using OBA;
3. Third Parties must provide, both on their own websites and in or around OBA ads, a link to a ‘relevant mechanism’ that allows the user to exercise a ‘do-not-track’ option;
4. Advertisers on whose behalf OBA ads are delivered must co-operate with the ASA to help identify the Third Party if the ASA is unable to do so;
5. Third Parties must not create interest segments specifically designed for the purposes of targeting OBA to children aged 12 or under;
6. Explicit consent is needed before using technology to track and use for OBA information on all or substantially all websites visited by web users on a particular computer.

These rules will not apply to:

- contextual advertising;
- web analytics;

The new regime

Six new rules

- ad reporting or ad delivery;
- the collection and use of information for OBA by site operators on their own websites; or
- the use of OBA in rich media, in-stream videos online or on mobile devices.

This very last exclusion is significant with the unstoppable rise of mobile. So much is recognized by CAP, which in its Help Note on the OBA Rules promises an extension of the rules to mobile ‘in due course’.

OBA Rules 1 and 2

OBA Rule 31 deals with the giving of disclosures about OBA use of web browsing behaviour by way of Notices. Third Parties must give two types of ‘clear and comprehensive notice’ that they are collecting and using web viewing data for OBA. The first type of notice (Third Party Website Notice) must appear on the third party’s own website and the second type of notice (Ad Notice) must appear in or around any OBA ads.

Only the Third Party Website Notice has to explain how a user can opt out of use of their online behaviour for OBA purposes. This is a legal requirement under the ePrivacy Directive, but it is odd that this is not mentioned in the context of Ad Notices. Both Notices must include a link to a ‘relevant mechanism’ for opting out of the collection and use of web viewing data for OBA.

There are different rules for the two Notices. The CAP Help Note tells us that for the Third Party Website Notice it is very unlikely to be sufficient ‘for this to appear either in the small print of the website, for instance in a privacy or cookie policy, or several clicks away from the home page’. A prominent pop-up or disclosure panel at the top of the web page should work, provided this can effectively coexist with any notices displayed to comply with the third party’s separate, legal obligation under PECR. The Ad Notice, on the other hand, should be an icon, symbol, text or similar that is easily discernible to the normal web user.

OBA Rule 3

Strangely, ‘relevant mechanism’ is not defined. CAP has clarified since publishing its Help Note that the mechanism in question can be either one of the Third Party’s own creation or the mechanism referred to in the ‘Background’ section of the OBA Rules and CAP Help Note.

This mechanism is already in operation and available at <http://www.youronlinechoices.eu>. CAP tells us that ‘the vast majority of UK-operating Third Parties’ are signed up to it, and thus there is heavy pressure for remaining Third Parties to take this option. The mechanism is enshrined in the European Advertising Standards Alliance Best Practice Recommendations for OBA² and an EU Industry Framework.³ It is now administered by the European Interactive Digital Advertising Alliance (EDAA).

The EDAA mechanism is a pan-European self-regulatory OBA notice and choice regime. It was initially devised at the instigation of the Internet Advertising Bureau (IAB) before the ePrivacy Directive’s introduction of the need for consent for cookies. A similar

system is already in operation in the United States, although it is unclear what level of take-up has been achieved. At its core is an ‘advertising option icon’ (Icon).⁴ This performs the purpose of providing disclosure and enabling the user to opt out of use of their web viewing data for OBA.

However, there are catches with the EDAA mechanism:

1. In order to use the Icon, the Third Party must sign up to the IAB Europe OBA Framework;
2. All those signing up to this Framework must become compliant with the principles it lays down and self-certify such compliance within 6 months after signing up;
3. When arranging for deployment of the Icon, the Third Party must follow the detailed ‘Technical Specifications for implementing the IAB Europe OBA Framework and EASA BPR in Europe’⁵;
4. To be able to use the Icon, a licence has to be obtained. There are two licence fee levels:
 - The regular fee of €5,000 a year; and
 - For small- or medium-sized enterprises, a reduced annual fee of €3,000.

The lower fee will only be payable if evidence can be provided that the enterprise derives annual revenue from online display advertising of below €3m.

It also appears that signing up for an Icon licence between now and the end of the year is not attractive, as the full annual fee will be charged for 2012.
5. Signatory Third Parties will be monitored by an independent certified provider to ensure that they adhere to the EU Industry Framework Principles. They will not receive a ‘trading seal’ unless they comply⁶.

OBA Rule 4

Under OBA Rule 1.8.1, advertisers benefiting from OBA must co-operate if they are approached by the ASA for information about the identity of the responsible Third Party. The ASA cannot impose financial penalties, but could steps be taken through the CAP to stop the appearance of the relevant OBA ads? The CAP Help Note says that an advertiser who is asked to co-operate may need to obtain details about which network carried the campaign or which third party served the ad. Beyond this, it sheds little light and no doubt online advertisers will be taking advice. They will be well advised to audit their OBA activity and all relevant Third Parties.

OBA Rule 5

‘Interest segments’ are preferences inferred from the data collected by a cookie about a user’s web viewing behaviour. The CAP Help Note points out that the prohibition at Rule 31.1.3 will target the construction of segments based on data collected from websites aimed at those under 13 years of age. In any investigation, the Third Party will be asked to explain how a segment was created and why it did not particularly target those under 13 years of age.

Penalties

The Sanctions section of the ASA's Regulatory Statement says:

- Hopefully, in most cases, co-operation will lead to immediate remedial action;
- Otherwise a formal investigation may be needed, leading to the adjudication being published on the ASA website;
- If the Third Party continues to breach the rules, measures would include bringing this continued non-compliance to the attention of the Third Party's potential clients and partners; and
- There are additional sanctions if the Third Party is a signatory to the EDAA mechanism:
 - removal of the trading seal of approval; and
 - removal of the licence to use the Icon.

Territorial reach

If complaints are made that the OBA Rules have been broken, the CAP Help Note tells us that 'country of origin' applies. The idea of this is that 'each Third Party will be subject to regulation by only one advertising self-regulatory body'. The CAP Help Note refers to the majority of UK-operating Third Parties being signed up to the EDAA mechanism.

This indicates that the jurisdictional test will be whether the Third Party is 'operating in the United Kingdom'. But does this mean there has to be a physical presence in the United Kingdom? If the Third Party is located in the United States, for example, how will the ASA compel compliance? In recent comments, CAP has indicated that, in such a case, the ASA is likely to refer the matter to a relevant self-regulatory authority in the United States that already has well-established OBA rules. This could be the Network Advertising Initiative or the Better Business Bureau.

Conclusion

CAP hails this initiative as a 'significant step to ensure that targeted marketing techniques can flourish'. It is certainly not insignificant in terms of the additional regulatory burden it creates. In terms of policing privacy in the digital advertising arena, it has historically been the ASA, not the ICO, which has the strong track record. It has a far higher profile as the 'go to' watchdog in the sector and has shown unflinching commitment to act when complaints are received. Third Parties and advertisers benefiting from OBA will be best advised to take this development seriously and take steps to ensure compliance before 4 February 2013.

Stephen Groom, Head of Marketing and Privacy Law, Osborne Clarke
E-mail: stephen.groom@osborneclarke.com

Notes

- 1 <http://www.asa.org.uk/News-resources/Media-Centre/2012/~media/Files/CAP/Misc/New%20Online%20Behavioural%20Advertising%20rules.ashx>
- 2 <http://www.easa-alliance.org/page.aspx/386>
- 3 http://www.youronlinechoices.com/uk/wp-content/uploads/2012/08/2012-06-08_iab_europe_obo_framework.pdf
- 4 <http://edaa.eu/certification-process/apply-for-licence/>
- 5 http://www.iabeurope.eu/media/86423/technical_specifications_for_iab_eu_obo_fw_v1.pdf
- 6 <http://www.iabeurope.eu/public-affairs/obo-framework/criteria-for-self-certification-of-compliance-with-the-obo-framework.aspx>