Why this matters**Regulatory attention**

Big data is clearly on the radar for regulators and the fact that the ICO has issued a 50-page report indicates its importance. The paper, however, is on the whole balanced and recognizes that big data is not always bad (as the media sometimes suggests) and that privacy and big data can be compatible by going back to basic privacy principles.

Existing practices apply

Many of the points and issues raised in the paper are not new, but reinforce the fact that the existing privacy rules continue to apply. One area that may be challenging to apply in practice will be getting consent where required and coming up with innovative means for notification.

Announcing the publication of the report, Steve Wood, the ICO's head of policy delivery, said, 'What we're saying in this report is that many of the challenges of compliance can be overcome by being open about what you're doing. Organizations need to think of innovative ways to tell customers what they want to do and what they're hoping to achieve. Big data can work within the established data protection principles ... established in UK and EU law [which] are flexible enough to cover big data. Applying those principles involves asking all the questions that anyone undertaking big data ought to be asking. Big data is not a game that is played by different rules'.

Sue Gold, consultant, Osborne Clarke, London

CAP top tips for affiliate marketers (and PhonepayPlus pipes up, too)

Anna Williams

Journal of Direct, Data and Digital Marketing Practice (2014) **16**, 137–140.
doi:10.1057/dddmp.2014.70

Who: Committee of Advertising Practice (CAP)

Where: United Kingdom

When: 10 July 2014

Law stated as at: 5 August 2014

What happened**Performance-based commission**

'Affiliate marketing' is a method of performance-based marketing where a third party (the 'affiliate') is rewarded by a brand for new customers attracted to the brand as a result of the affiliate's marketing efforts. Affiliates will often be rewarded on the basis of a commission for the sales that result from their efforts.

Previous ASA adjudications

The ASA has recently upheld a number of complaints where such affiliate marketing campaigns are concerned. For instance, in 2013 the ASA upheld complaints against LifeStyle Advantage Ltd (t/a Essence of Argan) as a marketing communication for a free trial did not make it clear that the consumer would be automatically charged for the product the following month and certain efficacy product claims had not been substantiated.

Using affiliates no defence

The manufacturer of the product in question responded to the ASA stating that the ad had been created by an affiliate and that they could not provide contact details for their affiliates. Nonetheless, the ASA held the manufacturer responsible for the content of the ads, and the fact the ads were designed by an affiliate was not considered a sufficient defence to relieve the brand of its responsibilities to ensure that claims in its advertising were robustly substantiated.

Online free storage

The ASA has also previously investigated complaints about an online data storage business whose ads were making misleading claims regarding unlimited free storage. The business protested that an affiliate marketer had been responsible for the content of the ad in question, but as the ASA considered that the business benefited every time a consumer clicked through and created an account, and that the affiliate was in effect an employee of the business, both the business and the affiliate marketer were held responsible under the CAP Code.

Common view with ASA

CAP's top tips

CAP claimed that both CAP and the ASA commonly saw the same types of issues arising with affiliate marketing and therefore in July 2014 they published their top three tips for compliance of marketing communications associated with affiliate marketing. Their list reads as follows:

1. *Make it clear that content is in fact an ad* — CAP acknowledged that this may sound obvious, but that many brands and their affiliate marketers have been on the receiving end of complaints upheld by the ASA because they cross the line between independent editorial content about a product and advertising copy making efficacy claims. The CAP Code requires that 'marketing communications must be obviously identifiable as such' and therefore CAP advises that, if there is any doubt as to whether people will consider an affiliate marketing communication to be editorial or marketing, it should be headed 'Advertisement feature' or similar to make the commercial intent of the communication clear.
2. *Brands should ensure that they have editorial control over their affiliates' content* — CAP highlighted that brands often mistakenly believe that, because their affiliate has written advertising content relating to their product and are promoting it themselves, the brand is not responsible for that content or sales promotion. CAP has reinforced that the ASA takes a different view on this matter. As the brand incites the affiliate marketer to promote its products or services and the brand benefits from each sale made by the affiliate (and then also enables the

affiliate to benefit by paying them in some way on the basis of sales), both the brand and the affiliate marketer are held responsible for the advertising that is circulated. In light of this, CAP has flagged that it is therefore wise for brands to set certain rules regarding the content generated for their products by their affiliate marketers.

3. *Ensure that significant conditions applicable to a promotion are communicated* — The CAP Code requires that all significant terms and conditions likely to affect a consumer's understanding of a promotion be communicated to them clearly and in advance. Exceptions to this rule can exist for ads appearing in media where space or time is limited (for instance, banner ads). In these cases, the significant terms and conditions for a promotion can be communicated on a landing page a maximum of one click away from the initial promotional copy. CAP has suggested that the ASA would likely apply the same rule to affiliate ads that were significantly limited by space, but the brand whose products or services are being promoted should ensure that the link to the product or service that the affiliate is providing links directly to the terms and conditions of the promotion in order to avoid the promotion being problematic. If an affiliate marketer is using content in a medium where space is not at a premium to promote a sales promotion, then significant terms and conditions will need to be included on the same page as the promotional content and the brand should ensure that this is the case.

Premium rate services complaints

PhonepayPlus communication

CAP is not the only body in the advertising space that has been considering the impact of affiliate marketing of late. On 30 July 2014, Phonepay Plus issued an update on the status of its own discussion paper on affiliate marketing following industry comment it had received. The original discussion paper was published back in March 2014. The update details the role PhonepayPlus has been playing in the interim period with industry to address its concerns regarding affiliate marketing where premium rate services are in some way concerned. So far, in 2014 alone, PhonepayPlus has received more than 600 complaints from consumers relating to premium rate services marketed using some form of co-registration.

Sharing and disclosure

PhonepayPlus supports initiatives for the prompt sharing of disclosable information between itself and industry, and sharing among the industry itself, to help identify emerging areas of risk relating to digital affiliate marketing that can be dealt with in an appropriate fashion.

Advertisers remain responsible

Why this matters

CAP's latest guidance is a reminder to advertisers who allow their affiliate marketers free rein over the content of their ads that they remain responsible for ensuring that all such advertising for their benefit is compliant with the CAP Code. The ultimate advertiser will be responsible for ensuring that the content of all such ads is compliant and also that the ads are correctly targeted (as a brand learnt the hard way when a gambling ad was mistakenly sent by an affiliate marketer to a child — the ASA

Contractual approval

upheld the complaint and also named the brand in its adjudication (Club Website Ltd, 8 January 2014)).

It is therefore prudent (and will help advertisers to limit their legal and regulatory compliance risks) for advertisers to enter into contracts with their affiliate marketers that cover this area of compliance. A brand would be wise to have approval rights over all ads created for its benefit or to at least have clear guidelines that all affiliate marketers are compelled to follow.

Anna Williams, associate director, Osborne Clarke, London

Bavarian DPA takes tough line on email encryption

Hendrik Schöttle

Journal of Direct, Data and Digital Marketing Practice (2014) **16**, 140–142.
doi:10.1057/ddmp.2014.71

What happened

In September 2014, 750 Bavaria-based companies found a notice letter from the Bavarian Data Protection Authority (DPA) in their mailboxes. After having scanned about 3,500 email servers (mx records) of about 2,200 companies with an automated scanning tool, the authority found that 750 email servers did not comply with current security standards. The authority requested the companies to update their servers accordingly. Now the companies have to react in order to avoid further steps — administrative fines are not excluded.

Automated breach discovery

The Bavarian DPA (Bayerisches Landesamt für Datenschutzaufsicht) had already used automated scanning tools in the past in order to discover data protection law breaches and prosecute the implicated companies. In this case, the DPA took a detailed look at data security and approached companies that had at least one of the following security issues:

- The email server did not offer encrypted connections (STARTTLS for the establishment of an encrypted connection and respective encryption for the following data exchange). *Note:* The DPA does not require end-to-end encryption, which is usually achieved by encrypting the emails themselves, for example by using PGP, GnuPG or a comparable encryption tool. The encryption that the DPA requests only affects the connection between email clients and servers. However, with public wireless hotspots becoming more and more widespread, it has become a common exercise by hackers and script kiddies to read unencrypted email traffic sent over publicly accessible, unencrypted wi-fi