Pulling back the curtain on targeted social media advertising

Alison Deighton, Partner at TLT LLP, considers how organisations using social media platforms for targeted advertising can continue without flouting data protection rules

Facebook is back in the news — and it is taking your data. Just after the sale of WhatsApp to Facebook was announced, WhatsApp's Chief Executive Officer, Jan Koum, stated that nothing would change with its privacy practices. Two years later, WhatsApp users have been greeted, rather unceremoniously, with an updated privacy policy. In short, Facebook will now start using data from WhatsApp users to better target Facebook and Instagram advertisements and to allow businesses to message users directly.

Although the move may not come as a huge surprise (at least to the more cynical amongst us), an interesting development is that WhatsApp users have been given 30 days to expressly opt-out of sharing data with Facebook for 'ads and products experiences'.

So what does this mean — and why do other organisations not offer this choice?

Targeted advertising mechanics

Social media platforms offer invaluable advertising tools for businesses. But how does the targeting of ads actually work?

There are currently two main offerings: one which enables businesses to send targeted advertising directly to their own customers; and another which establishes a set of 'lookalike' individuals who meet certain profile criteria.

Where organisations are targeting ads towards their own customers, the business shares an identifier, usually an email address or mobile number, in a 'hashed' form with the social media platform. The platform then matches this data with the information that it holds on its users. Where there is a match, this allows the organisation to send advertising messages directly to their own customers via their social media pages. These 'messages' include direct messages to an individual's social media inbox or page and display advertisements or banners.

For lookalike advertising, a number of different options are available. Platforms can identify key characteristics from a batch of known individuals and then identify others that display the same characteristics to create a 'lookalike' audience. Alternatively lookalike advertising can be targeted at individuals who have 'liked' a particular page or visited the business' website. Businesses can also measure how effective different types of advertising are by tracking the extent of interaction and successful conversions.

How does the law apply to this type of targeted advertising?

The two key pieces of legislation in the UK are the Data Protection Act 1998 ('DPA') and the Privacy and Electronic Communication Regulations 2003 ('PECR'). At the time when these pieces of legislation were drafted, social media platforms did not exist in their current form, never mind targeted advertising via these platforms. It is therefore necessary to interpret the requirements of the legislation in the context of ever more sophisticated technological possibilities, which leads to uncertainty for businesses and regulators alike.

DPA implications

The application of the requirements of the DPA are relatively straightforward. Where personal data are used to send targeted advertising via social media platforms, the following principles will apply:

- individuals must be informed about how their personal data will be used;
- a schedule 2 condition needs to be met, meaning that businesses need to be able to show either that they have consent to use personal data for targeted advertising purposes or that they have a legitimate interest in sending targeted advertising and such interests are not outweighed by the privacy expectations of the individual; and
- if an individual has opted out of marketing, this opt-out must be respected and this will extend to using personal data to send targeted advertising.

(Continued on page 10)

(Continued from page 9)

With many businesses now using social media advertising tools, it would be interesting to know how many of their customers understand how their information is used and analysed in order to serve advertisements via their social media accounts.

With increased transparency requirements on the way under the General Data Protection Regulation, (or the UK equivalent post-Brexit) the need for clear and easily accessible privacy notices is key. There is an opportunity for businesses to gain major advantages in consumer trust. They must strike the right balance between transparency and reassurance that data will be used in a beneficial way for the customer.

PECR requirements

The PECR present a more complex legal landscape.

Regulation 22 requires organisations to obtain consent before sending unsolicited direct marketing by 'electronic mail'. Social media adverts are certainly unsolicited and will fall within the wide definition of direct marketing set out in section 11 of the DPA: 'the communication (by whatever means) of any advertising or marketing materials which is directed to particular individuals.'

Prior consent will therefore be required if targeted advertising via social media platforms can be said to constitute 'electronic mail'. So what exactly is 'electronic mail'? PECR defines it as:

- any text, voice, sound or image message;
- sent over a public electronic communications network
- which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient; and
- includes messages sent using a short message service'.

"There is a need to be transparent about data sharing and the use of data for targeted advertising. It should be obvious to consumers what data are collected, the reasons for their collection and how they are used. This information needs to be provided at the point of data collection."

If we look at each of these limbs in turn in the context of targeted social media advertising, it is clear that some of the elements of the definition are clearly met. For others, the position is much less certain.

Social media advertising will certainly constitute text/images and voice/sound.

The courts have also given a broad interpretation to the question of whether social media platforms constitute a public electronic communications network. In the case of *Chambers v DPP* [2012] EWHC 2157, the court adopted a wide interpretation of the definition, commenting that "as Twitter is accessible to all who have access to the internet, it is a message sent via a public electronic communications network". It appears likely then, that all social media platforms would be considered to be a public electronic communications network.

Then comes the question of whether the advert is stored in the network or the recipient's terminal equipment until it is 'collected' by the recipient. Whether or not this is the case will depend on the social media platform being used to serve the advertising, and the way in which the advertising content is delivered. It is often difficult for businesses to determine where data are stored without having any technical knowledge of how the platform operates. However, messages directed to a social media 'inbox' would certainly appear to meet this requirement. It is possible that other advertisements that appear on a particular web page could also be caught if they are stored on the network until the individual logs in and sees a particular screen.

The final element of the electronic mail definition is whether or not the advertising constitutes a 'message'. If the advertising was by way of a direct message to an individual's social media inbox or page, again, a common sense approach would extrapolate the meaning of electronic mail to cover this sort of advertising.

In its guidance on direct marketing, the Information Commissioner's Office ('ICO') states that electronic mail includes, 'electronically stored messages, including email, text, picture, video, voicemail, answerphone and some social networking messages'. Whether an advertisement that appears on a particular web page would constitute a 'message' is less certain. When the PECR was drafted, it was aimed at one-to-one communications that demanded a response. Social media advertising does not neatly fall into this type of communication. But given the willingness of the courts to interpret the legislation widely to protect consumer rights, there is a risk that such advertising would be considered a message for these purposes.

What does the ICO say?

To date, the ICO has not provided any specific guidance on targeted advertising. As noted above, in its direct marketing guidance, the ICO stated that 'some social networking messages' are considered as electronic mail.

The ICO has indicated that PECR applies to direct messaging via social media i.e. a message directly to a person's inbox or their page. However, the ICO also acknowledges that PECR does not specify rules on other types of online marketing such

as display and banner advertisements.

Evidently, there is a struggle by both businesses and the ICO to interpret the extent to which PECR applies to different forms of targeted advertising. The public uproar to WhatsApp's updated privacy policy has prompted the ICO to produce a statement. Elizabeth Denham confirmed that her Office is 'looking into' the changes that WhatsApp and Facebook are making in relation to how they handle customers' personal data. Hopefully this will result in more definitive guidance emerging from this exercise.

So what does this mean in practice?

Whatsapp has utilised an opt-out mechanism to give its users a choice over whether or not it shares their data with Facebook to improve 'ads and product experiences'. However, the reason for asking for this consent is not necessarily because WhatsApp considers that prior consent is required under PECR for targeted advertising via Facebook. The more likely explanation is that WhatsApp now wishes to use data in a manner that it had explicitly stated it would not. Such a change of use requires users' consent.

For organisations already using social media platforms for targeted advertising, or for those considering taking the plunge, the following principles should be kept in mind:

- there is a need to be transparent about data sharing and the use of data for targeted advertising. It should be obvious to consumers what data are collected, the reasons for their collection and how they are used. This information needs to be provided at the point of data collection. If not, organisations may well need to ask for individuals' consent before sharing data for targeted advertising purposes;
- remember that personal data are not permitted to be used to send targeted advertising to any individuals who have opted out of their data being used for marketing purposes;
- if advertising messages are sent to social media inboxes, then they are likely to constitute a 'message' and consequently satisfy the 'electronic mail' limb of PECR. Therefore, organisations should obtain individuals' prior consent, in a similar manner as for marketing via other means such as email or SMS marketing. Data controllers should consider updating consent wording to refer to wider electronic communications; and
- if display advertisements or banners are being served on a web page then there is an argument that such advertising does not constitute a 'message' or, potentially, that it is not stored in the terminal equipment. But until the ICO provides definitive advice, the more cautious approach to ensure compliance with PECR will be to obtain prior consent as above.

Commercial risks and opportunities

The press attention surrounding the WhatsApp story demonstrates the importance of ensuring that data are handled in a way that consumers consider fair and useful to them. The benefits of doing so exist on all sides of the relationship: organisations can engage more meaningfully with their customers, and customers can benefit from advertising and offers that are of real relevance to them. However, it is clear that if individuals feel that their data are being sold to make a fast buck, and that they will be bombarded with unwanted advertising as a result, brands will suffer.

It is crucial to ensure that individuals are aware of how they can benefit from proposed data sharing. Enabling an element of control can also be an excellent means of building trust with customers. Indeed, transparency and consent are the bedrock of data protection compliance requirements and, when used in the right way, can be powerful tools for organisations in building their brand.

Alison Deighton
TLT LLP
alison.deighton@TLTsolicitors.com