How to guide
Mobile and cookies legislation

Published by
The DMA Mobile Marketing Council
First edition, April 2012

Contents

Acknowledgements 2
Introduction 3
1. Are mobile devices any different to PCs? 4
2. Legal issues from the Regulations 5
2.1 What does the legislation say? 5
2.2 What is a cookie? 5
2.3 Consumer Perceptions of the Regulations 5
2.4 How should positive consent be obtained? 6
2.5 The 'strictly necessary' exemption 7
2.6 Short form website terms and conditions and privacy / cookies policies 7
2.7 Enforcement and penalties 7
3. Technical issues and solutions 9
3.1 Messaging 9
3.2 Mobile web 9
3.3 Apps 9
3.4 Web Apps/HTML 5 10
3.5 QR or barcode scanning 10
3.6 Bluetooth 10
3.7 Near Field Communications or contactless 11
3.8 Other mobile channels 11
4. Compliance and best practice matrix 12
About the DMA 13
Copyright and disclaimer 14

Acknowledgements

The DMA wishes to thank the following members for their contribution to this white paper:

Written by:
Mark Brill, txt4ever / Formation

Contributions from:
Jonathan Bass, Incentivated
Jo Garcia, Traction Platform

Introduction

From 26th May 2011 additional measures generally referred to as 'cookies regulations' came into force as part of an update of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). From now on in this paper, we will refer to the recently amended regulations as "the Regulations."

Recognising implementation issues, the ICO has set a deadline of May 2012 before they start to enforce fully the Regulations insofar as they apply to the use of cookies and similar technology.

This paper looks at the legal, compliance, technical and best practice issues around the Regulations in relation to mobile devices. For the purposes of this paper, we have used "mobile devices" to cover both mobile phones and tablet devices which use mobile or mobile-style operating systems.

Prior to the new Regulations, brands were required to provide "clear and comprehensive information" (for instance by a privacy policy or terms and conditions) about the purposes of any cookies or similar technology which they used to access or store information on any "terminal equipment" (including mobile devices). These cookies etc might be used to track, store, retrieve or use information from users' visits to their websites and/or how they respond to emails. Cookie users were also obliged by law to provide users with an opportunity to refuse the operation of this technology.

However, following the introduction of the Regulations, which implement a Directive that applies across the European Union, the obligation to provide an opportunity to refuse the operation of a cookie has been changed to a requirement that organisations obtain opt-in consent to the use of these devices. For further information about what consent means please see the ICO Guidance on the rules on use of cookies and similar technologies published 13 December 2011.

Although the Regulations are well-intentioned, implementation at a practical level can be challenging. Currently the Government is working with web browser organisations to develop a technical solution to the opt-in requirement, but so far as we understand it, the ICO does not have a specific mobile strategy.

Mark Brill
Chair, Mobile Marketing Council

1. Are mobile devices any different to PCs?

Mobile phones can present a more complex landscape than PCs. Although the Regulations have been called the 'Cookies Law', they actually cover the use of any technology to access, store or retrieve information stored in "terminal equipment" such as mobile devices or laptops. However, the range and limitations of mobile browsers means that there is a greater need for marketers to implement their own solutions. Information stored in apps, including personal information, will also come under the Regulations, as do the hybrid web-apps or HTML5 apps. Some limitations of the mobile device may make it harder than the fixed-internet to present a detailed privacy policy at the point where an opt-in is required. Therefore marketers will need to consider carefully how to create the best user experience to achieve this.

For mobile users, the Regulations may also present something of a problem. As mobile devices are not shared, they are highly personal. What may be acceptable on a PC browser may well not be acceptable for the mobile user. This is particularly the case where location data is concerned; mobile users may regard their privacy as paramount.

In spite of some confusion around mobile and cookies, one key message in this white paper is, 'don't worry'. You can comply with the Regulations by:

- gaining a better understanding of the legal aspects through this document (though this document is not legal advice and specialist legal advisers should be consulted before finalising and executing any strategy for compliance with the Regulations)
- gaining a better understanding of your customers' or users' privacy expectations
- using our matrix at the end of this White Paper, which suggests how to work with the different technology channels
- monitoring and acting on guidance published from time to time by the ICO, before full enforcement of the new cookie rules in May 2012.

In short, brands that follow the principles of transparency and permission with their web and mobile users and take advice when appropriate should not fall foul of the legislation.

2. Legal issues from the Regulations

2.1 What does the legislation say?

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 amend the Privacy and Electronic Communications (EC Directive) Regulations 2003 . The part of the Regulations applicable to cookies and similar devices now reads:

> *6 (1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.*
>
> *(2) The requirements are that the subscriber or user of that terminal equipment--*
> *(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and*
> *(b) has given his or her consent.*
>
> *(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.*
>
> *(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.*
>
> *(4) Paragraph (1) shall not apply to the technical storage of, or access to, information--*
> *(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or*
> *(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.*

The key change is paragraph 2 (b) **'has given his or her consent'**. From 2003 until the new Regulations, organisations were only required to "provide clear and comprehensive information about the purposes" of the cookie, for instance via their published terms and conditions or privacy policy, and offer an opt-out. The obligation to provide clear and comprehensive information remains, but the change to opt-in consent has a much greater impact on how brands carry out their activities online and through mobile.

2.2 What is a cookie?

Technically speaking a cookie is a file containing information specific to a user, passed through an internet protocol such as a web browser (or mobile web browser) and stored on a person's device. However, the Regulations apply to any equipment used to "store or gain access to information stored in terminal equipment". In mobile, the storage of this kind of data can happen through different technology channels. Besides mobile web browsers it also includes personal information stored in apps.

2.3 Consumer Perceptions of the Regulations

In order to help brands and marketers implement best practice in relation to the changes in the regulations, the DMA surveyed consumers about their attitudes towards cookies. The survey was carried out at the end of July 2011 using Toluna Quicksurvey, with 1000 respondents. Key findings were:

- 89% of people were aware of cookies
- 60% knew what they were
- 72% thought desktop and mobile cookies worked in the same way
- 57% of people were concerned about internet security
- 66% were concerned about security in the mobile web
- 36% have opted out of website cookies

This suggests that public awareness of cookies and tracking is relatively high. More than half the respondents were concerned about security of their data, but when it comes to mobile that figure was closer to two thirds. Given that few sites have implemented an opt-in for cookies, the fact that 36% have opted out is also a significant figure.

For brand marketers, this confirms the need for transparency beyond just the regulatory requirements. Brands may be concerned that users will simply not opt in to cookies or tracking in apps when presented with a clear option. However, marketers will have to consider if the tracking is really necessary, and where it is, offer a clear explanation that will create trust with customers. Ultimately, to deliver best practice, brands will need to develop a great user experience.

2.4 How should positive consent be obtained?

Once positive consent has been obtained for the dropping of a cookie on a mobile device, the Regulations make it clear that it is not necessary for further consents to be obtained each time that cookie subsequently accesses or stores information on that same device. The PECR is not clear if that consent needs to be sought for each device. For example, if a user visits a site from their PC, should consent be sought again for their mobile phone and once again if they access it on a tablet device? It is generally difficult for marketers to know if someone has previously accessed the site from another device prior to delivering a cookie to the device from which the user is currently accessing the site. Best practice would therefore mean obtaining positive consent from the user in respect of each device, including the mobile they are using. However, in the case of email marketing, the sender of the message will have no idea which device the recipient will read the email message on and therefore in this case there is no need to get positive consent from the recipient in respect of each device.

Is it sufficient for consent to be obtained after the cookie has been dropped? The Regulations require "consent" not "prior consent" and in its latest ICO Guidance says that " it is difficult to see that a good argument could be made that agreement to an action could be obtained after [the event]". ICO goes on to say, however, that where it is "not possible" to delay the setting of cookies until users have had the opportunity to understand what cookies are being used and make their choice….websites should be able to demonstrate that they are doing as much as possible to reduce the amount of time before the user receives information about cookies and is provided with options."

In summary therefore, where it can be shown that prior consent is "not possible," ICO may well accept consent being obtained after the event, but this must happen just as soon as possible after the cookie has been set. Please see the section on 'Prior Consent' in the ICO Guidance on the rules on use of cookies and similar technologies published December 2011.

This may not be the view of the regulators in other European countries.

Turning to practical approaches to obtaining consent, ICO's updated Guidance contains useful examples of how this might be done. For example, a personalised URL (PURL) could take the user to a web page with a prominent panel at the top stating "We use cookies to make your experience of our website better. To comply with the new e-Privacy Directive, we need to ask you for your consent to set these cookies. [I agree] [No thanks] (link: "Find out more")

For more examples please see the section 'Practical Issues for those wishing to comply' in the ICO Guidance on the rules on use of cookies and similar technologies published December 2011 for other alternative methods of obtaining consent.

In the context of mobile web a positive response to a request, such as a pop-up or script window to accept the cookies would constitute consent provided, of course, suitable disclosures are provided about the cookies before that consent is given. The legislation also allows for consent to be given via browser controls (see Introduction and Section 2.1 What does the legislation say, above). To date, however, neither PC nor mobile browser software manufacturers offer sufficient functionality for users to give positive consent to the use of cookie technology using the settings on their browser software in the manner described in the PECR. Currently, therefore, marketers will need to obtain positive consent directly through the technology channel, rather than relying on user settings in the browser software to do so. As the ICO was not at the time of writing specifically considering mobile-web browser technologies, it is likely that any technology solutions for desktop will not necessarily be available for mobile devices in the first instance.

What is clear is that positive consent requires brands to be transparent about what cookie technology they will be using, and how they will use the information obtained through the use of such cookie technology. Best practice would be to publish a list of cookies and other tracking technologies, along with their purpose, which is clear, comprehensive and easily accessible to users through a privacy and/or cookie policy. As brands should now be

undertaking a cookies audit in order to meet the May 2012 compliance deadline, they would be prudent to include all mobile channels in that audit. There is some concern among marketers that a positive consent statement may be alarming to the user, and few people will give their consent. In mobile channels in particular, brands will need to carefully consider the user experience and the wording of positive consent statements. For example, some marketers have taken a more customer friendly approach, along the lines of:

'In order to deliver you the most relevant offers, we may add tracking information to your device. Please see our Privacy and Cookies Policy for more information

Click here to read the privacy and cookies policy
Click here to accept the privacy and cookies policy'

The wording in any privacy policy relating to the use of cookies should be clearly accessible. This is an acceptable way of getting consent to cookies for new subscribers but is not an acceptable way of getting consent to cookies for existing subscribers. Please see the section 'Practical advice for those trying to comply' the ICO Guidance on the rules on use of cookies and similar technologies published December 2011.

2.5 The 'strictly necessary' exemption

The legislation makes a clear exception for the use of cookie technology or trackable links which are "strictly necessary" for the provision of a service, which is provided at the request of the user. There is no requirement to gain consent to the use of such types of cookie technology, nor is there a requirement to provide clear and comprehensive information. However, best practice would be to include clear and comprehensive information about the use of such types of cookies in the interests of transparency and educating consumers about how cookies work. Examples of cookie technology which would fall into this exemption would include the security cookies used in respect of online financial services, and the cookies used to store online purchases in shopping carts used in both mobile websites and in apps. However, the ICO takes a strict view of what cookie technology would fall into the 'strictly necessary' exemption. It is likely that organisations who are using cookies which fall into the 'strictly necessary' exemption will also be using other types of cookie technology which do not fall into the 'strictly necessary' category and therefore positive consent is still required for these other types of cookies.

2.6 Short form website terms and conditions and privacy / cookies policies

For the limited screen space in mobile, best practice would suggest creating a short version of a short form cookie policy and/or cookie and privacy policy with the key information that can be easily presented on a mobile screen. Consideration should be given to a layered approach, where a link is provided to a website where users can get a fuller summary of the policies and another link, if they want to see the full version of the policies.

2.7 Enforcement and penalties

The ICO will carry out the enforcement of the Regulations. Neither the Regulations nor the ICO make any distinction in technologies but both focus on the activity of using cookie technology to access and store information held on a computer or similar device.

We contacted the ICO with regards to mobile cookies for this paper. It told us that the period until 25 May 2012 is for marketers to get their house in order and 'to take the steps they need to in order to comply with the PECR'. The important element is that organisations must be seen to be addressing the issue, even if they have not yet found the perfect method of how to obtain positive consent to the use of cookie technology.

It said it was 'unlikely to enforce the PECR against organisations taking steps to comply with the rules during this period'. However, it may use evidence of organisations not addressing the issues during this period, in determining what enforcement action to take after 25 May 2012. The ICO also confirmed that it does not make any distinction between the use of cookie technology in respect to mobile terminal equipment, and its use in respect to fixed terminal equipment such as PCs but 'would consider the individual circumstances of each case'. It is worth noting here that another change made by the Regulations was to greatly increase the penalties for breaching any part of the Regulations and extend the penalty notice procedure for major breaches of the principles under the Data Protection Act 1998 to breaches of the Regulations. The ICO would prefer to work with an organisation to resolve directly

a problem with it first; 'our approach is generally to seek compliance informally without first resorting to formal enforcement action'.

With regards to mobile technology solutions to opting in to cookies, work is still to be done: the Department for Culture Media and Sport (DCMS), the Government Department with responsibility for policy in this sector, is aware of the need to consider this area (it has said it is on the agenda) but at time of writing it has not had direct discussions with mobile specific developers.

3. Technical issues and solutions

This section considers the main mobile technology channels and steps to ensure that opt-in consent is taken.

3.1 Messaging

Tracking in SMS and MMS would take place by using a unique or personalised URL (PURL) in the message, although this is not commonly used. On clicking the link, this PURL can be associated with the mobile number (or CLI) and subsequently tracked. A PURL in an SMS or MMS is 'inferred' and tracking would only occur once the recipient lands on the web page. As there is no information stored on the mobile device (or terminal equipment) this would not fall within the Regulations.

3.2 Mobile web

The mobile web is growing rapidly with more and more consumers accessing brands via their smartphones. At the same time, brands are creating mobile specific and optimised websites to meet this demand. Mobile web browser software generally offers fewer opportunities than PC browser software for users to give their positive consent to the use of cookie technology, so the option of relying on functionality in the mobile web browser software to meet the Regulations is currently not possible in mobile. Similarly, the functionality in PC versions of websites, such as pop-up windows or Javascript boxes may not be possible to execute in the mobile channel. Marketers should therefore obtain specific consent for the use of cookies and other tracking technology in respect to mobile versions of websites (see comments above, under section 2.4 How should positive consent be obtained).

Acceptable practices:

- Where cookie or other tracking technology are used to access information stored on a user's mobile handset, positive consent can be obtained either through a landing page to which all visitors are directed, where they must accept the use of cookie or other tracking technology before they can move onto the page they have requested (see comments under 3.1 Messaging).
- Alternatively, in order to gain access to the mobile version of the website beyond the homepage, users could be required to go through a registration process, as part of which they would have to positively consent to the use of cookies or other tracking technology. See section 2.4, How should positive consent be obtained, for examples of how this could be done.

3.3 Apps

While mobile native apps are not referred to specifically within the Regulations, they would be relevant where apps set cookie or other tracking technology on a user's mobile handset, and are used by the marketing organisation to access information on the handset. Apps offer one significant benefit in terms of compliance; when a user first opens the app after downloading or before downloading it, they can be asked to accept a set of terms and conditions, in which positive consent to the use of cookie or other tracking technology can be obtained. Please see the section 'Practical Issues for those wishing to comply' in the ICO Guidance on the rules on use of cookies and similar technologies published December 2011 for further information about using terms and conditions as a means of obtaining consent for the use of cookie technology.

Apple has previously allowed tracking in apps via a unique device code, or Unique Device Identifier (UDID). Although they no longer intend to make this available to app developers for tracking, it is important to note that any unique device tracking such as a UDID would require positive consent under the Regulations. Marketers should also be aware that existing apps which use cookie or other tracking technology may need to be updated, and new disclosures about cookies may need to be presented to users (see section 3.1 Messaging – problematic practices above) and positive consent obtained.

Acceptable practice:

- Positive consent for the use of cookie or other tracking technology obtained at the point either the app is downloaded or used for the first time provided the consent is obtained before the cookie is dropped.

Problematic practices:

- Existing users of apps may need to positively consent to the use of cookie and other tracking if they have previously been offered the opportunity to refuse the use of such technology under the 2003 regulations. The DMA will clarify the position at a later date.
- Positive consent to the use of UDID tracking needs to be included in the app terms and conditions, if it is being used.

3.4 Web Apps/HTML 5

The hybrid or a web app typically uses HTML5 to give users a rich-content experience via the mobile web. Such apps may store cookies and other tracking information about their user. It is also important to be aware that HTML5 has the facility to cache data onto the user's handset and, with it, track data beyond cookies. Although a web app does not have to be delivered via an app store, the user experience is similar to an app. Positive consent can therefore be taken in much the same way as an app, with agreement to use of the cookie obtained the first time the app is accessed or downloaded.

Acceptable practice:

- Positive consent should be obtained when the user first downloads or opens the app.

Problematic practice:

- Existing users of apps may need to positively consent to the use of cookie and other tracking, if they have previously been offered the opportunity to refuse the use of such technology under the 2003 regulations. The DMA will clarify the position at a later date. App providers may be recommended to update their terms and conditions to include positive consent to the use of cookie and other tracking technology, and to get users to accept the new terms and conditions when the next version of the app is released.

3.5 QR or barcode scanning

The activity of scanning a code would not in itself require positive consent. In some instances, such as direct mail, it is possible to deliver an individual code to each user which can contain unique information such as a PURL. As with SMS and MMS, a PURL does not store tracking data on the mobile (terminal) device, it would not fall within the legislation.

Unique barcodes or QR codes delivered to a mobile device for ticketing or airline check-ins would also not store tracking information. Furthermore they would fall within the strictly necessary exemption discussed in para 2.5 above and would not therefore require positive consent.

3.6 Bluetooth

The Bluetooth channel has been used for proximity marketing in a number of areas. As a radio frequency, it is not covered directly by the Regulations. However, care needs to be taken when using Bluetooth to deliver websites, apps or content which may use cookies or other tracking technology.

Acceptable practice:

- Where tracking technology is sent to the handset, positive consent should be obtained when the user initially opens the content

3.7 Near Field Communications or contactless

NFC is only just starting to roll out for payments and, as yet, few marketing campaigns have been developed in the channel. Although the ICO has not published any guidelines on this channel, as it is part of the radio spectrum, it would fall under the Regulations. As with the other channels, NFC marketing may present a file to the handset which may store trackable information. Alternatively, NFC content may be delivered via an app. In either case, positive consent to the use of cookie or other tracking technology should be obtained before the first time the user accesses the file or app on the handset.

3.8 Other mobile channels

While there are no other mobile technologies in use for brand marketing, channels such as social media pages, social location check-ins or augmented reality are being widely adopted in mobile marketing. However, none of these specifically come within the Regulations and are delivered via web, apps or messaging (including email). Thus, following the acceptable practice for the relevant channels will include all other mobile channels.

4. Compliance and best practice matrix

	Service tracking	Cookies	PURL	App tracking	Track-able gifs	Notes
Messaging (SMS and MMS)					Only relevant to MMS	PURL in an SMS or MMS is 'inferred'. Tracking would only occur once the recipient lands on the web page
Mobile email						The same as desktop email - please refer to email paper
Mobile web						Strict definition of service. Browsers may not offer appropriate technology solutions
Apps						Opt-in taken on first opening. Caution with apps already installed on handset
Web apps (HTML5)						Caching in HTML5 may require an opt-in
QR codes, or Image Recognition Scanning						Where PURL is used it is 'inferred'. Tracking would only occur once the recepient lands on the web page
Bluetooth						Bluetooth not covered by PECR, but content sent over the network may require opt-in if tracking is used
NFC						No guidelines as yet, but care should be taken with content or apps if tracking or cookies are used

Consent not required

Consent must be taken

Consent not required, but may have implications if the user is taken to website or app

About the DMA

The Direct Marketing Association (DMA) is Europe's largest professional body representing the direct marketing industry. With a large in-house team of specialists offering everything from free legal advice and government lobbying on direct marketing issues to research papers and best practice, it is always at the forefront of developments in the industry.

The DMA protects the direct marketing industry and consumers. It promotes the highest standards through self-regulation and lobbies against over-regulation. The DM Code of Practice sits at the heart of everything we do – and all members are required to adhere to it. It sets out the industry's standards of ethical conduct and best practice.

Our 10 DMA Councils/Board Committees cover the whole marketing spectrum – from the digital world of social media and mobile marketing to the 'real' world channels of door drops and inserts. The Councils are made up of DMA members and regularly produce best practice and how to guides for our members.

We also have a packed calendar of conferences, workshops and discussions on the latest topics and best practice, and 80% of them are free for members and their staff.

As the industry moves on so do we, which is why we've recently launched a number of new services for our members – a VAT helpline, a Social Media Helpdesk and an IP Protection Service.

Visit www.dma.org.uk regularly to keep up to date with all our services.

Copyright and disclaimer