Cookies law: exemptions for providers of online games

The new cookie law has been in force in the UK for almost two months, and requires websites to gain explicit consent from users before using cookies. However, there are a number of exceptions to the rule that could lessen the burden for online gaming service providers. Simon Halberstam, Partner at Kingsley Napley, discusses the new rules in detail, what they mean for online gambling operators and the focus of the Information Commissioner.

On 26 May 2012 the Electronic Communications (EC Directive) Regulations 2003, which governs websites' use of cookies in the UK, came into force. At the time of writing, very few websites are compliant.

The new law requires websites to gain explicit user consent to receive a cookie prior to deployment. The precise requirements for compliance were not, and remain somewhat, unclear. The Information Commissioner's interpretation of the new Regulations is summarised below.

Consent

Consent must involve an end-user knowingly indicating acceptance of the cookie(s) that it is downloading, this could for example be by way of click acceptance.

Although the cookies Regulations do not use the term 'prior', the Commissioner expects cookies to be sent only after consent and full information about the cookies to be downloaded has been given. It is recognised that cookies are often automatically downloaded the moment a user arrives on a site. If possible, web managers should postpone the download of cookies until users have been given sufficient information to make a choice about whether or not they want cookies on their machines. If delaying the download of cookies is not possible, websites should ensure they minimise the time between the first cookie being downloaded and the point where sufficient information is provided to the user and consent to permit the cookie to remain on its machine can be given.

Responsibility for compliance

The Commissioner considers that the person or entity setting the cookie is primarily responsible for compliance with the cookie Regulations. However, when a third party's cookies are deployed via a website, the Commissioner takes the stance that both the website owner and the third party are responsible for compliance.

In practice, the information requirements and opportunity for a user to give its consent will be provided on the website that the cookies are dropped from. As such, third parties dropping cookies, and the sites through which they drop cookies, are encouraged to work together to achieve compliance. Third parties should seek to impose contractual obligations upon the websites through which they drop cookies in respect of compliance with the consent and information requirements in the Regulations.

Avoidance tactics have also been considered by the Commissioner. A website hosted overseas (outside the EU) will be likely to fall within the ambit of the Regulations if:

- the organisation which owns the website is based in the UK; or
- the website itself is targeted at the European market; or
- products and services are provided from the website to customers predominantly based in Europe.

Enforcement

The Commissioner has also revealed the primary enforcement actions available to him for organisations that refuse or fail to comply with the Regulations, namely:

- Information notice. A request for specific information from an organisation within a specified time frame.
- Undertaking. An organisation must carry out specific action to improve its level of compliance.
- Enforcement notice. An organisation must carry out specific actions to ensure compliance with the Regulations. Failure to comply with this notice may be considered a criminal offence.
- Monetary penalty notice. A fine of up to £500,000 to be used only for the most serious breaches.

Enforcement action will be proportionate to the associated privacy concerns. As such, cookies that do not greatly impinge on a user's privacy rights (e.g. first party analytical cookies and those used to support the accessibility of sites and services) are likely to register extremely low on the Commissioner's priority list for enforcement.

The Commissioner has gone as far as suggesting that, while not considering them exempt from the Regulations, he is unlikely to take action in respect of cookies that do not impinge on users' privacy. On the other hand, organisations dropping cookies that focus on gathering user's personal information will be the main focus for enforcement.

Potential Exemptions for providers of online gaming services

Of particular interest to operators in the online gaming sector is the statutory exemption from obtaining prior consent where a

deployed cookie is 'strictly necessary for the provision of an information society service requested by the subscriber or user'.

In this context, an 'information society service' is defined as 'any service normally provided for remuneration, at a distance, by means of electronic equipment... at the individual request of a recipient of a service'. The Information Commissioner has indicated that this definition covers cookies that manage online 'shopping baskets', serving to remember information about products or services that an individual has indicated a desire to purchase whilst it navigates around, or temporarily leaves, the site.

This exemption should serve to lighten the burden for the online gaming industry. Specifically, it could allow sites to continue to use cookies to record information such as an individual's balance of funds, ticket purchases, and winnings in much the same way as they do now. As involvement in online gaming activity is actively requested by users when they choose to play games online, the download of cookies which specifically manage their engagement with that service seems likely to fall within the exception set out above.

What needs to be done now?

Web managers in the UK should therefore be doing the following:

- Ascertaining what type of cookies are used by their websites and how they are downloaded onto users' machines (effectively a 'cookie audit').
- Gauging the likelihood of existing cookies' fitting within the 'provision of service' exemption detailed above.
- Deciding on which method(s) of obtaining consent to cookies are best for their website, given the results of the cookie audit.
- Recording the cookie audit and implementation methods in an easily digestible form, lest the ICO investigate the site.

The fundamental problem seems to be a disconnect between the law and technology. In most cases the law is running to try to keep up with the technology.

Suggested methods of implementation

Below are a few options, which have been suggested to procure user consent before cookies are downloaded. Please note that consent only needs to be provided by a user the first time each type of cookie (used for the same purpose) is downloaded onto its machine:

- Pop-ups each time a new type of cookie is to be downloaded onto a user's machine.
- Having in place a privacy policy setting out the site's use of cookies; the terms of which a user must positively accept upon visiting the site for the first time (e.g. via a tick box).
- Settings and feature-led consent. If cookies are downloaded when a user does something e.g. watches a video or personalises the site, obtaining the user's consent prior to feature access.

Web managers should bear in mind the 'strictly necessary' exemption, but be careful not to place excessive reliance on it.

What next?

The ICO has suggested that, in the near future, consent could be validly provided through users' web browsers. ICO guidance envisages a future scenario whereby a user accesses a website via a sufficiently sophisticated web browser set up to reject certain cookies and accept others, allowing a web manager to assume that the user has provided its consent accordingly. However, it is acknowledged that many web browsers are not sufficiently sophisticated for this method to be currently viable. The Government is therefore currently consulting with the major web browser manufacturers and it is envisaged that an announcement as to compliance via this unobtrusive method will eventually be made.

However, the Article 29 Working Party (a group of data protection regulators from EU Member States) has given a non-binding (albeit very persuasive) opinion on consent via web browsers. The Working Party has suggested that reliance on users navigating websites via sophisticated web browsers is not, in itself, a substitute for procuring their positive consent to the download of cookies. Instead, the Working Party has suggested that web browsers need to be supplied to consumers with a default setting of rejecting cookies. In order for consent to be validly given via these browsers, users would also have to be provided with comprehensive information about cookies before actively changing their browser settings to allow cookies.

Conclusion

The fundamental problem seems to be a disconnect between the law and technology. In most cases the law is running to try to keep up with the technology (e.g. super-injunctions failing to keep pace with the rise of social media). However, in this case the law is way ahead making unrealistic demands of the current technological landscape and necessitating that developers build innovative solutions to meet the new legal requirements.

Simon Halberstam Partner
Kingsley Napley
SHalberstam@kingsleynapley.co.uk