Diving into the EC's draft ePrivacy Regulation: steps for online gambling operators

The European Commission's newly proposed ePrivacy Regulation was unveiled on 10 January 2017. Anne Rogers and Simon Halberstam of Simons Muirhead & Burton LLP discuss the proposed Regulation in detail and what it means for online gambling operators and crucially, what they need to do today in order to ensure that they comply.

On 10 January 2017, the European Commission ('Commission') unveiled its newly proposed ePrivacy Regulation ('Proposed Regulation') to reinforce trust and security in digital services and the handling of personal data as part of the Commission's Digital Single Market strategy. The Proposed Regulation would replace Directive 2002/58 (often known as the ePrivacy Directive) and needs to be read together with the General Data Protection Regulation ('GDPR'), which will come into force on 25 March 2018. We look at the key changes applicable to online gambling operators and their affiliates.

Extraterritorial effect

The Proposed Regulation, like the GDPR, will have extraterritorial effect. It applies to the processing of electronic communications data carried out in connection with the provision and use of electronic communications services in the European Union ('EU'), regardless of whether or not the processing takes place in the EU. The definition of 'electronic communications services' is the same as that in the proposed new European Electronic Communications Code. This definition is very broad and is likely to apply to all services that have a communications element - meaning gambling apps and gambling websites, even if they are only 'ancillary' to another service. Gambling operators will therefore be caught even if they are resident outside of the EU but provide electronic communications services to end-users in the EU. It does not matter whether the services are paid for or not.

Using cookies and direct marketing

As is the case now, the rules on direct marketing and use of cookies and other tracking technologies (including device finger printing and spyware) apply to all websites, regardless of whether they fall within the definition of electronic communications services. The key proposed changes to the rules for cookies are as follows:

Consent

Under the current legislation, it is sufficient to inform users on your website what cookies you use and what their purpose is. However neither the method by which consent must be given by the website user nor the timing of such consent is prescribed. The most common model used is 'implied consent,' which basically means that it is acceptable to use cookies when a user visits the website, as long as it is given information and the option to change how cookies are used. This is often achieved through cookie banners. The Proposed Regulation requires that consent to the downloading of cookies must be 'freely given, specific, informed, active and unambiguous.' This may be expressed by a statement or clear affirmative action 'at the moment of installation.' Where web browsers are already installed, consent must be requested at the time of the next update or, at the latest, by 25 August 2018. It remains to be seen how this will work in practice. For instance, what will be the default setting if a user doesn't accept the use of cookies prior to installation?

Exceptions

The Proposed Regulation sets out a number of exceptions to the cookie consent rules including if it is necessary for: 1) the sole purpose of carrying out the transmission; 2) providing an information society service, e.g. adding items to a shopping cart; or 3) web audience measuring (this only applies to first party cookies, however).

Privacy settings

In the context of cookies, consent may be expressed by browser settings and the Proposed Regulation places specific obligations on browser providers to ensure that appropriate consent settings and options are given to individuals to prevent third parties from: 1) storing information on their devices; and 2) processing data already stored on an end user's device. The Proposed Regulation suggests offering end users a number of different privacy settings in a user friendly manner, ranging from higher (e.g. 'never accept cookies') to lower (e.g. 'always accept cookies') and intermediate (e.g. 'reject third party cookies'). In practice, if a user has rejected the use of third party cookies at installation and changes their mind, they are unlikely to go into their browser settings to change such settings. Gambling websites that wish to rely on cookies for marketing, tracking and behavioural purposes may therefore want to consider using opt-in consents to override this through the use of pop-up boxes or similar.

Collection of device information

The collection of device information e.g. for Wi-Fi logins is prohibited, other than for the purposes of establishing

Anne Rogers Associate
anne.rogers@smab.co.uk

Simon Halberstam Partner
simon.halberstam@smab.co.uk

Simons Muirhead & Burton LLP, London

the connection, unless a 'clear and prominent' notice is displayed 'on the edge of the area of coverage' informing the user of: how the data will be collected, the purposes for which it will be used, the person responsible for collecting it and any other information required under the transparency requirement of the GDPR to make such processing fair. The Proposed Regulation and the Information Commissioner's Office ('ICO'), the UK's data protection regulator, suggest using standardised icons, layered models and just in time notices to make information user friendly.

Direct marketing

Overall, the rules on direct marketing remain largely unchanged.
The key changes are:

- Scope. The recitals note that the direct marketing rules will apply to communications sent by 'instant messaging applications,' 'MMS' and 'Bluetooth' as well as the more traditional telephone calls, email and SMS.
- Telephone marketing. Any organisation that wishes to carry out telephone marketing must either: 1) display calling line identification, or 2) present a specific code/or prefix identifying the fact that the call is a marketing call.
- Consent. The consent required for any direct marketing is the same as that for cookies and that required under the GDPR, i.e. consent must be freely given, specific, informed and unambiguous. Pre-ticked boxes, for instance, will no longer be acceptable. As is the case now, prior opt-in consent is required for email and SMS marketing.

Many will be relieved to see that a soft opt-in is still sufficient 'in the context of the sale of a product or a service' (initially there was concern this option would be removed). This means that emails may still be sent to existing customers to market similar products or services, subject to an opt-out being provided free of charge at the time that the data was collected, and with each subsequent email marketing message. Unlike under the current UK Privacy and Electronic Communications (EC Directive) Regulations 2003 this will however no longer extend to the 'negotiations for the sale' of a product or service. It is likely therefore that businesses will no longer be able to rely on obtaining soft opt-in consent from consumers who have previously requested quotes for similar products or services but then not proceeded with the transaction.

Metadata and electronic communications data

Confidentiality provisions

The Proposed Regulation states that both the content and metadata of any communication, 'including calls, internet access, instant message applications, email, internet phone calls and personal messaging provided through social media' should be kept confidential. This is a significant change from the existing position and operators should note that any interaction with individuals must be kept confidential, for example, any information users share with a chatbot on the website.

Use of metadata and electronic communications data

Service providers will need users' consent to use metadata (e.g. location data) to provide services. The two exceptions to this are transmission and/or security. For the use of communications content, in order to provide services, the rules are stricter. Providers of electronic communications services may process electronic communications content only if they pass the two step test: 1) they have obtained end users' consent to such processing for the service; and 2) such service cannot be fulfilled without the processing of such consent. An exception to this rule is if all end users have given their consent for a purpose which cannot be fulfilled by processing information that is made anonymous and the provider has consulted the supervisor authority.

Consent

Consent for the use of both communications content and metadata for the provision of services can be withdrawn at any time, but in addition, service providers must remind end users every six months that they have the right to opt-out.

Enforcement

Gambling operators and their affiliates face enforcement of their obligations under the Proposed Regulation by the ICO and the Gambling Commission.

The ICO

The ICO will have stronger enforcement

Website operators should review their privacy policy with their legal advisors and introduce the concepts of layering and if applicable, just-in-time notices.

continued

powers than under the current regime. The most significant changes will be the level of fines the ICO will be able to impose, and these are in line with the GDPR: operators and their affiliates could face fines of up to €20 million or 4% of annual global turnover for security breaches, infringement of time limits for erasure and unlawful processing of data; with a maximum fine of €10 million or 2% of annual global turnover for breach of privacy obligations, failure to provide relevant cookie information and sending unsolicited marketing messages.

On 10 November 2016, the ICO announced that it was specifically cracking down on the online gambling sector's use of personal data to promote online gambling. The ICO said it was writing to more than 400 companies, all believed to be e-gaming marketing affiliates, demanding they set out 'how they use people's personal details and send marketing texts.' This includes where they got people's personal information and how many texts they have sent. Back in March 2016, the ICO said it was expressly working with the Gambling Commission to combat spam marketing, particularly for SMS and calls.

The Gambling Commission

In line with the Gambling Commission's strategy to improve standards and 'ensure that the consumer is firmly at the heart of [the Gambling Commission],' the Gambling Commission is cracking down on gambling operators and their affiliates' use of personal data. On 26 January 2017, the Gambling Commission published a consultation on proposed changes to its enforcement strategy to move away from voluntary settlements and focus instead on licence reviews ('Consultation'). The Consultation also proposes higher fines on licence holders for regulatory breaches.

The Gambling Commission may take regulatory action against gambling operators situated overseas but who provide services to UK consumers, but it is not obvious that the regulatory obligations on operators extend to data protection matters. The Gambling Commission does, however, hold its licensees responsible for any third parties with whom they contract for the provision of any aspect of the licensee's business related to gambling activities (e.g. marketing by an affiliate).

What needs to be done now?

- Review marketing practices and terms with affiliates. Gambling operators should review their marketing practices and terms with affiliates with their legal advisors to ensure they are sufficiently robust in terms of ensuring compliance with the Proposed Regulation and the GDPR. In particular, operators should review how consent is obtained. Consent must be expressed by a statement or clear affirmative action. This means that pre-ticked boxes or silence will not constitute consent. Individuals must also have the ability to be able to withdraw consent as easily as they provided consent initially to any marketing activities.
- Carry out a cookie audit. Website operators should ascertain what types of cookies are used by their websites and revise their consent mechanisms, if necessary. This is part of the European Privacy by Design requirements. Reminders should also be sent every six months to remind end users that they have the right to opt-out of the use of their data for the provision of services.
- Review privacy policy. Website operators should review their privacy policy with their legal advisors and introduce the concepts of layering and if applicable, just-in-time notices. Layering allows a user to gain a headline summary of how its data is being used and an option to click on a long form policy for more information. This is particularly useful for apps and more user friendly for consumers. We would recommend holding back on the use of 'standardised icons' as the Commission and ICO have yet to provide an illustration of what these will look like.

What next?

The Proposed Regulation is not in its final form yet and still has to pass through the European Parliament. In the UK, the Proposed Regulation repeals the Privacy and Electronic Communications (EC Directive) Regulations 2003 and will take effect following Brexit if the ICO decides to implement it (as it intends to with the GDPR).

Conclusion

Provided the Proposed Regulation passes through the legislative process without significant amendments, gambling operators should consider and incorporate these new requirements into their GDPR planning.