DORSEY
DORSEY+WHITNEY LLP

Proposal for new European ePrivacy Regulation

by Ron Moscona

On 10 January 2017, the European Commission announced its proposal for new legislation which would update the law relating to privacy in electronic communications. The Commission has proposed a draft ePrivacy regulation that would repeal and replace the existing ePrivacy Directive (2002/58/EC) ("**ePrivacy Directive**"). The draft regulation aims to further the Commission's Digital Single Market Strategy by complementing and conforming privacy rules in the telecommunications sector with the General Data Protection Regulation (2016/679) ("**GDPR**"), which comes into force on 25 May 2018.

The EU's rules on data protection and privacy in electronic communications have always been intertwined and will remain so in the future under the twin regimes of the GDPR and the new ePrivacy Regulation. While the data protection rules (and the GDPR) set out a broad regime for the management of personal data by businesses and public institutions, the ePrivacy rules focus on the specific privacy duties of providers of telecommunication services in relation to the privacy of users' communications. The ePrivacy rules, however, are not only of interest to telecommunication providers as they regulate the use of all electronic communications including emails, fax, telephone, social media etc. and the use of cookies and similar devices on websites and mobile applications.

New technologies and communication platforms

Having conducted an evaluation of the ePrivacy Directive, the European Commission found that, although its objectives and principles remain sound, there have been important technological and economic developments in the market, which the ePrivacy Directive has not kept pace with. New "over-the-top" ("**OTT**") services, such as internet voice calls, instant messaging and web-based e-mail services, have an increasing presence in the market. The Commission found that these new services are not adequately covered by the ePrivacy Directive, which has resulted in a "void of protection of communications conveyed through new services". The Commission therefore

Related People

- Ron Moscona

Related Capabilities

- Privacy & Social Media
- Intellectual Property Litigation

concluded that new legislation was required and a directly applicable regulation was chosen in order to create uniform protection across the EU.

The draft regulation aims to bring ePrivacy rules in line with general data protection rules under the GDPR and it will bring OTT communication service providers, such as WhatsApp, Skype, Gmail, Facebook, etc., more expressly within the scope of the EU's ePrivacy laws (these communication platforms may already be covered by the existing directive however the position is not altogether clear).

The draft regulation also clarifies the territorial scope of the ePrivacy framework. The existing directive does not specify its territorial extent and the question was never properly or comprehensively addressed by the Court of Justice of the EU. The new ePrivacy Regulation will deal with the question head on and will apply to entities anywhere in the world that provide publicly-available electronic communications services to, or gather data from the devices of, end users located in the EU.

Communications content and metadata

The new rules aim to guarantee privacy for both content and metadata (e.g. time of a call and location) derived from electronic communications. Under the new rules, providers of communications services can only process the content of electronic communications if the end-users concerned have given their consent and the provision of that service cannot be fulfilled without the processing of such content. For any other purpose, content can only be processed if end-users consent to the processing of their content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted a supervisory authority.

Metadata can only be processed by service providers if it is necessary: (i) to fulfil quality of service requirements; (ii) for billing or interconnection payment purposes; or (iii) for detecting fraudulent use of the service. For any other purposes, metadata can only be used if the end-user has given their consent to the processing of their metadata for one or more specified purposes, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

Additionally, unless end-user consent has been obtained, service providers must delete metadata or make that data anonymous after it is no longer needed for the purpose of the transmission of a communication or, if kept for billing purposes, after the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

It may be recalled that in December 2016 the Court of Justice of the EU struck down national legislation in both Sweden and the United Kingdom which gave excessive powers to law enforcement and investigation agencies to require telecommunication providers to store metadata and to make it available to such agencies for crime investigation and anti-terrorism purposes. That decision took into account the anticipated new proposals for the ePrivacy Regulation and is closely related (see our update note

concerning that decision – EU court strikes down security legislation over privacy concerns).

Under the new rules, once consent is given for metadata and/or content to be processed, providers will be able to use the data to provide additional services (including services to third parties using the metadata as a rich resource for statistical and other data). The rules require using anonymisation unless this makes fulfilling the intended purpose impossible. Where service providers wish to use communication content (rather than metadata) for purposes other than providing the service itself, in addition to having to obtain the end-user's consent, the service provider will need to consult with its regulator. The Commission claims that this framework will provide traditional telecommunication operators with more scope to utilise data than they previously had and will therefore provide additional business opportunities in the digital space.

Update to the "cookies law"

The proposed regulation also aims to update and streamline the rules relating to the storage and tracking of cookies and other fingerprinting devices. The Commission concedes that the current rules have resulted in an overload of cookie-consent requests. Under the new rules, consent will not be needed for non-privacy intrusive cookies improving the end-user's internet experience or for cookies set to count visitors to a website (provided that such analytics is carried out by the service provider itself, i.e. websites using third party analytics such as Google Analytics will still require user consent).

Under the draft regulation, providers of web browsers and similar software are required to provide their users with cookie and tracking controls through their settings. As part of the browser software installation, or on the next update if the browser software has already been installed prior to the implementation of the new regulation, the software must inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting. This proposal removes the burden from website publishers and should mean that a cookie information box is not needed if consent has already been given through browser settings. However, in order for this to work in practice, there will have to be some degree of communication between the web browser and the website publisher in order to ascertain whether an end-user has consented or not. Web publishers and the advertising industry may have cause for concern that the proposed regulation will lead to more end-users blocking access to third-party advertising. This is of particular concern to providers of free online content, since advertising is often their primary source of revenue. Smaller advertisers may also be concerned that these new rules will favour larger providers such as Facebook and Google, who have the scale to gather permission from users more easily.

Unsolicited marketing communications

In keeping with the existing law under the ePrivacy Directive, the use of email and other

electronic communications for making unsolicited marketing communications without will be subject to an opt-in by the consumer and would otherwise be prohibited. Offences against these rules is one of the main focuses of enforcement activities across the EU and it is not uncommon for significant penalties to be imposed on offenders.

One of the main objectives of the new ePrivacy Regulation is to expand the rules against unsolicited marketing communications to new platforms such as social media and other OTT platforms as well as to apply them (for the first time) to telephone calls.

The new regulation will maintain the main exception applicable under the existing law which allows a trader to make unsolicited marketing communications to a consumer who purchased similar goods or services from the trader (as long as the consumer provided the electronic contact details voluntarily in connection with the original sale and subject to her right to require such marketing communications to be discontinued).

Additionally, under the new rules, marketing callers must display their telephone number or use a special prefix so that the call can be identified by end-users as a marketing call.

New enforcement powers

The proposed regulation introduces significant new enforcement powers (mirroring those in the GDPR), with potential penalties that may be imposed on offenders in amounts up to EUR 20 million or 4% of the total worldwide annual turnover of the offending entity, whichever is higher.

The legislative process

The EU Commission's proposals will be scrutinised by EU law makers in the European Parliament and the Council of Ministers. Both bodies must formally approve the legislation for it to take effect and, as such, there is scope for further amendments to the proposed regulation.

The GDPR proposals were delayed for several years (much longer than originally anticipated) largely due to heavy amendments to the draft legislation required by the European Parliament. However, the Commission has called upon the European Parliament and Council to work towards the adoption of the regulation before 25 May 2018, which is the date that the GDPR will enter into application.