March 3, 2017

# Cookies Crumble? The draft EU Regulation on Privacy and Electronic Communications

## Background

**Attorneys**
Rohan Massey

The European Commission recently published a proposed Regulation on Privacy and Electronic Communications (the "Regulation"). The Regulation aims to update and broaden the scope of current rules under the ePrivacy Directive (2002/58/EC) on confidentiality of electronic communications as well as align the rules for electronic communications, cookie usage and direct marketing with the forthcoming General Data Protection Regulation ("GDPR").

In line with the GDPR, penalties for infringement may be severe, with fines for infringement of the cookies and unsolicited communication rules potentially amounting to the greater of €10 million or up to 2% of the worldwide annual revenue. Infringements of the rules relating to confidentiality of content and metadata may be higher, with fines capped at the greater of €20 million or up to 4% of the worldwide annual revenue.

Though the new Regulation is planned to come into effect at the same time as the GDPR on 25 May 2018, it must first be formally approved by both the Parliament and the Council on a relatively ambitious timetable before it becomes law. Ultimately, the Commission hopes that the proposed Regulation will increase the protection of people's private lives and open up opportunities for new businesses.

## Scope of the Proposed Regulation

The Regulation covers almost all businesses that operate in Europe but, like the GDPR, also extends to businesses outside the EU if they provide services to users in the EU (including where such services are offered free of charge).

The Regulation applies to the processing of communications data carried out in connection with electronic communications services and to information related to end users' terminal equipment. The Regulation proposes extending coverage from telecoms companies and ISPs to also include providers of over-the-top ("OTT") services, including popular instant messaging applications. It further covers anyone using cookies or similar tracking technologies as well as anyone engaging in electronic marketing, whether or not they are providing an electronic communications service.

The Regulation does not apply to electronic communications services that are not publicly available. It also is inapplicable to government authorities engaged in detecting crime or otherwise protecting public safety.

## Electronic Communications Data

The Regulation distinguishes between two types of electronic communications data: electronic communications content and electronic communications metadata. Content refers to the actual information exchanged in an electronic communication, including text, voice, videos, images and sound, including, for example, a picture or video sent using instant messaging. Metadata refers to data processed by a network for the purposes of transmitting content, including information relating to the source and destination of a communication; the location, date, and duration of a communication; and the method of communication. For instance, data identifying that an instant message was sent at a specified time is metadata.

Many of the rules in the regulation require consent. Consent must be "freely given, specific, informed and unambiguous," which is the same standard as the GDPR. Consent can be expressed by a statement or clear

affirmative action. This allows consent to be expressed by using the settings of an application, which simplifies the acceptance or refusal process for users.

## Confidentiality

Under the Regulation, both electronic communications content and metadata must be kept confidential and must not be interfered with. However, the Regulation permits a limited number of exceptions to this basic rule in the following circumstances:

- Both content and metadata may be processed in order to (1) transmit the communication; (2) maintain or restore security; or (3) detect technical faults or errors in the transmission of the communication.
- Metadata may also be processed if (1) it is necessary to meet mandatory EU quality of service requirements; (2) it is necessary for billing; (3) it is necessary for detecting or stopping fraud or abuse; or (4) the end user consents to the processing for a specified purpose which could not be carried out using anonymised data.
- Content may also be processed if (1) for the sole purpose of providing a specific service, if the service cannot be provided without such processing and provided the end user has consented to the processing; or (2) the end user consents to the processing for a specified purpose which could not be carried out using anonymised data and the provider consults the GDPR's supervisory authority.

## Data Erasure

Electronic communications service providers must either erase or anonymise content after its receipt by the intended recipient. Metadata must similarly be erased or anonymised when it is no longer needed for transmitting the communication. The same exceptions of confidentiality listed above also apply to erasure of data. Metadata may be further retained until the end of a period in which a bill or payment may be lawfully challenged under national law.

## Cookies and Terminal Equipment

The Regulation prohibits the use of cookies (and similar tracking technologies, such as hidden identifiers and device fingerprinting) unless (1) it is necessary for the sole purpose of transmitting the communication; (2) the end user has consented; (3) it is necessary for providing an information society service (e.g., to add items to an online shopping basket) requested by the end user; or (4) it is necessary for web audience measuring if carried out by the information society service requested by the end user. No consent is needed for first-party cookies used by a website to carry out web audience measuring.

In addition, if cookies are used, the Regulation prohibits collecting device information unless (1) it is done only to establish a connection; or (2) users are notified how the data will be collected, the purposes for which it will be used; and certain other information.

All communications software (e.g., web browsers and other applications allowing the retrieval and presentation of information on the internet) must offer functionality to prevent the use of third-party cookies. Upon installation, the software must inform the end user about the privacy settings options. To continue with the installation, the end user must consent to one of the settings. For software already installed as of 25 May 2018, these requirements must be complied with by the first update of the software and no later than 25 August 2018.

## Direct marketing

The rules in relation to electronic direct marketing are broadly equivalent to current legislation under the ePrivacy Directive – subject to limited exceptions, opt-in consent will still be required before businesses are permitted to send electronic direct marketing. However, notable changes include the widening of the scope of the application of the rules to cover all electronic communications services, which include communications sent through instant messaging applications and Bluetooth.

For telephone calls, however, Member states may permit the placing of direct, non-automated, voice-to-voice marketing calls, provided that the end user has not expressed an objection to receiving such communications. Those placing marketing calls must inform end users of the marketing nature of the communication and of their identity. They must also give the end user the chance to easily exercise his/her right to withdraw his/her consent.

## Comment

The proposed scope of the Regulation is quite broad, encompassing almost all modern businesses and providers of electronic communications services. By replacing the current e-Privacy directive with a regulation, the Commission aims to provide a uniform set of rules that protect privacy for people and businesses.

The Regulation may allow for new business opportunities, as traditional telecoms operators will have more opportunities to use data and provide additional services once consent is given. The Commission also says that the rules on cookies have been simplified, for example by not requiring consent for cookies to simply monitor web traffic, although given the stricter consent requirements in respect of other cookies used, even with browser level consent controls, those cookie pop-ups look unlikely to disappear or even to crumble.