Council of the European Union

Brussels, 4 February 2019
(OR. en)

5934/19

Interinstitutional File: 2017/0003(COD)

TELECOM 41
COMPET 93
MI 89
DATAPROTECT 22
CONSOM 35
JAI 84
DIGIT 21
FREMP 12
CYBER 28
CODEC 263

NOTE

From:	Presidency
To:	Delegations
No. Cion doc.:	5358/17 TELECOM 12 COMPET 32 MI 45 DATAPROTECT 4 CONSOM 19 JAI 40 DIGIT 10 FREMP 3 CYBER 10 IA 12 CODEC 52
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Discussion on possible compromise solutions

INTRODUCTION

Throughout the month of January, the Presidency organised several WP TELE meetings with a view to analyse in depth some of the outstanding issues for the ePrivacy proposal (ePR), namely the impact of ePR on new technologies and the consent requirements, processing of electronic communications data for the purposes of child protection and the exclusion of national security and defence from the scope of ePR.

Based on the discussions in the WP TELE and on the written comments sent by delegations, the Presidency is presenting below possible compromise solutions for the above mentioned issues. The compromise solutions will be discussed at the attaché meeting of the WP TELE of 7 February.

PROPOSED MODIFICATIONS

1/ ePR and new technologies

Delegations expressed concerns about the way ePR proposal will interact with new technologies, in particular in the context of Machine-to-Machine, Internet of Things or Artificial Intelligence. The concerns seemed to relate mainly to situations of multiple end-users and to the question of consent. The Presidency is therefore proposing to address those issues in recital 13, 20a and 21 as follows:

"(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, regardless if these networks are secured with passwords or not, the confidentiality of the communications transmitted through such networks should be protected. The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited pre-defined group of end-users, e.g. to members of the corporation, courts, court administrations, financial, social and employment administrations. Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation. **This Regulation also does not apply to electronic communications data circulating within a home WIFI network. However, as soon as these data exit such a network and enter a publicly available electronic communications network, this Regulation applies to such data, including M2M/IoT and personal/home assistant data. The provisions of this Regulation regarding the protection of end-users' terminal equipment information also apply in this case to terminal equipment connected to the home WIFI network".**

"(20a) End-users are increasingly requested to provide consent to the storage and access to stored data in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users are overloaded with requests to provide consent, leading to what has been referred to as 'consent-fatigue'. Implementation of technical means in electronic communications software to provide consent through transparent and user-friendly settings, can be useful to address this problem. An end user may therefore grant consent to a specific provider for the use of processing and storage capabilities of his or her terminal equipment for one or multiple specific purposes across one or more services of that provider. Such consent can be given to several providers. For example, an end-user can give consent to the use of all or certain types of cookies by whitelisting one or several providers. To that end, providers should ensure that end users can easily set up and amend such white lists and withdraw consent in a user-friendly and transparent manner.

(21) Use of the processing and storage capabilities of terminal equipment or access to information stored in terminal equipment without the consent of the end-user should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is necessary and proportionate for the legitimate purpose of enabling the use of a specific information society service requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket.

Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of the information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.

Conversely, to the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the information society service requested, consent should be required. Where the terminal equipment is provided to the end-user by the provider of the information society service, consent should normally be given by the end-user who requests the service. Where that end-user enables the use of the terminal equipment by other end-users, such as employees, it should respect the rights of those other end-users in accordance with Regulation (EU) 2016/679, employment and other applicable laws.

In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use."

2/ Child protection

Throughout the discussions on the proposal, both at the WP and at the Council level, there was a clear support to include an explicit permission to process data for the purposes of detecting and deleting material constituting child pronography. The Presidency is therefore proposing to include an additional ground for processing electronic communications data in **new point (d) of Article 6(1) and to insert a new Article 6(1a)** as follows:

(d) **it is necessary to enable the detection and deletion of material constituting child pornography, as defined in Article 2(c) of the Directive 2011/93/EU**.

New Article 6(1a): **Processing for the detection and deletion of material constituting child pornography, in accordance with paragraph 1(d), shall not analyze the actual communications content and shall not store any copies of that content. Processing shall be subject to appropriate safeguards, be limited to the sole purpose of detecting child pornography, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the end user, including carrying out of an impact assessment in accordance with Article 35 of Regulation (EU) 2016/679 and a consultation of the supervisory authority.**

3/ National security and defence

A number of delegations expressed doubts about the wording of **points (a) and (aa) article 2(2)** on the exclusion from the scope of national security and defence, which seemed to have created some interpretation issues. The Presidency is therefore proposing to merge the two points as follows:

(a) activities which fall outside the scope of Union law**, such as activities concerning national security and defence**;

~~**(aa) activities concerning national security and defence**~~;