VERBAND DER INTERNETWIRTSCHAFT E.V.

Comments

on the Amendments to the ePrivacy Regulation

Berlin/Brussels, 9 October 2017

The European Parliament committees are currently deliberating on the proposal for the ePrivacy Regulation[1]. The Parliament's decision and the introduction of the trilogue procedure is planned for end of October of this year.

As an addendum to the detailed commentary on the Commission's draft,[2] eco would like to avail of the opportunity afforded by the current committee debates to once again highlight a number of the regulation's key aspects and the related amendments.

I. Central Challenges:

Over the course of the deliberations, a more detailed examination of the following general aspects is advised:

- **Precise delineation of the scope of the regulation**

The scope of the ePrivacy Regulation should be rigorously defined, both in geographic and substantive terms. The Commission's proposal already contained a number of ambiguities concerning which services and software products are actually affected (e.g. in Articles 2 and 10) – and this has far-reaching consequences for their design and security. Therefore, the scope of the ePrivacy Regulation's application should be critically examined in order to ensure coherence with other European legal acts such as the EU General Data Protection Regulation (hereafter GDPR) and the European Electronic Communications Code (hereafter EECC).

- **Continued assurance of quality of services**

In part, the Commission's proposal already contained prohibitive regulations for the processing of communication and metadata. Provision was thus not made for the processing and storage of communication content. Furthermore, the reduction in the processing and storage of data, if these are anonymized, is already much tighter and more stringently stipulated than in the

[1] Draft of the European Commission concerning the proposal for a Regulation of the European Parliament and Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM (2017) 10 final)

[2] You will find the detailed commentary here: https://www.eco.de/wp-content/blogs.dir/20170228_eco_pos_eprivacyreg.pdf

GDPR, for example. A modern digital economy with high-quality digital services requires an appropriate legal framework. The debate on the amendments should reflect this.

II. Comments on the Individual Amendments

- **Affected persons and organizations (Article 1)**

The Commission's ePrivacy Regulation proposal envisages that natural and legal persons be equally affected. The expansion of the application area raises concerns and will be difficult to implement. As such, eco advocates a regulation that either pertains to specific natural persons or that adopts a different approach to guaranteeing the security and confidentiality of electronic communications.

In light of the above, eco takes a positive stance to the amendments as tabled by the IMCO Committee, numbered 181,182 and 188 in relation to Article 1 of the regulation. eco considers the greater harmonization of the protection of personal data – which would also be more in line with the GDPR – to be important. In this context, Amendment No. 119 from the ITRE Committee is also helpful, as are Amendments No.186 and No.187 from the IMCO Committee.

- **Legal framework between the ePrivacy Regulation and EECC – affected services (Articles 2-4)**

The scope of the ePrivacy Regulation also needs to take the development of other regulations – such as the EECC and, where relevant, the BEREC regulation – into account. In order to have a stringent and clearly defined regulatory framework, it is therefore important to ensure the greatest possible coherence between the various legal acts. The Commission's proposal has left the issue unclear, and has also ultimately created ambiguity about the services and platforms involved.

Amendment No. 121, tabled by the ITRE Committee, clarifies Article 2, a clarification which is welcomed by eco. Likewise, eco welcomes Amendment No. 131 on Article 4, which eliminates the ambiguities in Article 4 regarding the services and platforms at issue.

Conversely, provisions which would extend the substantive scope of the ePrivacy Regulation even further should be dispensed with. Amendments such as No. 201 from the IMCO Committee remove the condition that electronic communications services must be publicly available in order to be brought into the scope of the ePrivacy Regulation. eco opposes this proposal. eco takes an equally critical view of the proposal that current provisions should be extended to hard and software capable of retrieving or displaying data from the Internet, as called for by Amendment 199 of the IMCO Committee. For similar reasons, eco recommends a rejection of Amendments Nos. 221, 222, and 223 of the IMCO Committee. Amendments Nos.

234 to 239 introduce new definitions, thus increasing the fragmentation of the regulatory framework. Accordingly, these should be rejected. On the other hand, limiting the scope of the ePrivacy Regulation to the transfer of data appears sensible, since this is often no longer the responsibility or the remit of a service provider. From this perspective, Amendments Nos. 225 and 226 are deemed to be constructive.

- **Ensure the confidentiality of communication (Article 5)**

The confidentiality of electronic communications is very extensively conceived in the proposed regulation. Notably, this extends far beyond securing communications.

What is particularly problematic here is the attempt to extend the regulation even further, such as is the case in Amendments Nos. 246 and 248 proposed by the IMCO Committee, Nos. 149,151 and 153 by the ITRE Committee, or Amendment No. 399 by the LIBE Committee. The very expediency of such a regulation is open to debate. An over-extension of the regulatory framework of the ePrivacy Regulation and intervention in areas which go far beyond the protection of the confidentiality of electronic communications should therefore be eschewed.

Amendments Nos. 397 or 398 by the LIBE Committee, or Nos. 244 and 250 by the IMCO Committee (identical in places and submitted by the same applicant) point out how such a specification could be achieved.

- **Examine exemptions for legal data processing (Article 6)**

In the processing of electronic communications data, the Commission's proposal currently allows for very few exceptions. The many types of problem which could be generated from this situation include dealing with spam filters in email boxes, the processing of such data, or problems with openly designed communication services. In this context, the wording of Article 6 should be brought more in line with the GDPR.

Against this backdrop, the further restriction of the transfer of data to a "technically strictly necessary level" or for accounting purposes, as suggested by several amendments (e.g. IMCO 259, 260, 263, 264, 276, 277, 279, 280, LIBE 421, 422, 423, 426, 427, 428, 429, 447), is viewed negatively.

It would be more expedient to remove the problematic provisions in Article 6, as suggested in Amendments Nos. 157,160,167 of the ITRE Committee or 418, 419, 425, 447 of the LIBE Committee.

An alternative practicable method would be an appropriate augmentation of the existing provisions. Amendments 420, 424, 441, 443, 444, 454, 458, 471, 472, 474, 475, 476, 478, 479, 480, 484, 488, 490, 491, 496, and 497 of the LIBE Committee, and 262, 269, 275, 281 and 286 of the IMCO Committee, suggest interesting approaches aimed at achieving a high level of data protection under the GDPR, in particular with regard to consent stipulations and the design of open and interoperable communication services.

- **Develop appropriate means of storing data (Article 7)**

The storage of communication and, in particular, metadata has already proved problematic in the Commission's proposal. For example, it is doubtful that the proposed form of storage of metadata for quality assurance of services would actually be possible. Accordingly, deletions such as those worked with in Article 6 could be used to achieve greater coherence with the GDPR. Amendments Nos. 498 and 507 of the LIBE Committee represent a possible approach to this. Appropriate adjustments could also be a viable alternative to resolving the existing problems. Amendments Nos. 510 and 503 in particular present useful approaches here.

- **The digital industry must be able to work in a specialized way (Article 8)**

Measures for dealing with end devices, and the possibilities available for services to communicate with these devices, are central to the Internet industry. It is therefore unsurprising that many observers are concerned that the Commission's ePrivacy Regulation proposal imposes excessive restrictions on this system, on the basis of overly strict rules. As such, the fact that many amendments seek to make these provisions even stricter raises concerns.

For example, in the IMCO Committee, this applies to Amendments Nos. 321 and 322, 359, 360, 362, 367, 369, 372, and 376 and – when it comes to limiting measures to those that are technically strictly necessary – Amendments Nos. 317, 318, 325, and 326. From the ITRE Committee, Amendments Nos. 203, 204, 207, 208, 220, 242, 243 – and, in relation to the strict (technical) necessity Nos. 205, 206, and 212 – are equally problematic.

In the leading LIBE Committee, this pertains to Amendments 515, 517, 523, 539, 540, 554, 555, 575, 580, and 583, and for the strict (technical) necessity 521, 522, 524, 535, and 553 (some of the amendments derive in part from the same authors and/or are identical in text).

What would make more sense is to give due consideration to the circumstances of a collaborative digital industry which requires different labor streams, and to the measures for contracted data processing with specialized providers, such as made possible by the GDPR. A recognition of service quality and integrity as a possible motivation for processing data is also evident in these amendments and is particularly reflected in Amendments Nos. 528, 529, 531, 532, 534, 538, 543, 544, 546, 549, 550, 551, 564, 565, 566, 570, 571, 573, 582, 589, 590, 594, and 595 of the LIBE Committee; in Amendments 320, 329, 330, 352, and 356 of the IMCO Committee; and in Amendments 215, 216, 217, 218, 227, 228, and 229 of the ITRE Committee.

In this context, the extent to which the implementation of the ePrivacy Regulation actually requires its own implementing acts also needs to be examined. The GDPR already provides for these and the first of these acts have already been enacted. Here, the information society and telemedia services

are explicitly alluded to. In this light, Amendments Nos. 605, 606, and 607, tabled by the LIBE Committee, should be examined in more detail. From the IMCO Committee, the corresponding motions are Amendments Nos. 380, 381, 382, and 523 (in relation to Article 25).

- **Develop coherent consent rules (Article 9)**

The GDPR sets the standards for consent. The EU Commission has modified these in the scope of its proposal for the ePrivacy Regulation. This is intended to meet the specific requirements of the digital world. Nevertheless, the proposal contains problematic and bureaucratic constraints which could produce “consent fatigue” among users.

In seeking operational consistency with the GDPR, consideration should be given to whether Amendments Nos. 609, 617, 618, 619, 626, and 627 of the LIBE Committee, or Amendments Nos. 397 and 401 of the IMCO Committee, or 254, 257, 258, 260 and 261 of the ITRE Committee, would represent useful additions. On the other hand, provisions for the use of services which are considered unconstructive include Amendments Nos. 392, 402, and 403 of the IMCO Committee, Amendments Nos. 633 or 634 of the LIBE Committee, and Amendment No. 259 of the ITRE Committee.

- **The provisions on privacy by design should not be extended through further specifications (Article 10)**

The provisions for "information to be provided" go too far. They do not just cover Internet browsers – as is often asserted – but also any software used. Arising both from this and from the overly broad definitions, software updates and online functions of software cannot be optimally used. eco therefore calls for the removal of this provision.

This is envisaged in Amendments Nos. 268 and 269 of the ITRE Committee, Amendments Nos. 635, 636, and 637 of the LIBE Committee; and Amendments Nos. 405, 406, 407 and 408 of the IMCO Committee.

On the other hand, provisions that extend the requirements for privacy by design beyond the specified level of protection should not be pursued further. Amendments Nos. 639, 640, 645, 646, 647, 648, 649, 650, and 659 of the LIBE Committee, or 273, 275, and 276 of the ITRE Committee, or 413, 414, 419, and 427 of the IMCO Committee are not helpful, as they go beyond the scope of the regulation of software manufacturers.

Nonetheless, if provisions to this effect are adopted in this Article, consideration should be given in each case to an extension of the implementation framework, as suggested by Amendments Nos. 666 of the LIBE Committee or 288 of the ITRE Committee.

- **Security provisions must not make anonymous and pseudonymous communication impossible (Article 11)**

The restrictions on the collection of data under Articles 5 to 8 is intended to be regulated in Article 11. The Commission's proposal refers to "internal procedures" which are to be developed in order, for example, to deal with requests from investigating authorities. This is viewed critically, as it could conceal an obligation to read encrypted communication or the release of contact data after prior identification of a user. eco is opposed to such obligations.

A removal of the Article is therefore appropriate, as envisaged by Amendments Nos. 669 and 679 of the LIBE Committee or 433 of the IMCO Committee.

Alternatively, amendments could also be used to clarify the situation, such as for example Amendment No. 674 of the LIBE Committee or Amendment No. 433 of the IMCO Committee.

- **Set a realistic timeframe for the ePrivacy Regulation**

It is already clear that the timeframe for the ePrivacy Regulation will not be tenable. Its entry into force on May 25, 2018, concurrent to the GDPR, would pose enormous challenges, not only for companies and service providers, but also for software developers. Amendments to this effect have already been discussed in the LIBE Committee.

eco recommends that an arrangement be found which allows for a flexible management of the regulation’s inception and for an appropriate implementation period, such as that prescribed in Amendment No. 825 from the LIBE Committee.

About eco

eco – Association of the Internet Industry represents the interests and supports all industries involved in generating economic value creation through the Internet. The association represents more than 1000 member companies.

Amongst others, these include ISPs (Internet Service Providers), carriers, suppliers of hard and software, content and service providers, and communications companies. This makes eco the largest association of Internet service providers in Europe.