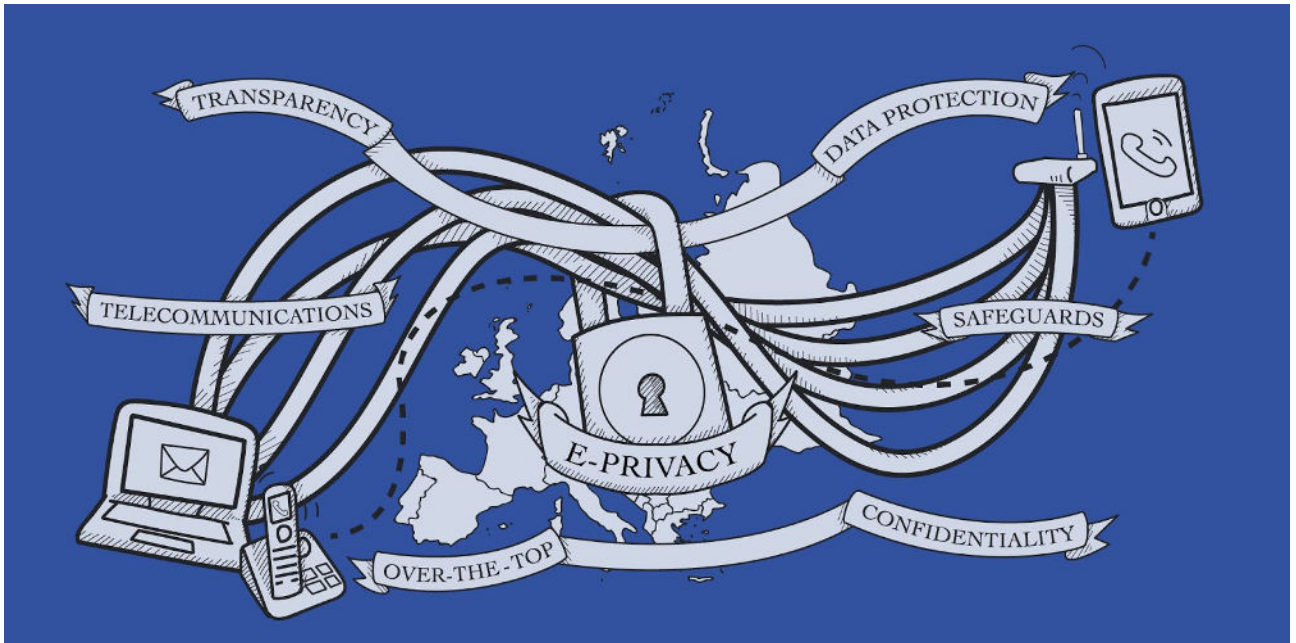


Access Now analysis of the proposed ePrivacy Regulation, LIBE report & amendments



Access Now welcomes the Commission’s proposal for the ePrivacy Regulation (hereinafter “Commission’s proposal or proposed Regulation”) which aims to upgrade the rules on the right to privacy and the confidentiality of communications to today’s digital era. We have taken an active role in the review of this important legal instrument, by providing comments to the EU Commission [consultation](#) of Spring 2016 and [policy recommendations](#) in December 2016. We have analysed also the Commission’s proposal and [proposed amendments](#) to improve the future Regulation.

Access Now welcomes the draft LIBE report (hereinafter “draft report”) prepared by Rapporteur Marju Lauristin which strengthens protection for users’ rights. We have analysed below 827 tabled amendments to the proposed Regulation, including the draft report. Having in mind a scenario where users would be put in control of their information, their rights would be effectively protected and trust in businesses would be ensured, we have produced a list of best and worst proposals below.

For More Information, Please Contact

Fanny Hidvégi | European Policy Manager | fanny@accessnow.org
Estelle Massé | Senior Policy Analyst | estelle@accessnow.org

Specific objectives of the proposed Regulation

1. Alignment with the GDPR

Aligning the e-Privacy reform with the GDPR will be crucial in order to avoid a conflict of laws, uncertainty for users' rights, and undue administrative burden for industry. Currently, the Commission's proposal, the draft report and proposed amendments make inconsistent references to the GDPR. For instance, when "consent" is mentioned, the proposed Regulation sometimes refers to the rules agreed under the GDPR and sometimes it does not. We understand that the rule on "consent" should always follow the measures agreed under the GDPR. We welcome the decision of the LIBE committee to seek guidance from the EU Parliament legal service on that matter in order to know how should the GDPR be referenced in the ePrivacy Regulation.

2. No legitimate interest

Access Now strongly opposes the introduction of "legitimate interest" (Article 6.1(f) of GDPR) and "further processing" (Article 6.4 of the GDPR) as legal basis for processing under the proposed Regulation.

It is imperative to ensure control over access to and processing of the extremely personal and sensitive information of our daily communications that take place over the phone, messaging apps, or the web. Explicit consent will give users the appropriate level of control of their information, as well as predictability. Both the metadata and the content of these communications can reveal highly sensitive information about users, and this information must therefore be protected with the highest legal standard for processing, as reaffirmed by the CJEU jurisprudence on data retention.

We **support the following amendments**, which strengthen users' control: **AMS 191, 192 and 193**.

We **strongly oppose the following amendments**, which by introducing either legitimate interest or further processing as legal basis for processing communications data, put users' rights at risk: **AMS 205, 206, 212, 232, 236, 441, 443, 475, 476, 478, 479, 480, 481, 526, 568, 569, 207, 208, 213, 472, 473, 474 and 565**.

3. Protection against tracking

Current rules within the e-Privacy Directive fail to distinguish between different types of online tracking, and enforcement has largely focused on the use of cookies. Tracking goes far beyond cookies and can happen across websites, applications, and even devices. These shortcomings should be addressed in the future Regulation, and the review process must create technologically neutral obligations and safeguards around the use of tracking tools and techniques in general, rather than targeting a specific technology.

We **support the following amendments**, which protect users against tracking: **AMS 22, 23, 250, 252 and 253**.

4. Strengthening the rules on privacy by design and by default

Access Now welcomes the improvement proposed by the Rapporteur to increase the clarity and efficiency of the rules on privacy by design and by default. We however recommend to extend those to hardware as well, and to not limit their application to software.

We therefore **support the following amendments 252, 638, 639, 640, 655, 657, 680 and 681**.

5. Limiting the scope of exceptions to what is necessary and proportionate

Access Now welcomes the Rapporteur's and shadows' approach to clarify the exceptions under Article 11 to the protections laid down in the proposed Regulation. Many amendments reflect the jurisprudence established by the CJEU, in particular when indicating that exceptions should be based on suspicion and under strict judicial oversight.

We **support the following amendments 27, 102, 103**, as well as identical amendments tabled by Shadows.

6. Include provision on mandatory transparency reporting

Transparency reporting is a pathway for technology companies and telecoms to disclose threats to users' privacy and freedom of expression. Such reports educate the public about enforcement of company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, internet shutdowns, content restrictions, and a host of other practices that impact users' fundamental rights. Consequently, publishing transparency reports in a harmonised manner following a specific set of criteria will increase user trust in online services and products and the internet in general. This will contribute to the digital economy and the full enjoyment of the Digital Single Market.

Access Now **supports the following amendments 675, 682, 683, 802 and 803**.

7. Ensure NGO representation

To improve users' access to remedy, the e-Privacy Regulation should clearly authorise consumers and non-for-profit organisations to represent a user or a group of users in claims in front of supervisory authorities and courts. NGOs should also be authorised to bring complaint on their own. To ensure meaningful access to remedy, the legislation should also make clear that participation in administrative enforcement mechanisms do not preclude or prevent users from seeking judicial remedy.

We **support AMS 796** and **strongly welcome AMS 125 and 795**.

8. Ensure robust enforcement

The future e-Privacy Regulation should apply the “cooperation and consistency” enforcement mechanism agreed upon under the GDPR. In particular, DPAs and the European Data Protection Board (EDPB) should be able to provide guidance and recommendations on how to effectively implement the ePrivacy Regulation.

We **welcome amendments 38 39, 788, 789 and 790.**

Additional comments

Beyond the specific objectives highlighted above, Access Now would like to comment on the following amendments:

1. Access Now supports:

Amendments **seeking to include definitions of key concepts within the proposed ePrivacy Regulation**, instead of referencing the Electronic Communications Code.

AMS 2: which aims to ensure that both content and metadata is protected under the proposed Regulation. The amendment also clarifies that this Regulation does not only protect the right to privacy and confidentiality of communications but also positively impacts free expression and freedom of thought, conscience and religion.

AMS 6: which aims at reducing avenues for member states to limit protection under this Regulation and ensure harmonisation across the Digital Single Market.

AMS 12: which further clarifies what metadata is.

AMS 13: which is a positive clarification of scope of exceptions and would provide legal certainty for user rights.

To ensure that all data processed by the terminal equipment are covered and protected under the proposed Regulation, we support the addition of the words “processed by” suggested by the Rapporteur and several Shadows in particular in **amendments 7, 41, 42, 391, 392 and 393.**

AMS 61, 62, 63, 64, 65 and 66: are important to clarify the scope of the legal basis for processing communications data under the proposed Regulation. We also support similar amendments tabled by MEPs Albrecht, In't Veld, Macovei and Ernst.

AMS 83: which aims at clarifying that refusal of consent cannot lead to denial of access or of basic functionality of a product or service. The contrary would negate the definition of consent as agreed under the GDPR. We also **support amendments 563, 575 and 633** which have the same objective.

AMS 116, 276, 674, 776, 777 and 778: which aim to protect privacy and security tools such as encryption and prevent unauthorised access to users' communications data.

AMS 161: which aims at modifying recital 7 to allow the EDPB to issue guidance for a harmonised application of the Regulation. Alternatively, Access Now would support the deletion of recital 7 altogether as suggested by the Rapporteur and several shadows.

AMS 174: which aims at clarifying the scope of application of the proposed Regulation to all messaging functions, including newsfeeds and more.

AMS 224, 437, 438 and 493: which aim at ensuring the functionality of accessibility tools.

AMS 343: which aims at extending the application of the proposed Regulation to EU institutions.

AMS 345: which aims at clarifying the territorial scope of the Regulation.

AMS 396: which aims at ensuring that protection for the confidentiality of communications apply to both content and metadata. We support this amendment jointly with **AMS 399 and 400** which would provide for strengthened users' privacy and better define the purpose of the proposed Regulation.

AMS 486 and 485: which provide for a clearer framework for the processing of the content of communications.

AMS 515, 516, 535, 553 and 554: which significantly strengthen the protection against offline tracking and would provide for efficient safeguard for users' rights.

2. Access Now opposes:

AMS 15: which proposes measures that do not fall within the scope of this proposal. Indeed, the issue of quality of service is covered under the Regulation 2016/2120. Furthermore, the current wording of the amendment would undermine rules on the principles of net neutrality safeguarded under Regulation 2016/2120.

AMS 141 and 142: which suggest deletion of Recital 3 which clarifies that consent must be understood as agreed under GDPR.

AMS 151: which negates the nature of the ePrivacy as an instrument that particularises the GDPR. We oppose amendments 329, 330 and 331 for the same reason.

AMS 172 and 173: which remove ancillary communications from the scope of the Regulation and would therefore create loopholes in the protection of confidentiality of communications.

AMS 176 and 179: which would exclude the Internet of Things and machine to machine communications from the scope of the proposed Regulation. This would hinder trust in the IoT industry and put user's privacy and confidentiality of communications at risk.

AMS 395 and 402: which aim at limiting scope of protection of confidentiality of communications only to the content of communications, leaving all metadata unprotected.

AMS 433: This amendment is unclear and refers to the undefined concept of “abusive” use of a service.

AMS 447: The justification provided for this amendment is incorrect. The court [has recognised](#) the sensitivity of metadata. In that sense, they require specific protection under the Regulation.

Ams 467, 468 and 469: which would disproportionately broaden the scope of processing authorised under this Regulation.

AMS 497: which conflates processing of content and phone data usage. The amendment is extremely unclear and would severely interfere with user's' right to privacy.

AMS 498: which seeks the deletion of Article 7 and therefore limits the scope of protection provided for in this Regulation.

AMS 532, 533, 534, 538, 558 and 559 which seek to disproportionately extend the use of data and capabilities from terminal equipment, in particular related to user experience and terms of use. The measures proposed under this amendment could lead to discrimination on the network and conflict with Regulation 2016/2120. Furthermore, the suggested exception for research and marketing purposes are far too broad and open to abuse. We also **oppose amendments 566 and 567** which seek to rely on an opt-out mechanism for user to express their choice. This is unacceptable and does not provide for adequate control for users.

AMS 576 and 609: which negate the definition of consent by linking it with the access and functionality of products or services.

AMS 626: which negates the right to withdraw consent.

AMS 635, 636 and 637: which suggest deleting Article 10 paragraph 1 and would therefore diminish trust in services and products. The proposed amendment would also reduce the proposed safeguards for users' right to privacy.

AMS 673: which would extend the scope of Article 11 and would therefore increase legal uncertainty for users' rights.

AMS 765 and 766: which seek the deletion of Article 17.1 which provides for safeguard ensuring security and privacy of products and services.

AMS 814: which seeks to remove penalties in case of violation of rules laid out in the proposed Regulation. This amendment misinterprets the relationship between the proposed ePrivacy and the GDPR.