Brussels, May 2019

Comments to the WP TELE on interinstitutional file 2017/0003 (COB) - Reform of the ePrivacy legislation

INTRODUCTION

To support the work of the WP TELE under the ongoing Romanian Presidency and upcoming Finnish Presidency regarding the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation), Access Now would like to share comments and proposals on a series of concrete issues with the delegations.

Access Now strongly supports the much-needed efforts to reform the EU's ePrivacy legislation and would have welcome the conclusion of a general approach under the Romanian Presidency. The reform is essential to strengthen individuals' right to privacy and confidentiality of communications across the EU as well as rebuilding and reinforcing public trust and security in the digital economy. While we are pleased to see some progress in the advancement of discussions, we have serious concerns with some of the proposals discussed in the WP TELE since February which, in our opinion, contradict the objective of the reform.

Our proposals below have been organised into four categories which focus on a number of issues discussed by WP TELE. We are available for any questions you may have on these proposals and we would be happy to provide suggestions on other aspects of the text.

For ease of reference, any changes introduced by this document on the basis of the Presidency texts of 22 February, 13 March, and proposals from 8 delegations on data retention from 14 February, are underlined. This last document was obtained by Access Now through a request to access document sent to the Council of the EU.

1. The ePrivacy Regulation should be future-proof and technologically neutral

Recital 13 of the Presidency text of 22 February suggests to take out, at least partially, home fixed or wireless networks from the scope of the Regulation. Affirmative obligations to protect the confidentiality of communications and the integrity of devices connected to home networks, including to router and smart home assistants, are of paramount of importance in the era of the Internet of Things. While the development of IoTs is still at its infancy the number of privacy abuses already reported is alarming for users and certain products had to be taken off the market. Security

and privacy are an essential prerequisite for the long term success and sustainability of connected products which is why we suggest amending recital 13 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 of whether these networks are secured with passwords, 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 publicly available electronic communications data using publicly available electronic communications services and public electronic communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as **~~home (WIFI or fixed or wireless) networks or~~** corporate networks, access to which is limited **~~pre-defined group of end-users, e.g. to family members,~~** members of a corporation, courts, court administrations, financial, social and employment administrations. This Regulation also **~~does not applyies~~** to electronic communications data circulating within a home WIFI network**~~. As soon as these electronic communications data exit such a closed group network and enter a publicly available electronic communications network, this Regulation applies to such data,~~** including when it is 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 of terminal equipment connected to the **~~a closed group network such as a~~** home (WIFI or fixed or wireless) network**~~ which in turn is connected to public electronic communications network~~**.

Recital 15a of the Presidency text of 22 February indicates that the prohibition of scope of Article 5 on the confidentiality of communications and prohibition of interception should only apply until reception of content of communication. Limiting the scope of “transmission” and the protection to the communications data only in transit, and not after reception, is both contrary to users’ expectations and technically complex to implement. The confidentiality and protection of a message should remain the same whether or not the user has received or opened said message. We recommend amending recital 15a as follow:

> (15a) The prohibition of interception of electronic communications data content under this Regulation should apply **~~until~~** during **transit and after reception** of the content of the electronic communication by the intended addressee**~~, i.e. during the end-to-end exchange of electronic communications content between end-users~~**. Receipt implies that the end-user gains control over, and has the possibility to interact with, the individual electronic communications content, for example by recording, storing, printing or otherwise processing such data. The exact moment of the receipt of electronic communications content may depend on the type of electronic communications service that is provided. For instance, depending on the technology used, a voice call may be completed as soon as either of the end-users ends the call. For electronic mail or instant messaging, depending

on the technology used, the moment of receipt is may be completed as soon as the addressee has collected the message, typically from the server of the electronic communications service provider. Upon receipt, electronic communications content and related metadata should be erased or made anonymous by the provider of the electronic communications service except when processing is permitted under this Regulation ~~**or when the end-users has entrusted the provider of the electronic communications service or another third party to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679**~~.

Recitals 20, 20a, 21, 21a of the Presidency texts of 22 February and 13 March refer to "cookies" "cookies and similar tracking technologies" and "cookie or similar identifier". The objective of the Regulation is to establish rules on tracking which indeed can de done via the use of "cookies and similar technologies" however the emphasis on this specific type of technology and the use of the qualifier "similar" is not future-proof and does not provide legal certainty as new types of trackers may develop in the future and these may not be "similar" to cookies. We recommend instead using the following terminology everywhere in the text where a reference to "cookies" or tracking is made **"tracking technologies and/or identifier"**.

2. The ePrivacy Regulation should encourage privacy-friendly innovation

Article 10 of the proposed ePrivacy Regulation has been deleted in the Council text since several months. The principles of privacy by design and by default are central to the protection of privacy and confidentiality of communications ensures that hardwares, and not only softwares, placed on the market will come with heightened protection to the benefit of users and security of the networks. By enshrining these principles, the EU can drive privacy-friendly innovation in the Digital Single Market. These principles contributes to products and services security and can therefore bring trust in the market, as well as benefiting users' rights. We recommend re-introducing article 10 as follow:

Article 10
Privacy by design and by default

1. The settings of all hardware and the components of the terminal equipment shall be configured to, by default, prevent third parties from storing information, processing information already stored in the terminal equipment and preventing the use of the equipment's processing capabilities by third parties.

2. Software and operating systems permitting electronic communications, including the retrieval and presentation of information on the internet, shall be configured by default to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment, and prevent the use of others trackers.

3. Upon installation, the software and operating systems shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.

3. In the case of software which has already been installed on (date of entry into

application of the Regulation), the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than (6 months after entry into application).

3. The ePrivacy Regulation is not a law enforcement instrument

In the Digital Rights Ireland and Tele2 rulings, the Court of Justice of the European Union (CJEU) clarified the authorised scope of data retention mandates and indicated that that mandatory mass retention of communications data is in violation of Articles 7 and 8 of the EU Charter of Fundamental Rights, in particular as such indiscriminate measure fails to meet the criteria of necessity and proportionality.

We are aware of the political difficulties raised in Council around the issue of data retention and acknowledge the challenges raised by a number of delegations indicating in their 14 February note that "after two years of work in the DAPIX Working Party, no solution has yet been found on how to implement a targeted/restricted retention" despite the guidance provided by the CJEU. Nevertheless, the proposals put forward by both the Presidency and the delegations related to Article 2 (2) (a), Article 6 (2a) and Article 11 does not bring legal certainty as it would seek to both exclude activities related to national security and defence from the scope of the law, while also suggesting exception to allow member states to develop data retention mandates for these purposes. Finally, the proposed fails to reflect the jurisprudence of the Court which cannot be ignored as it partly derives from the interpretation of the rights protected under the EU Charter. We therefore suggest the deletion of Article 2 (2) (a) and recommend the following language on Article 11.

Article 11
Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5to 8 where such a restriction is limited to suspects of serious crime, and respects the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure, including prior judicial authorisation or by an independent authority, in a democratic society to safeguard defence, public security, and the prevention,investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication systems. Any legislative measure referred to in this paragraph shall be in accordance with the Charter of Fundamental Rights of the European Union.

2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response. Providers of electronic communications services shall keep details about requests made pursuant to paragraph 1, which shall

be made available to the competent supervisory authority upon request. This shall include:

(a) the in-house staff member who handled the request;
(b) the identity of the official or body asking for the information;
(c) the purpose for which the information was sought;
(d) the date and time of the request;
(e) the legal basis and authority for therequest, including the identity and status or function of the official who authorised the making of the request and whether this was a judicial or prosecuting or state security official;
(f) the number of end-users to whose data the request related;
(g) the data provided to the requesting official or body;
(h) the period covered by the data.

3. All providers of electronic communicationsservices shall provide every year to the competent supervisory authority and to the public, a transparency report, providing the number of requests received pursuant to paragraph 1, from which authorities, the number of granted requests, and the numbers of end-users affected by the requests. Such transparency reporting shall also include information about privacy and data protection practices and policies, inform users about avenues for remedies in case of abuses and feature clear and easily understandable information about end-users rights protected under this Regulation.

4. Providers of electronic communications services shall be subject to enforcement actions by the competent authority including fines pursuant to this Regulation.

On a separate matter, **Article 6 (1a)** of the Presidency texts of February and March, as well as several discussion papers provide for an exception for the processing of communications data for the fight against child pornography. The fight against child pornography would indeed benefit from greater coordination at EU level and require the processing of personal information, including communication data. However, the language proposed in the Presidency texts of February 22 could actually limit the work of law enforcement authorities which may require to process such content, beyond the deletion of the material online, for prosecution and investigation.

Based on its legal basis, the ePrivacy Regulation is not an appropriate tool for the fight against child pornography, terrorist content, or any other crimes. Nothing in the current ePrivacy Directive and draft regulation would prevent that fight and as is, no specific language is required to ensure that this fight can continue. As a solution to satisfy political purposes, the legislator could perhaps state this fact into a recital.

4. The ePrivacy should ensure predictability in the use of communications data

To effectively protect users' rights to privacy and confidentiality and ensure predictability, the Regulation must established clear ground for processing communications data. Such processing should generally be limited to users' consent, as defined under the GDPR, and exceptions must be as narrowly defined as possible.

Recital 17aa, Article 6 (2a) and (2aa) of the Presidency text allows for the further processing of users' communications metadata under certain conditions. While we appreciate efforts to create safeguards around this processing, the sensitivity of users' communications data, including metadata, means that such further processing cannot be authorised. We therefore recommends the deletion of these proposed measures.

CONCLUSION

We thank the representatives of the WP TELE for the work done so far in the negotiations of the ePrivacy Regulation. We look forward to working with you for the swift conclusion of a general approach under the Finnish Presidency.

For more information, please contact:
Estelle Massé, Senior Policy Analyst and Data Protection Lead estelle@accessnow.org

About Access Now: We are an international organisation that defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age. We are a team of 50, with local staff in 12 locations across 6 continents.