Presentation by civil society groups (Access Now, EDRi, and Privacy International) to WP TELE Council attachés on the ePrivacy Regulation, 31 May 2018

Introduction

- **Badly regulated data protection drives monopolies** - to the detriment of innovation, competition, trust, security and uptake of new services. The weaknesses in current regulation of privacy and confidentiality is helping build monopolies. This makes sense: the bigger your existing database, the bigger the value of any new data set and vice versa.

- The **Google/Facebook duopoly is strangling publishers**. The duopoly has two thirds of revenue and close to 99% of market growth. What you have seen every day in the lobbying you have experienced is self-harm is a lobbying strategy.

- **Privacy and security worries are strangling new entrants while they are strangling fundamental rights**. the United States National Telecommunications and Information Administration of the US Department of Commerce spoke of privacy and security worries creating a "chill on discourse and economic activity" in 2016, following a major survey of consumer attitudes.

In essence:

1. The **balance** between ePrivacy and GDPR is the same as between ePrivacy and the 1995 Directive.
2. **Communications are particularly sensitive and particularly complex**, requiring an instrument that complements and particularises the general legislation.
3. It is important both for commercial and fundamental rights reasons, to have **clear and predictable rules** to engender trust, thereby enhancing competition, innovation and privacy.
4. The challenge we face is unfettered tracking of every intimate aspect of our connected lives. **Real consent means increased transparency and increased control of personal data.** Current industry practices that use behavioral economics to drive people to "click once for yes or 327 times for no (which is the "consent" option on the Tumblr blog service) offer neither transparency nor control. Sometimes clicking "OK" is the only option available. Such practices show that, without meaningful options for consent, individuals lose control and without control, the essence of data protection is lost. This is even more significant in relation to the sensitive data protected in the ePrivacy Regulation than in the GDPR.

Please find below some **specific comments and recommendations on Articles 5-11**:

Articles 5-6

- Regarding **Article 5**, **we support the proposal of the Presidency in the text from May 4 to revert back to referring to "interference"**.
- In accordance with the title of the Chapter, we recommend adding a provision clarifying that the **confidentiality of electronic communications shall also apply to data related to or processed by terminal equipment**.
- Today most communications services providers used for emails, instant messaging or online messaging undertake both transmission and storage. Messages are stored in a central server, in part because they are intended to be read from multiple devices so the service providers still can access and process the message even after it was received by the users. To address this issue, **we recommend changing recital 15a to indicate that communication data - not just content - should be protected as long as it is in the electronic communications network and/or accessible by the electronic communications provider**. In addition, the recital should refer to the prohibition of « interference » and not be limited to interception in order to be brought in line with Article 5.
- Finally, concerning the different grounds for processing foreseen under **Article 6** of the proposed Regulation, it is crucial to ensure the processing of communications data is generally limited to users' consent, as defined under the GDPR, and that exceptions are as narrowly defined as possible to prevent abuses and ensure predictability.
- We support **exceptions** the Presidency maintain or propose:
- 1. for the transmission of the communications **(Article 6 (1) (a)**),
  2. maintaining or restoring the security of the network and services (**Article 6 (2) (b)**), and
  3. for the provision of a service explicitly requested by an end users who has given consent when such request does not affect fundamental rights of another user, that the processing does not exceed the duration necessary for the **provision of the requested services and that it is limited to that purpose only (Article 6 (3) (aa)**).
- We are however concerned about the proposals around the use of metadata for statistical counting and scientific research in **6(2)(e) and (f)**, despite the safeguards proposed. There should be at least an additional safeguard ensuring that the retention period of such metadata is limited to 24 hours and that there is no sharing with third party.
- We are also unsure about the need of **Article 6 (2) (a) and (b)** which are overly broad and and **Article 6 (2) (d)** which covers a scenario already addressed in different EU legislation that remains applicable. We would recommend clarifying the first two points and moving point (d) to a recital to ensure that the legislation is future-proof.

Articles 7-8:

1- There is no justification to treat the confidentiality of metadata and content differently in Article 7.

- **Both of these categories of communications data are sensitive data needing sufficient protection**. Furthermore, the distinction between content and metadata is often not clear-cut, which also calls for similar protection and a similar regulatory regime.
- **New recital 17b** allowing processing of metadata for scientific research or statistical purposes needs to be narrowed so this does not become a blank cheque for future Cambridge Analyticas that will exploit metadata.
- **Risks about misuse of metadata are not abstract**: while the content of the messages sent via WhatsApp are encrypted, the metadata are commercially exploited by Facebook.

2- The text needs fine-tuning regarding measuring

- Although the text is generally good, we are **missing some clarity regarding what "audience measuring" refers to in Art. 8.1 (d)**.

- In order for the ePrivacy Regulation to protect privacy and confidentiality, **no communications data should be made accessible to third parties without a legal basis** and this data should not be unlawfully merged with data collected from other sources. From the text and recital is not clear what kind of third parties would need non-anonymised data of terminal equipment for some unspecified audience measuring.

3- Tracking walls are a threat to confidentiality and the opposite to informed consent

- **It is not justified to require users to agree to an unlimited "take it or leave it" amount of unnecessary processing of their personal data**. Websites, apps and smart devices are increasingly essential for individuals to be able to communicate and participate in our society.
- **We do not need cookie banners.** That is a deliberately bad implementation of the Directive, in fact it is so bad that is seems like it is done on purpose to undermine the legislation. The key issues with tracking walls is that if individuals are expecting to be subjected to surveillance when when reading their newspapers or watching a TV series offline, the same should apply online. To reduce the need for cookie banners, **the ePrivacy Regulation should promote technical standards for expressing user consent or objection** to tracking through signals (such as DNT), and make these signals legally binding on all parties.
- Regarding current texts being discussed, **we read recital 20 as specifically authorising tracking walls**, perhaps even to the extent of particularising GDPR Article 7(4) with a lower level of protection than the GDPR, contrary to the stated aim of the ePR.
- Furthermore, and still in **recital 20**: **the language is not entirely accurate and not technologically neutral** since it talks mostly about cookies although it mentions "or similar identifiers" in parts of the text.
- Some **good examples of how to deal with cookies** are NS.NL (where you are given a real choice to accept or not cookies), the website of USA today (where all tracking is disabled for EU readers) and the National Public Radio, in the USA, which offers a plain text version of the site, with no tracking, as an alternative to the tracked version (https://text.npr.org)

4- We welcome recent texts from the Council related to offline tracking: the latest version from the Council goes in the right direction by allowing the use of offline tracking for statistical counting only and not for any other more invasive uses. Exceptions would need careful consideration during the trilogue discussions.

<u>Articles 10-11</u>

Article 10

- Given the security vulnerabilities of many products connected to the internet, **privacy by design is necessary to prevent market failure in the area of the Internet of Things and connected devices**.
- The **settings** of all the components of terminal equipment placed on the market, including both software and hardware, should be configured **by design and by default to prevent third parties from storing information**, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment's processing capabilities.
- **As noted by the EDPS, the proposed privacy by option is contrary to Article 25 of the GDPR**. Adopting privacy by option rather than privacy by design and default will send a contradictory message to users and companies. It will inevitably lead to uncertainty and possibly litigation.

- We recommend that **Article 10** is amended to introduce obligations on providers of electronic communications services to offer default privacy protective settings to prevent other parties from storing information on the terminal equipment of a user and from processing information already stored on that equipment.
- The **Eurobarometer on ePrivacy** showed that almost **90% of EU citizens want such privacy-friendly default settings** (FlashEurobarometer 443 (December 2016). With the entry into force of GDPR it is clear that individuals now expect privacy to be the default settings.

Article 11

- The Court of Justice of the European Union (**CJEU**) clarified, in two different judgements (**Digital Rights Ireland** – joined cases 293/12 and 594/12 and **Tele2-Watson**, joined cases C-203/15 and C-698/15), that mandatory bulk retention of communications data breaches the EU Charter of Fundamental Rights, **because it amounts to a violation of the principles of strict necessity and proportionality**.
- Any attempt to subvert CJEU case law by adding "clarity to the legal context" without a legal basis that respects the Charter should be dismissed. Among these attempts is the idea by a number of delegations to introduce a minimum storage period (of 6 months) for all categories of data processed under **Article 6(2)(b)**. If approved, **this would impose indiscriminate retention of personal data in a way that has already been ruled as unlawful by the Court of Justice of the European Union** in Tele2/Watson.
- If **Article 6(2)(b)** establishes a legal basis for processing communications data in order to maintain or restore security of electronic communications networks and services, or to detect errors, attacks and abuse of these networks/services, the processing should still be limited to the duration necessary for this purpose.
- Further, the general principles of GDPR Article 5 should apply, e.g. storage limitation in **Article 5(1)(e)**. If the technical purpose can be achieved with anonymised data, this is no justification for processing data for identified or identifiable end-users.

Scope of the regulation and scope of the "restrictions"

- Seeking to remove from the scope of the e-privacy Regulation activities related to national security is an attempt to limit individuals' enjoyment of their rights. **We are therefore concerned by the attempt (in Article 2(2)(a)** - material scope of application and related Article 11) **to exclude from the scope of application of this proposal activities concerning national security and defence**.
- We are also concerned by the inclusion among the grounds for restrictions the very **broad and ill-defined ground of "important objectives of general public interests"** (see Article 23 (1)(d) of the GDPR).
- **We recommend to keep the grounds for restrictions in line with those mentioned in Article 15 of the current ePrivacy Directive**, namely safeguards of national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.