Proposal for a Regulation on Privacy and Electronic Communications

reinforcing trust and security in the Digital Single Market

Brussels, January 2017

#ePrivacy17

ePrivacy European Commission proposal

Agenda

- 10.00 **Introductory statement** *by Kuba Boratynski, DG CNECT*
- 10.15 **Session on confidentiality of communications**

  by Rosa Barcélo and Peter Eberl, DG CNECT
- 11.00 **Coffee break**
- 11.30 **Session on the enforcement and alignment of the ePrivacy proposal with the GDPR** *by Céline Deswarte, DG CNECT and Michele Voznick, DG JUST*
- 12.15 **Session on confidentiality of terminal equipment and unsolicited communications** *by Rosa Barcélo and Fenneke Buskermolen, DG CNECT*
- 12.50 **End**

#ePrivacy17

European Commission

ePrivacy
European Commission proposal

The Commission's proposal to modernise EU digital privacy rules

Ensuring stronger privacy in electronic communications, while opening up new business opportunities

1. Existing rules to apply also to internet-based voice & messaging services

2. Guaranteed privacy for both content & metadata on electronic communications

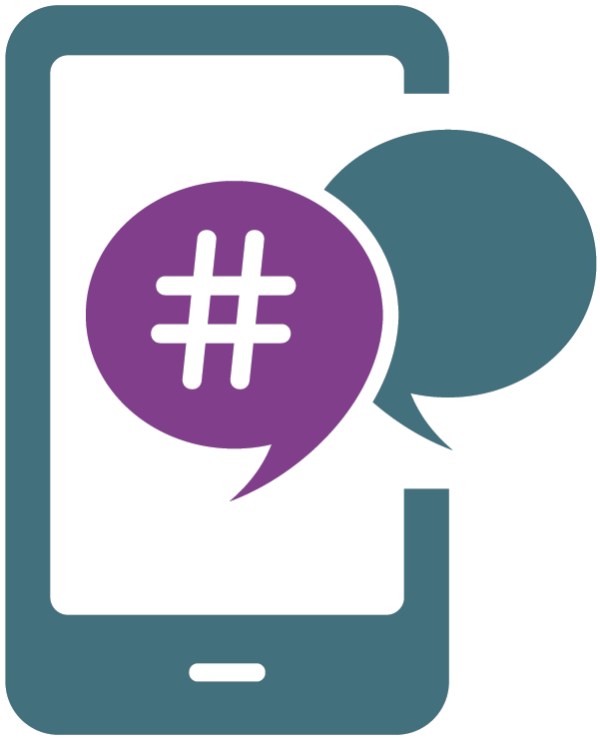
3. New business opportunities for traditional telecoms operators when processing communications data

4. Simpler rules on cookies

5. Protection against spam

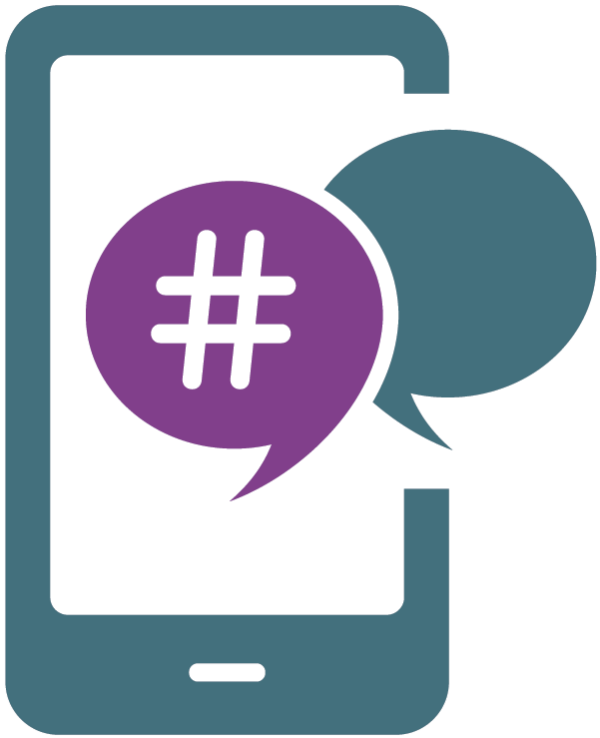
6. Stronger rules & more effective enforcement

1. Proposal for a Regulation applies to a variety of players



- Providers of **electronic communications services**;
- Providers of **publicly available directories**;
- **Software providers permitting electronic communications**;
- Natural and legal persons who use ECS to **send marketing material.**

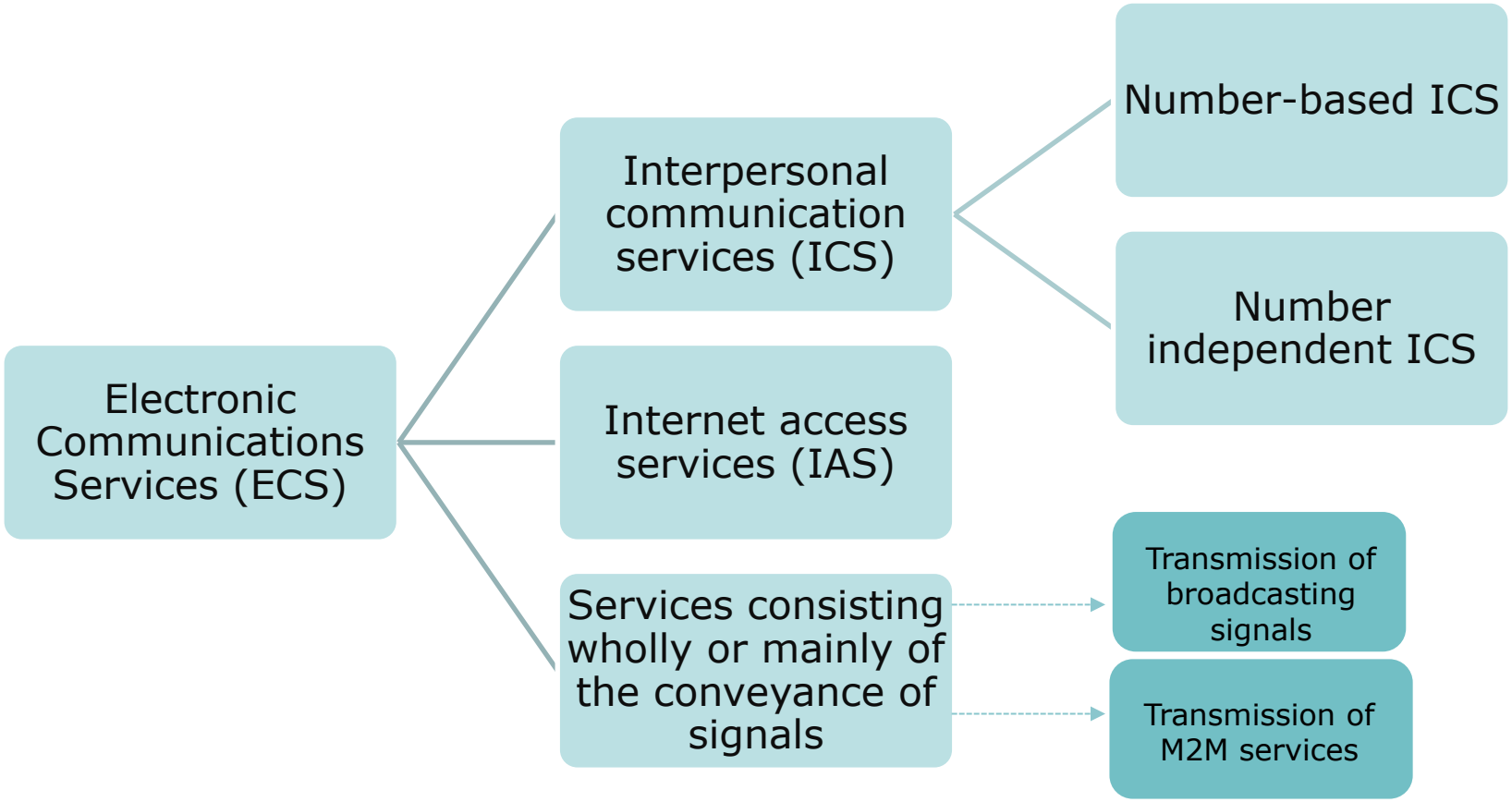
2. Electronic communications services



- **Privacy rules will apply to traditional telcos but also to new providers of electronic communications services:**
  - Such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, or Viber
- **Business and citizens will benefit from updated rules to reflect technological developments**
  - The confidentiality of consumers' communications will be protected across the EU, irrespective of the technology used

European Electronic Communications Code (EECC): Services

New definition of 'Electronic communication services' (ECS)



European Electronic Communications Code (EECC): Services

Scope of services provisions

Provisions applicable to **all ECS**:

- **Security provisions**
- **Equivalence in access for disabled end-users**
- **Interoperability** (safeguard power in case of "appreciable threat" to end-to-end connectivity)
- **Emergency services** (safeguard power in case of "appreciable threat" to effective access to emergency services)
- **Confidentiality provisions** (see proposal for ePrivacy Regulation)

Other provisions apply to IAS and/or number-based ICS, or to all ECS other than number-independent ICS

3. Guaranteed privacy for both content & metadata of electronic communications

- **Privacy will be guaranteed for both content and metadata** derived from electronic communications
  - e.g. who was called, the timing, location and duration of the call, as well as websites visited
- **Both content and metadata will need to be anonymised or deleted** if users have **not given their consent**, unless the data is required for instance for billing purposes

4. New business opportunities for traditional telecoms operators when processing communications data

- **Once users have given their consent** to process communication content and/or metadata, **traditional telecommunications** services will have **more opportunities** to use data and **provide additional services**
  - e.g. they could produce heat maps indicating people's presence; this would help public authorities & transport companies develop new infrastructure projects

Article 6.1

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:
(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

Article 6.2

Permitted processing of electronic communications data

2. Providers of electronic communications services may process electronic communications metadata if:
(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/212011 for the duration necessary for that purpose; or
(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or
(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

Article 6.3

Permitted processing of electronic communications data

3. Providers of the electronic communications services may process electronic communications content only:
(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or
(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

Article 7.1

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

Article 7.2

Storage and erasure of electronic communications data

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

Article 7.3

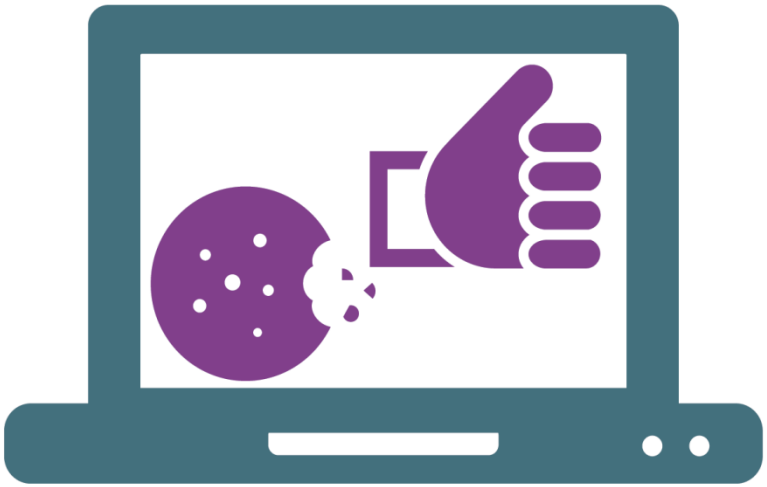
Storage and erasure of electronic communications data

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

4. Stronger rules & more effective enforcement

- **Updating the current Directive with a directly applicable Regulation** will guarantee **the same level of protection** for all people and businesses
  - Businesses will benefit from one single set of rules across the EU
- **Alignment** with GDPR: The **enforcement** of the Regulation will be the **responsibility of national data protection authorities (DPAs)** and adaption of fines
  - This will ensure their **uniform application** across the EU

5. Simpler rules on cookies



- The **"cookie provision",** which has resulted in an overload of consent requests for internet users, will be **streamlined**
- **Browser settings** will offer an **easy way to allow or refuse cookies**
- The proposal clarifies that **non- intrusive cookies** improving internet experience (e.g. your shopping cart history) **do not require consent**
- **Cookies set by a visited website** counting the number of visitors to that website **will no longer require consent**

Recital 20

Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, **are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms**. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the **information related to such equipment requires enhanced privacy protection**. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes.

Article 8.1

Protection of information stored in and related to end-users' terminal equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

Article 8.1

Protection of information stored in and related to end-users' terminal equipment

1. (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
(b) the end-user has given his or her consent; or
(c) it is necessary for providing an information society service requested by the end-user; or
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.

Article 10.1

Information and options for privacy settings to be provided

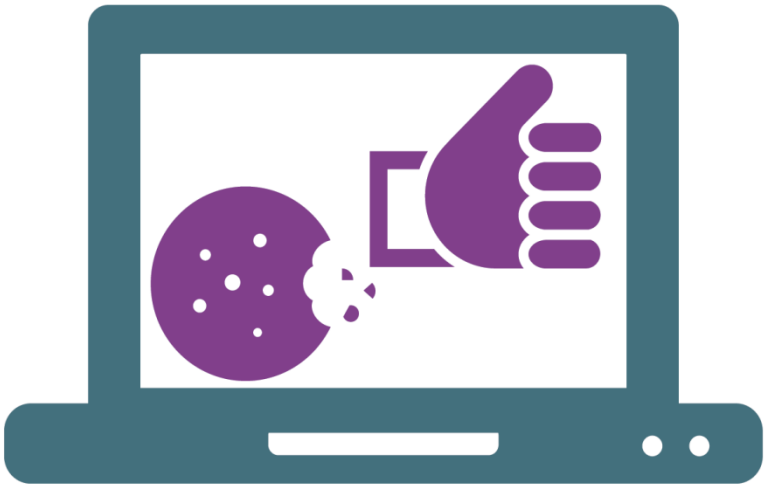
1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

Article 10.2

Information and options for privacy settings to be provided

2. Upon installation, the software 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.

6. Specific new provision on collection of certain data packages



- Collection of information emitted to maintain or restore an connection as well as MAC address, IMEI, IMSI, etc.
- **Use of such information for purposes other than maintaining or restoring of a communication:**
  - Obligation to inform users (displaying prominent notices)
  - Security measures

Recital 25

Accessing electronic communications networks requires the **regular emission of certain data packets** in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a **unique address assigned in order to be identifiable on that network**. Wireless and cellular **telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc.** A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to end-users, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.

Article 8.2

Protection of information stored in and related to end-users' terminal equipment

2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.
The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

7. Protection against spam

- **People will need to agree** before marketing messages are addressed to them by automated calling machines, SMS or e-mail
- For **voice-to-voice calls**, people will be **protected by default** or unless Member States put an opt-out regime in place (**do-not-call list**)
- Marketing callers will need to display their phone number or **use a special pre-fix**

8. Publicly available directories

- **Natural persons**' data can be included in a **publicly available directory** on the basis of **consent**
- Publicly available directories inform about **search functions** and obtain natural persons' consent before enabling them
- **Legal persons** are given the **possibility to object** to being included in a publicly available directory

New ePrivacy rules overview

1. **Update current rules**, extending their scope to all electronic communication providers

2. **Create new possibilities to process communication data** and **reinforce trust and security** in the Digital Single Market

3. **Align the rules** for electronic communications with the new world-class standards of the **EU's General Data Protection Regulation**